ALGEBRA

LARRY SUSANKA

Abstract. This is an appendix for a book I have (mostly) written on measure theory. It constitutes an introduction to abstract algebra, oriented toward some applications to analysis.

It is an essentially self-contained presentation though it does reference in a few places material of the rest of the text regarding notation, the Integers, the Axiom of Choice and other matters. Most of those references are to Chapter One "Some Preliminaries" which has been included here.

It does contain quite a few of the results one sees in a typical introductory course in the subject, including groups, rings, modules, algebras and their homomorphisms as well as some examples.

Contents

Date: April 22, 2020.

Some Preliminaries April 22, 2020

1. Functions

A **relation**, or more precisely a **binary relation**, is a nonempty subset of some product set

$$\boldsymbol{S \times T} = \{\, (s,t) \mid s \in S \text{ and } t \in T \,\},$$

the set of **ordered pairs** formed from nonempty sets S and T.

The **domain** of a relation f consists of the set of first components of any member of f, while the **range** consists of the set of second components, and these sets can be denoted **Domain(f)** and **Range(f)** respectively.

Relations are used to model many different ideas, but three basic kinds of relations will be of interest over the next few sections. The first of these is the familiar concept of "function."

A **function** f (sometimes also called a **map**) from S to T, described by $\boldsymbol{f\colon S \to T}$, is a relation as above with domain S and range contained in (not necessarily equal to) T and which has the following property:

$$(a,b) \ \in \ f \text{ and } (a,c) \ \in \ f \Rightarrow b = c.$$

These properties insure that there is one and only one ordered pair in f having a as first coordinate for every member a of S. The range of a function is, in many sources, called the **image** of that function.

Note that the concept of function is domain dependent: the same set of pairs thought of as a subset of $R \times T$, where S is contained in but not equal to R, won't be a function. And there is a certain latitude with regard to T: it can be replaced in the description $f\colon S \to T$ by any set containing $Range(f)$.

Often, though, it is T itself under study and how $Range(f)$ sits (or could sit) in T reflects important information about T. In that context T will be called the **co-domain** of function f.

If f is a function, the notation $f(a)$ or f_a is used for $b \in T$ when $(a,b) \in f$. Occasionally a function will be said to **index** its range, and in this case the range is said to be **indexed by** the domain, whose members are called **indices**.

If A is a set[1] and $f\colon S \to T$ we define

$$\boldsymbol{f(A)} = \{\, f(s) \mid s \in A \cap S \,\} \quad \text{and} \quad \boldsymbol{f^{-1}(A)} = \{\, s \in S \mid f(s) \in A \,\}.$$

Both sets can be empty. If $f^{-1}(\{t\})$ contains at most a single member of S for each $t \in T$ we call f **one-to-one** and if $f(S) = T$ we say f is **onto** T.

If f is one-to-one and onto T then f can be used to construct a function $\boldsymbol{f^{-1}\colon T \to S}$ by defining $f^{-1}(t)$, for each $t \in T$, to be that member s of S with $f(s) = t$. This **second** definition of f^{-1} is an abuse of notation that could cause ambiguity in case, for example, both t and $\{t\}$ are members of T.

If f is one-to-one but not onto T then f cannot be used to define f^{-1} as a function from T to S. However f^{-1} would be a function thought of as the set of pairs $\{\, (f(s), s) \mid s \in S \,\}$ in $f(S) \times S$.

---

[1]We presume here that the set A is not actually an element of domain or range of function f.

The **restriction** of a function $f\colon S \to T$ to a nonempty set $A \subset S$ is denoted $\boldsymbol{f|_A}$ and defined to be $\{\,(a,b) \in f \mid a \in A\,\}$. $f|_A$ is a function with domain A. If g and f are functions and $f \subset g$ then $g|_S = f$ and g is called an **extension** of f.

Here are a few more items of notation:

The set of functions with domain S and co-domain T is denoted $\boldsymbol{T^S}$.

If T is the two element set $\{0,1\}$, T^S will sometimes be denoted $\boldsymbol{2^S}$.

The collection of all subsets of a set S form a set denoted $\boldsymbol{\mathbb{P}(S)}$, called the **power set** of S.

If A and X are any sets, the notation $\boldsymbol{X - A} = \{\,x \in X \mid x \notin A\,\}$ is used. $X - A$ is called the **complement of A in X**.

If A and X are nonempty sets and $f\colon A \to \mathbb{P}(X)$ the notation $\boldsymbol{\bigcup_{a\in A} f_a}$ denotes $\{\,x \in X \mid x \in f_a \text{ for some } a \in A\,\}$. The notation $\boldsymbol{\bigcap_{a\in A} f_a}$ denotes $\{\,x \in X \mid x \in f_a \text{ for every } a \in A\,\}$.

Sets S and T with similar properties can arise from different sources. Recognizing that two sets are essentially the same in some way often comes through the presentation of a one-to-one function $g\colon S \to T$ that is onto T.

When we have this in mind, we will say that S and T are **identified** and that g identifies the element $s \in S$ with the element $g(s) \in T$. The notation $\boldsymbol{s \leftrightarrow g(s)}$ can be used to illustrate such an identification. These identifications can range in utility from a trivial convenience to something more substantial, a shift in context.

For instance, on the trivial side, if n is a positive integer, the set $\{1,\dots,n\}$ can be identified with $\{0,\dots,n-1\}$ through the function described by $x \leftrightarrow x-1$. More substantial examples of this vocabulary in action follow.

2^S can be identified with $\mathbb{P}(S)$ via $f \leftrightarrow \{\,a \in S \mid f(a) = 1\,\}$.

Suppose $S_0,\ \dots,\ S_{n-1}$ are nonempty sets for some integer $n > 2$. Define $S_0 \times S_1 \times S_2$ to be $S_0 \times (S_1 \times S_2)$. More generally, $S_0 \times \cdots \times S_{n-1}$ is given by a recursive definition as $S_0 \times (S_1 \times \cdots \times S_{n-1})$. This last is called the set of all "ordered n-tuples" formed from the S_i in the specified order. Let W denote the set of all functions $f\colon \{0,\dots,n-1\} \to \bigcup_{i=0}^{n-1} S_i$ having the property that $f(i) \in S_i$ for $i = 0,\dots,n-1$. Then $S_0 \times \cdots \times S_{n-1}$ can be identified with W by $(a_0,\dots,a_{n-1}) \leftrightarrow f$ where $f(k) = a_k$ for $k = 0,\dots,n-1$.

2. Equivalence Relations

Our second use of relations is the standard method used by mathematicians to lump together objects that are manifestly different but which are similar in some way. In this context we focus on the similarities and ignore other properties.

An **equivalence relation** on S is a relation $P \subset S \times S$ that has three properties:

$(a,a) \in P\ \forall a \in S$ and (**reflexivity**)

$(a,b) \in P \Rightarrow (b,a) \in P$ and (**symmetry**)

$(a,b) \in P$ and $(b,c) \in P \Rightarrow (a,c) \in P$. (**transitivity**)

For equivalence relations, the notation $\boldsymbol{a \sim b}$ is usually used when $(a, b) \in P$.

A **partition** of any set S is a set of subsets of S whose union is S and whose **pairwise** (that is, each pair of them) intersections are **void** (that is, the empty set.) Any pair of sets whose intersection is empty is called **disjoint**, and a union of pairwise disjoint sets is called a **disjoint union**.

After presenting an equivalence relation on S, one would typically form, for each a in S, sets $[a] = \{\, b \mid a \sim b \,\}$. These sets are called **equivalence classes** and together form a partition of S denoted $\mathbf{S/P}$ or $\mathbf{S}/\!\sim$. Often any member of an equivalence class will be used to refer to the whole class without comment, and it is the set of classes that is of primary interest.

Alternatively, any partition of a set S could be used to form an equivalence relation on the set, where $a \sim b$ precisely when a and b are in the same partition member.

Most people have seen equivalence relations from grade school. The rational numbers constitute a very important first example.

Let S be the set of all ordered pairs of integers (c, d) indicated here by c/d where we require that $d \neq 0$. (For a discussion of the construction of the integers, see Section 5.) We say that $c/d \sim e/f$ if and only if $cf = ed$. It is easy to show this is an equivalence relation. For each c/d in S let $[c/d] = \{\, e/f \in S \mid cf = ed \,\}$. The sets $[c/d]$ form a partition of S. Any ordered pair might be called upon to represent the whole class. That is what is meant by "$2/6 = 4/12$." The collection of these classes is normally referred to as the **rational numbers**, denoted $\mathbb{Q}$.

The operations $[a/b] + [c/d] = [(ad + bc)/(bd)]$ and $[a/b][c/d] = [(ac)/(bd)]$ are **well-defined**.

In this context, "**well-defined**" means that the operations, defined here using particular representations of the equivalence classes involved, do not in fact depend on which representative is used. **Statements of this kind, wherever found in the text, require proof.** If not obvious or proved in the text, the reader should supply the proof as an exercise, or simply accept the statement as true. Since all books contain errors, oversights, mis-statements or infelicitous phrasing, the former course is the safer.

$\mathbb{Q}$ has multiplicative and additive identities $[b/b]$ and $[0/b]$ respectively, otherwise known as 1 and 0.

Another example is the usual representation, found in many beginning Physics classes, of vectors in the plane as "arrows" with a given length and direction. One takes the point of view that a vector is determined by these two quantities alone and its location is irrelevant. So a vector is really a class of arrows that are alike in these two ways. One refers to the whole class by identifying any member of the class. In the world of vector operations such as vector addition or scalar multiplication the usual representative for a class is the arrow with tail at a specified origin, with coordinate axes centered there. With this choice the coordinates of the tip alone suffice to describe the class, and common vector operations are conveniently calculated.

The concept of equivalency, along with the companion concept of identification, can be seen throughout mathematics.

3. Order Relations

In this section we try to extract the essence of the idea of "less than" as thought of in the following three examples:

> 3 is said to be "less than" 7 on the number line because it is to the left when one represents the real numbers ordered as a line in the usual way.
>
> Consider a desk covered with many layers of paper. We might say one piece of paper is "less than or equal to" another if its distance to the table top is equal or less than the other: an ordering by "height above the table."
>
> We think of one set as "bigger than or equal to" another if it contains the other. Sets can be said to be **ordered by containment**, a very important example.

The relations we use to model these ideas are called **order relations**.

A **pre-order** on a set S is a relation $P \subset S \times S$ that has the reflexivity and transitivity properties: $((a,a) \in P \ \forall a \in S)$ and $((a,b) \in P$ and $(b,c) \in P \Rightarrow (a,c) \in P)$.

The notation $\boldsymbol{a \leq b}$ will be used to indicate that $(a,b) \in P$, while $\boldsymbol{a < b}$ will indicate that $(a,b) \in P$ but $(b,a) \notin P$.

Suppose $B \subset S$. b is called an **upper bound** for B (in the pre-ordered set S if that specificity is warranted) if $b \in S$ and $a \leq b \ \forall a \in B$.

If B has an upper bound, B is called **bounded above**. If, further, $c \in S$ and $a \leq c \ \forall a \in B \Rightarrow b \leq c$ then b is called a **least upper bound** for B.

If b is a unique least upper bound for B (that is, the only one) then b is also called the **supremum** of B, denoted $\boldsymbol{\sup B}$ or $\boldsymbol{\sup(B)}$. The supremum of a set $\{a,b\}$, if it exists, is denoted $\boldsymbol{a \vee b}$.

An element b of S is called **maximal** if $c \in S$ and $b \leq c \Rightarrow c \leq b$.

A function $f\colon J \to S$ is called **bounded above** if its range is bounded above. The **supremum of a function** f is denoted $\boldsymbol{\sup(f)}$ or $\boldsymbol{\bigvee_{\alpha \in J} f(\alpha)}$ and is defined to be $\sup\{\, f(\alpha) \mid \alpha \in J \,\}$ whenever the supremum exists.

In the case of $J = \mathbb{N}$, the non-negative integers, a function $f\colon \mathbb{N} \to S$ is called a **sequence** in S. In this case the notation $\boldsymbol{\bigvee_{i=0}^{\infty} f(i)}$ may be seen in place of $\bigvee_{i \in \mathbb{N}} f(i)$.

When $J = \{k, k+1, \ldots, n\}$ we may write $\boldsymbol{\bigvee_{i=k}^{n} f(i)}$ rather than $\bigvee_{\alpha \in J} f(\alpha)$.

The definitions of $\boldsymbol{\geq}$, $\boldsymbol{>}$, **lower bound, bounded below, greatest lower bound, infimum,** $\boldsymbol{\inf B}$, $\boldsymbol{\inf(B)}$, $\boldsymbol{a \wedge b}$, **minimal**, $\boldsymbol{\inf(f)}$, $\boldsymbol{\bigwedge_{\alpha \in J} f(\alpha)}$, $\boldsymbol{\bigwedge_{i=0}^{\infty} f(i)}$ and $\boldsymbol{\bigwedge_{i=k}^{n} f(i)}$ are the obvious adaptations of the list of definitions above with ordered pairs (that is, inequalities) reversed.

A set or function as above is called **bounded** if it is bounded both above and below. Otherwise, it is called **unbounded.**

Since functions are defined to *be* sets there is potential for ambiguity in the definitions just given involving functions, which focus on the order properties in

the range alone. The ordered pairs in a function will not usually have an order specified for them so this will rarely be an issue.

The pre-order P is called a **partial order** if, in addition to reflexivity and transitivity, we have:

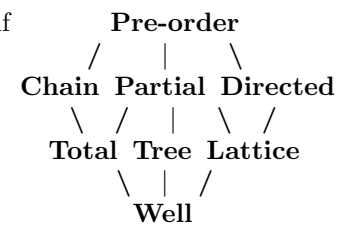
$$a \leq b \text{ and } b \leq a \Rightarrow a = b. \qquad \textbf{(antisymmetry)}$$

A partial order can be created from any pre-order on a set S by the following process. Let $a \sim b$ if and only if $a \leq b$ and $b \leq a$. Consider the set of equivalence classes $S/\sim$ generated by this equivalence relation. We will say $[a] \leq [b]$ precisely when $a \leq b$. This relation is well-defined (that is, it does not depend on the representatives of the classes used to define it) and a partial order on $S/\sim$.

Note that if P is a partial order, least upper bounds and greatest lower bounds are unique if they exist. Also, in this case, if b is maximal, $a \in S$ and $b \leq a$ then $b = a$. A similar result holds if b is minimal.

If P is a pre-order and $A \subset S$, A is called a **chain** if whenever a and b are in A then either $a \leq b$ or $b \leq a$.

If P is a pre-order and for each pair a and b in S one can find c in S such that $a \leq c$ and $b \leq c$ we say that P **directs** S, and S with P is called a **directed set**.



P, or sometimes S with P, is called a **lattice** if it is a partial order for which each pair of elements has a greatest lower bound and a least upper bound.

If S with partial order P is itself a chain, P is called a **total order**. In some contexts a total order is also called a **linear order**.

A total order on S which has the property that every nonempty subset of S contains a minimal element is called a **well-order**.

For brevity, one often refers to S as "**ordered by** P," P is said to "**order** S" and S is said to "**have the order** P." This vocabulary is extended to the various types of orders. Sometimes, when this will not cause ambiguity, the set S will be said to be ordered and the specific order P will be understood to exist without explicit mention.

As an example of this vocabulary in use we have the following interesting result:

Subsets of well-ordered S are well-ordered with the order **inherited** from S.

We define, for each α in pre-ordered S, the sets

$$\boldsymbol{I_\alpha} = \{\, \beta \in S \mid \beta < \alpha \,\} \quad \text{and} \quad \boldsymbol{T_\alpha} = \{\, \beta \in S \mid \beta \geq \alpha \,\}$$

are called **initial** and **terminal segments** in S, respectively.

Note that the T_α are distinct for different values of α in partially ordered S, but the I_α need not be distinct. They will be distinct if S is totally ordered.

If S is partially ordered and $\alpha, \beta \in S$ and $\beta > \alpha$ we say that β is **a successor** to α and α is **a predecessor** to β. If, further, there is no other member of S between α and β we say that β is **an immediate successor** to α and α is **an immediate predecessor** to β.

Suppose S is a generic well-ordered set. Unless there is a compelling reason to deviate, it will be standard practice to denote the first element of S as 0 and the second member by 1. For $\alpha \in S$, we will use $\boldsymbol{\alpha + 1}$ to denote the least successor to α. Unless α is the supremum of S, this immediate successor to α will always exist in well-ordered S.

$\alpha+1$ is called **the successor** to α and α is called **the predecessor** to $\alpha+1$. The vocabulary recognizes the fact that there can be at most one immediate successor or immediate predecessor in any totally ordered set.

Any member of S **except the first** that cannot be written as $\alpha + 1$ for some α in S is called a **limit member** of S. A limit member has predecessors (many of them) but no *immediate* predecessor.

If S is partially ordered and if, for each $\alpha \in S$, the initial segment I_α is well-ordered with the order inherited from S we call S with this order a **tree.**

A **branch** of a tree S is a nonempty subset B of S which is a chain with the induced order and which is maximal in the following sense:

$$\text{for each } s \in S, \text{ either } s \in B \text{ or } \{s\} \cup B \text{ is not a chain.}$$

So the well-ordered set $I_\alpha \cup \{\, \alpha \,\}$ is contained in branch B whenever $\alpha \in B$.

A **root** of a tree S is a member r of S for which $S = T_r$. A tree S is called **rooted** if it has a unique root.

3.1. ***Exercise.*** *(i) Is it true that the intersection of two or more (distinct) branches in a rooted tree is an initial segment?*

(ii) If S is a tree and $r \in S$ then T_r is a rooted tree.

If S is well-ordered and A is any union or any intersection of initial segments then A is either all of S or itself an initial segment. To see this, let α be the least member of S, if any, that is not in A. Then A is I_α. Similarly, if A is any union or intersection of terminal segments in well-ordered S, then A is itself a terminal segment or void.

3.2. ***Exercise.*** *Suppose S is a well-ordered set. Prove:*

$$S = I_\alpha \cup T_\alpha \text{ for every } \alpha \text{ in } S \qquad I_0 = \varnothing \qquad T_0 = S$$

$$T_\alpha \text{ is never empty} \qquad I_{\alpha+1} = I_\alpha \cup \{\alpha\} \text{ whenever } \alpha + 1 \text{ is defined.}$$

A function $f\colon A \to B$ between two pre-ordered sets is called **non-decreasing** if $f(\alpha) \le f(\beta)$ whenever $\alpha \le \beta$. f is called **increasing** if $f(\alpha) < f(\beta)$ whenever $\alpha < \beta$. Neither condition implies that f is one-to-one. However if the order on A is a total order, the second condition does imply that f is one-to-one.

f is called **non-increasing** if $f(\alpha) \ge f(\beta)$ whenever $\alpha \le \beta$. f is called **decreasing** if $f(\alpha) > f(\beta)$ whenever $\alpha < \beta$.

f is called **monotone** if it is non-increasing or non-decreasing.

Suppose $f\colon A \to B$ is a function *between two partially ordered sets.* If f is non-decreasing and f^{-1} exists and is non-decreasing, f is called an **order-isomorphism** and A and B are said to be **order-isomorphic**.

3.3. ***Exercise.*** *(i) Suppose $f\colon A \to B$ is non-increasing, where A is totally ordered and B is partially ordered. In the definition of order-isomorphism applied to f the requirement that f^{-1} be non-decreasing is redundant.*

(ii) Suppose $f\colon A \to B$ is non-increasing, where A is totally ordered and B is well-ordered. Then f is eventually constant: that is, there is an $a \in A$ for which $c \geq a$ implies $f(c) = f(a)$.

(iii) If S is well-ordered, S is order-isomorphic to $\{\, I_\alpha \mid \alpha \in S \,\}$ ordered by containment.

(iv) If S is partially ordered, S is order-isomorphic to $\{\, \{\alpha\} \cup I_\alpha \mid \alpha \in S \,\}$ ordered by containment.

(v) If S is partially ordered, S is order-isomorphic to $\{\, T_\alpha \mid \alpha \in S \,\}$ ordered by ***reverse containment****: that is, $T_\alpha < T_\beta$ if $T_\alpha \neq T_\beta$ and $T_\alpha \supset T_\beta$.*

Parts (iii) through (v) of the exercise show that any partial order—and well-orders in particular—can be thought of as containment orders on families of subsets of S in several ways.

4. The Integers

We sketch in some detail the recognition of a set we will identify with the natural numbers, as you have come to know them from ordinary counting and grade-school arithmetic.

You, no doubt, have some conception of the nature of a set and readily assert the existence of sets with certain properties, combine sets in various ways, and understand what you must show to claim equality of two sets.

These conceptions were around *long before* mathematicians found it necessary to (try to) create bulletproof axiomatic structures founded on inexorable and indisputable logical chains to justify theorems. Having been burned a few times we have had a certain amount of humility forced upon us, and the various "obvious" properties of sets (which we have already used many times without remark in the preceding pages) is explored in some detail in Sections **??** and **??**. These sections really do need to be examined, sooner or later.

As an example of the kind of thing that must be made explicit, and to get things started, the following assumption (to be accepted without proof) is required.

Axiom of the Empty Set:

There exists a set, denoted $\varnothing$, which has no elements.

Without this (or some similar) assumption, we cannot conclude that there are any sets whatsoever! That would mean all our discussions about sets have been about nothing, a situation tailor-made for irony if ever there was one. We accept this axiom.

If X is a set, for now we will let X^* be the set $\{X\} \cup X$.

We let $0 = \varnothing,\ 1 = 0^*,\ 2 = 1^*,\ 3 = 2^*$ and so forth. Another way of writing this is: $0 = \varnothing,\ 1 = \{0\},\ 2 = \{0, 1\},\ 3 = \{0, 1, 2\}$ and so on.

In addition to axioms justifying the obvious operations indicated above, to complete the definition of the natural numbers it is necessary to invoke another axiom of set theory, called the Axiom of Infinity. Essentially this axiom asserts that there exists at least one non-finite set and this is *not* an obvious fact; at least, it is not obvious to *everyone.*

Axiom of Infinity:

> There exists a set A with $\varnothing \in A$ and such that whenever X is a set and $X \in A$ then $X^* \in A$.

Note that the intersection of any pair of sets of the type whose existence is guaranteed by this axiom is also of this type.

Let A be one of these sets. The **natural numbers**, denoted $\mathbb{N}$, consist of the intersection of all subsets S of A for which $\varnothing \in S$ and such that whenever X is a set and $X \in S$ then $X^* \in S$. In light of the last observation, $\mathbb{N}$ does not depend on the specific choice of A, only that there is at least one such set.

It is only because of the Axiom of Infinity that we know that $\mathbb{N}$, which we might have carelessly denoted $\{\, 0, 1, 2, 3, \dots \}$, is actually a set, and therefore eligible to participate in the various set operations and assertions we might make about sets.

The empty set is said to **have 0 elements**. If S is a nonempty set and n is a **positive integer** (that is, $n \in \mathbb{N}$ and $n \neq 0$) we say **S has n elements** if there is a one-to-one and onto function $f\colon S \to n$. We say S is **finite** if it has n elements for some $n \in \mathbb{N}$. S is called **infinite** if it is not finite. We will discuss this concept again in Sections **??** and **??**.

The natural numbers are partially ordered by containment, and it turns out that this ordering on $\mathbb{N}$ is actually a well-order.

Henceforth, if $n \in \mathbb{N}$ we will use $\mathbf{n + 1}$ in preference to n^*.

The definition of $\mathbb{N}$ is just what we need to create **Proof by Induction.**

If we have some property P which is either true or false for members of $\mathbb{N}$, let

$$S = \{\, n \in \mathbb{N} \mid P \text{ is true for } n \,\}.$$

If $0 \in S$ and if $n \in S$ implies $n + 1 \in S$ then S is a set of the kind whose existence is asserted in the Axiom of Infinity. Since $\mathbb{N}$ is the intersection of all such sets, $S = \mathbb{N}$.

In other words, **we would then be authorized to conclude that *P* is true for every member of** $\mathbb{N}$**.**

4.1. ***Exercise.*** *(i) As an (easy) exercise using induction, show that every member of* $\mathbb{N}$ *except* 0 *contains* 0 *among its elements, and can be written as* $n + 1$ *for some* $n \in \mathbb{N}$*.*

(ii) Let $S = \{\, n \in \mathbb{N} \mid x \in n \Rightarrow x \in \mathbb{N} \,\}$*. Then* $S = \mathbb{N}$*. Every element of a natural number is a natural number.*

(iii) Let $S = \{\, n \in \mathbb{N} \mid x \in n \Rightarrow x \subset n \,\}$*. Then* $S = \mathbb{N}$*. Every element of a natural number is a subset of that natural number.*

(iv) $m + 1 = n + 1 \Rightarrow m = n$*.*

(v) For $j \in \mathbb{N}$ let $S_j = \{\, n \in \mathbb{N} \mid j \subset n \Rightarrow j = n \text{ or } j \in n \,\}$. Then $S_j = \mathbb{N}$. (hint: $\mathbb{N} = S_0$ since the condition for membership in S_0 is trivially satisfied for all members of $\mathbb{N}$, and also 0 is in every S_j. Now suppose $n \in S_j$ and $j \subset n+1 = n \cup \{\, n \,\}$. If $n \notin j$ then we have $j \subset n$ so by hypothesis $j = n \in n+1$ or $j \in n \subset n+1$. On the other hand, if $n \in j$ we have $n \subset j \subset n+1 = n \cup \{\, n \,\}$ so $j = n+1$ or $j = n \in n+1$.)

(vi) For $j \in \mathbb{N}$ let $S_j = \{\, n \in \mathbb{N} \mid j \subset n \text{ or } n \subset j \,\}$. Then $S_j = \mathbb{N}$. This implies that $\mathbb{N}$ is a total order with containment order.

(vii) Now define B to be the set:

$$\{\, n \in \mathbb{N} \mid \text{ if } k \in W \subset \mathbb{N} \text{ for some } k \subset n \text{ then } W \text{ contains a least member.} \,\}$$

Obviously $\varnothing \in B$ and it is not hard to show that if $n \in B$ then $n+1 \in B$. We conclude that $B = \mathbb{N}$ so $\mathbb{N}$ ***is well-ordered by containment order.***

(viii) The natural numbers have another interesting property. Every set of natural numbers that is bounded above has a least upper bound and contains this least upper bound.

We can use the facts from this exercise and induction to show that **a set C cannot have both m elements and n elements for natural numbers $n \neq m$.**

To see this, let S consist of those members s of $\mathbb{N}$ for which there is a member n of $\mathbb{N}$, $n \neq s$, and a set C which has both s elements and n elements. Obviously $\varnothing \notin S$, so every member of S has the form $k+1$ for some natural number k. Should S be nonempty, it would contain a least member, and this leads easily to a contradiction. We conclude S is empty, and there is at most a single natural number n for which the statement "C has n elements" is true.

Note that each positive integer n is, itself, a well-ordered set which has n elements. Any natural number n is, in fact, the initial segment I_n in $\mathbb{N}$.

$\mathbb{N}$ **is an infinite set.** To see this, suppose $h\colon \mathbb{N} \to k+1$ is one-to-one and onto. Then $h(m) = k$ for some $m \in \mathbb{N}$. Define $f\colon \mathbb{N} \to \mathbb{N}$ by $f(a) = a$ when $a < m$ and $f(a) = a+1$ if $a \geq m$. But then $h \circ f\colon \mathbb{N} \to k$ is one-to-one and onto. Since it is obvious that there can be no one-to-one function $h\colon \mathbb{N} \to 1$, the result follows.

Our next steps, left to the energetic reader, are to define negative integers and then the **integers**, denoted $\mathbb{Z}$, comprised of the natural numbers and the negative integers. The order on $\mathbb{N}$ is used to form a total order on $\mathbb{Z}$.

Though addition and multiplication of integers could be defined now, demonstrating that they have the usual properties such as commutativity, the distributive law and so on using the tools we have built to this point is a lengthy series of applications of induction. Connecting these operations to the order relation on the integers also requires more than a bit of work.

For instance, if a, b and m are positive integers and $m = ab$ then both $a \leq m$ and $b \leq m$. And if $a > 1$ then $b < m$. But what does it take, exactly, to prove that? Laying out every last detail about basic integer arithmetic is a big project, falling under the heading of number theory and logic. Gottlob Frege and Bertrand Russell are among the luminaries who broke teeth on it. You might wish to review Exercises **??** and **??** and the more sophisticated techniques assembled in Appendix **??**. In this work we will simply assume various "obvious" facts about integers.

With the integers in hand, one can define the rational numbers, $\mathbb{Q}$, as suggested in Section 2.

4.2. ***Exercise.*** *Till now we have had no specific well-ordered sets (other than $\mathbb{N}$ and its initial segments) with which to work. Now we can create examples.*

(i) Let $\mathcal{S}$ denote the set $\left\{ m + \frac{n}{n+1} \mid n, m \in \mathbb{N} \right\}$ with the usual order from $\mathbb{Q}$. Show that $\mathcal{S}$ is well-ordered.

(ii) For any $f \in \mathbb{N}^{\mathbb{N}}$ let

$$Support(f) = \{ n \in \mathbb{N} \mid f(n) \neq 0 \}.$$

Define $\mathcal{F}$ to be those members of $\mathbb{N}^{\mathbb{N}}$ for which $Support(f)$ is a finite set. For $f \in \mathcal{F}$ let m_f denote the greatest member of $Support(f)$.

We will define an order $\leq_R$ on $\mathcal{F}$ called ***reverse lexicographic order.***

Declare $f \leq_R f$. Suppose $f, g \in \mathcal{F}$ and $f \neq g$. Let j be the ***last*** *integer for which $f(j) \neq g(j)$. Declare $f \leq_R g$ if $f(j) < g(j)$.*

Show that $\mathcal{F}$ is well-ordered with $\leq_R$. (hint: First show transitivity and conclude that $\leq_R$ is a total order. With that in hand, suppose H is a subset of $\mathcal{F}$ with at least two members. Let n_1 denote the least m_f of any $f \in H$. Let

$$H_1 = \{ f \in H \mid m_f = n_1 \} \quad \text{and} \quad G_1 = \{ g \in H_1 \mid g(n_1) \leq f(n_1) \ \forall f \in H_1 \}.$$

If G_1 contains a single member we stop: this member is the minimal member of H. If G_1 contains more than one member, let n_2 denote the smallest integer for which there is some $g \in G_1$ with $g(n_2) \neq 0$ but $g(k) = 0$ for all k with $n_2 < k < n_1$. Possibly, $n_2 = n_1 - 1$. Now let

$$G_2 = \{ g \in G_1 \mid g(n_2) \leq f(n_2) \ \forall f \in G_1 \}.$$

If G_2 contains a single element it is the least member of H. If G_2 contains more than a single member we can continue, creating by this procedure a strictly decreasing list $n_1, n_2, \ldots$ in $\mathbb{N}$. Such a list cannot be infinite in any well-ordered set. It must terminate at some least n_k, and the sole member of G_k is the minimal member of H.)

(iii) Define $\mathcal{F}_1$ to be those members f of $\mathcal{F}$ with $m_f = 0$ or 1. This set inherits the reverse lexicographic well-order from $\mathcal{F}$. How is this order on $\mathcal{F}_1$ related to that on $\mathcal{S}$ from part (i)?

(iv) We will define a different order $\leq_L$ on $\mathcal{F}$ called ***lexicographic order.*** *Declare $f \leq_L f$. Suppose $f, g \in \mathcal{F}$ and $f \neq g$. Let j be the* ***first*** *integer for which $f(j) \neq g(j)$. Declare $f \leq_L g$ if $f(j) < g(j)$ and $g \leq_L f$ otherwise. Though $\mathcal{F}$ is totally ordered with $\leq_L$, it is not well-ordered.*

The difference between $\leq_R$ and $\leq_L$ boils down to the following fact. It is impossible to create a strictly decreasing sequence of m_f values, but it is certainly possible to have a strictly increasing sequence of these values.

$$100000\ldots,\ 010000\ldots,\ 001000\ldots,\ 000100\ldots,\ 000010\ldots,\ \ldots\ldots$$

(v) Suppose A and B are disjoint well-ordered sets. Create an order on $A \cup B$ corresponding to "elements of A all follow any element of B," while retaining the given orders on A and B. Show that this order is a well-order.

(vi) Sometimes it will be convenient in certain arguments to have a well-ordered set with a last member. In general, well-ordered sets might not ***have*** *a last member. Suppose C is well-ordered with first element a_1 and more than one element. Give $A = C - \{a_1\}$ the inherited well-order and let $B = \{a_1\}$. Using (v) create a well-order on C that* ***does*** *have a last member.*

(vii) Suppose A and B are well-ordered sets. Create a well-order on a ***subset*** *of A^B analogous to the reverse lexicographic order $\leq_R$ we created for $\mathcal{F}$ in part (ii).*

5. The Real Numbers

We will now make one of the common definitions of the real numbers and discuss some important properties of this set. The following construction is due to Dedekind.

Let $\mathbb{Q}^+$ be the set of *non-negative*[2] rational numbers. We define $\mathbb{R}^+ \subset \mathbb{P}(\mathbb{Q}^+)$ to consist of exactly those sets A of non-negative rational numbers with the following three properties:

(i) A has no largest member and

(ii) $q \in A \Rightarrow p \in A \ \forall p \in \mathbb{Q}^+$ with $p \leq q$ and

(iii) $A \neq \mathbb{Q}^+$.

$\mathbb{R}^+$ is (obviously) nonempty and called the set of **non-negative real numbers**. A non-negative real number, created this way, may be called a **Dedekind cut.**

If r and s are non-negative real numbers, we say $r < s$ if $r \neq s$ and $r \subset s$.

This relation is a total order on $\mathbb{R}^+$ but it is not a well-order. In fact no explicit well-order of the real numbers is known.

If r and s are nonempty (that is, "**positive**") members of $\mathbb{R}^+$ and $t \in \mathbb{R}^+$ we define binary operations "$+$" and "$\cdot$" by:

$$t + \varnothing = t \quad \text{and} \quad r + s = \{\, u \in \mathbb{Q}^+ \mid u < q + p \text{ for some } q \in r \text{ and } p \in s \,\},$$
$$t \cdot \varnothing = \varnothing \quad \text{and} \quad r \cdot s = \{\, u \in \mathbb{Q}^+ \mid u < q \cdot p \text{ for some } q \in r \text{ and } p \in s \,\}.$$

It is an exercise to show that $r + s$ and $r \cdot s$ are non-negative real numbers and the operations satisfy the commonly listed properties of addition and multiplication with multiplicative identity given by $\{\, [a/b] \in \mathbb{Q}^+ \mid 0 < a < b \,\}$ and additive identity $\varnothing$, which will henceforth be denoted 1 and 0, respectively. Multiplicative inverses exist for positive real numbers.

Note that this is the third usage for the symbol 1 in this section. $1 \in \mathbb{N}$ was defined to be $\{\varnothing\}$ and $1 \in \mathbb{Q}^+$ was defined as a set of ordered pairs $\{\, a/a \mid a \in \mathbb{Z} \text{ and } a \neq 0 \,\}$. We unify these disparate definitions by identifying $n \in \mathbb{N}$ with $[n/1] \in \mathbb{Q}$, and $q \in \mathbb{Q}^+$ with $\{\, p \in \mathbb{Q}^+ \mid p < q \,\} \in \mathbb{R}^+$.

Let S be any nonempty set of non-negative real numbers. If S has an upper bound in $\mathbb{R}^+$, we can show that $\bigcup_{A \in S} A \in \mathbb{R}^+$. In fact it is the supremum of S.

[2]We include 0 in $\mathbb{Q}^+$ and $\mathbb{R}^+$. Many authors don't.

Let S be any nonempty set of non-negative real numbers. $\bigcap_{A\in S} A$ might actually contain a largest rational. If it does not, then $\bigcap_{A\in S} A \in \mathbb{R}^+$ and is the infimum of S. If it does contain a largest rational, remove that rational from the intersection. The result is now in $\mathbb{R}^+$ and is the infimum of S.

If $r\colon \mathbb{N} \to \mathbb{R}^+$ is a non-decreasing sequence of non-negative real numbers that is bounded above we let

$$\lim_{\mathbf{n}\to\infty} \mathbf{r_n} = \sup\{\, r_n \mid n \in \mathbb{N}\,\}$$

If $r\colon \mathbb{N} \to \mathbb{R}^+$ is a non-increasing sequence of non-negative real numbers let

$$\lim_{\mathbf{n}\to\infty} \mathbf{r_n} = \inf\{\, r_n \mid n \in \mathbb{N}\,\}$$

In either case, this number is called the **limit** of the corresponding sequence.

At this point it is an exercise to extend all of the above to a definition of the **negative real numbers** and then to the **real numbers**—consisting of both non-negative and negative real numbers. Extend the total order on the non-negative real numbers to the real numbers. Then define **multiplication, division, addition** and **subtraction** for these numbers, and show they have the familiar properties. Define **absolute value**. Define **limits of bounded monotone sequences** of real numbers.

Henceforth we let $\mathbb{R}$ denote the **real numbers.**

Define **intervals** $[a,b)$, (a,b), $(a,b]$, $(-\infty,b)$, $(-\infty,b]$, (a,∞), $[a,\infty)$ and $[a,b]$ for real numbers a and b with $a \le b$. The **standard topology on** $\mathbb{R}$ is that formed from a basis consisting of all intervals (a,b) with $a,b \in \mathbb{Q}$.

If $r\colon \mathbb{N} \to \mathbb{R}$ is a bounded sequence we define

$$\limsup(\mathbf{r}) = \lim_{n\to\infty}(\sup\{\, r_k \mid k \in \mathbb{N} \text{ and } k > n\,\}) \quad \text{and}$$
$$\liminf(\mathbf{r}) = \lim_{n\to\infty}(\inf\{\, r_k \mid k \in \mathbb{N} \text{ and } k > n\,\})$$

Since the supremum and infimum above are being taken over smaller and smaller sets, the sequences whose limits are referred to are monotone and the limits are defined.

When these limits are equal we refer to their common value as the **limit of the sequence** r and denote this number by $\lim_{\mathbf{n}\to\infty} \mathbf{r_n}$. When the limit exists and is L we say the **sequence converges** or, when specificity is required, **converges to** L.

In applications, it is common for sequence values r_n to be defined only for n in a terminal segment of $\mathbb{N}$. Limits, if they exist, depend only on the value of r on any terminal segment. So when considering limits, we might define r_n values in any way that is convenient or not at all for n in any particular initial segment of $\mathbb{N}$.

Show that $\,|\,|a| - |b|\,| \le |\,a-b\,| \le |\,a\,| + |\,b\,|$. This is the **triangle inequality**.

Show that the limit of a sequence r exists and is a number L exactly when the limit of the sequence $|\,r - L\,|$ exists and is 0.

Two sequences r and s are called **equivalent** if $\lim_{n\to\infty} |\,r_n - s_n\,| = 0$. The exercises above can be used to show that equivalent sequences converge or not together, and if they converge it is to the same limit.

A sequence r is called a **Cauchy sequence** if

$$\lim_{n\to\infty}(\sup\{\,|\,r_n - r_k\,|\;\;|\;k > n\,\}) \quad \text{exists and is } 0.$$

It is a fact that a sequence of real numbers converges precisely when it is Cauchy, and the definition of equivalent sequences from above forms an equivalence relation on the set of convergent sequences.

These last concepts can be used in an alternative construction of the real numbers. One examines the set of all Cauchy sequences of rational numbers, and partitions that set using the equivalence relation for sequences defined above. This does involve the creation of a preliminary definition of limit, but only for rational sequences that converge to 0. The set of these classes constitute the real numbers in this formulation.

There is a more general concept of limit that pops up sometimes. This is where the indexing set is a more general directed set and not necessarily $\mathbb{N}$, and we might as well define it here.

If J is a directed set, a function $r\colon J \to Y$ is called a **net** in Y. A net is a generalization of the idea of a sequence.

Now suppose $r\colon J \to \mathbb{R}$ is a net in $\mathbb{R}$ and $L \in \mathbb{R}$.

We call L the **limit of the net** r and write $\boldsymbol{r_\alpha \xrightarrow{\alpha} L}$ if and only if

$$\forall\varepsilon > 0\ \exists\alpha \in J \text{ so that } \alpha \le \beta \Rightarrow |\,r_\beta - L\,| < \varepsilon.$$

Limits of nets in $\mathbb{R}$, when they exist, **depend only on the values of the net on any particular terminal segment of J.** So when considering these limits, we are free to modify or define the r_α values in any way that is convenient or not at all for α outside of any terminal segment of J.

It is possible for a directed set such as J to have a supremum, $\sigma = sup(J)$. In that case the limit is simply the number r_σ.

When the limit of a net in $\mathbb{R}$ exists we say the **net converges** or, when specificity is required, **converges to** L.

A net in $\mathbb{R}$ has at most one limit.

In case $J = \mathbb{N}$, show that $\lim_{n\to\infty} r_n$ exists and equals L if and only if r converges as a net and $r_n \xrightarrow{n} L$.

Suppose D is a nonempty subset of $\mathbb{R}$ and $c \in \mathbb{R}$. Make D into a directed set by $a \preccurlyeq b$ if and only if $|\,c-a\,| \ge |\,c-b\,|$. Now suppose that $D \subset A \subset \mathbb{R}$ and $f\colon A \to \mathbb{R}$. The function $f|_D$ is a net in $\mathbb{R}$ which might converge.

In case $c \notin D$ and if D contains a set of the form $\{\,x \in \mathbb{R} \mid x \ne c \text{ and } |\,x-c\,| < \xi\,\}$ for some $\xi > 0$ and provided $f|_D$ converges, a limit of this net is denoted

$$\boldsymbol{\lim_{x\to c} f(x).}$$

If there is any D satisfying the conditions above then the existence of this limit and its unique value do not depend on the particular D (satisfying the specified conditions) used in its definition, and therefore the directed set D will not usually be explicitly identified.

The various properties of $\mathbb{R}$, such as the total order on $\mathbb{R}$ and the existence of suprema and infima of bounded subsets of $\mathbb{R}$, have numerous consequences of importance here. The reader should recall, prove, look up or accept the following miscellaneous facts about the real numbers. The various topological concepts can be found in Appendix **??**.

5.1. ***Exercise.*** *(i) Suppose $f\colon (a,b) \to \mathbb{R}$ and $c \in (a_1, b_1) \subset (a,b)$. $\lim_{x\to c} f(x)$ exists and equals L if and only if $\lim_{n\to\infty} f(x_n)$ exists and equals L for every sequence $x\colon \mathbb{N} \to (a_1, c) \cup (c, b_1)$ with $\lim_{n\to\infty} x_n = c$.*

(ii) If $\lim_{x\to c} f(x)$ and $\lim_{x\to c} g(x)$ both exist and equal L and M respectively, then $\lim_{x\to c}(f(x) + g(x))$ and $\lim_{x\to c}(f(x)g(x))$ exist and $\lim_{x\to c}(f(x) + g(x)) = L + M$ and $\lim_{x\to c}(f(x)g(x)) = LM$. If $M \neq 0$ then $\lim_{x\to c}(1/g(x))$ exists and equals $1/M$.

(iii) Modify the definition of the directed set D in such a way that one-sided limits $\lim_{x\to c+} f(x)$ and $\lim_{x\to c-} f(x)$ are produced for appropriate functions f. Show that when properly restated the results of (i) and (ii) follow for your limits and that $\lim_{x\to c} f(x)$ exists exactly when both $\lim_{x\to c+} f(x)$ and $\lim_{x\to c-} f(x)$ exist and are equal.

5.2. ***Exercise.*** *(i) $f\colon (a,b) \to \mathbb{R}$ is continuous (with respect to the subspace topology on (a,b)) if and only if $\lim_{x\to c} f(x)$ exists and equals $f(c)$ for all $c \in (a,b)$.*

(ii) Constant functions are continuous, and the product and sum of continuous functions with common domain are continuous.

(iii) If $f\colon (a,b) \to (c,d)$ and $g\colon (c,d) \to \mathbb{R}$ are continuous then so is $g \circ f$.

(iv) The function $f\colon (0,\infty) \to (0,\infty)$ defined by $f(x) = x^2$ is one-to-one and onto $(0,\infty)$. Its inverse function is denoted $f^{-1}(x) = \sqrt{x}$. These functions are continuous and non-decreasing on their respective domains.

(v) The function $g\colon (0,\infty) \to (0,\infty)$ defined by $g(x) = 1/x$ is one-to-one and onto $(0,\infty)$. It is its own inverse function. It is continuous and non-increasing.

(vi) $A \subset \mathbb{R}$ is compact if and only if A is closed and bounded. This is the ***Heine-Borel Theorem****.*

(vii) Suppose $f\colon (a,b) \to \mathbb{R}$ is continuous and $[a_1, b_1] \subset (a,b)$. Let $B = \{\, f(x) \mid x \in [a_1, b_1] \,\}$. Suppose $\inf(B) \leq L \leq \sup(B)$. Then $\exists c \in [a_1, b_1]$ with $f(c) = L$. This is called the ***Intermediate Value Theorem****.*

(viii) Suppose $f\colon (a,b) \to \mathbb{R}$ is continuous. If K is a compact subset of (a,b) then $f(K)$ is compact. If J is a subinterval of (a,b) then $f(J)$ is an interval.

(ix) If $f\colon (a,b) \to (c,d)$ is one-to-one and onto and continuous then the inverse function $f^{-1}\colon (c,d) \to (a,b)$ is continuous.

(x) If $f\colon (a,b) \to \mathbb{R}$ is continuous, the values of f on $\mathbb{Q} \cap (a,b)$ determine the values of f on all of (a,b).

If a is a sequence of real numbers we define a new sequence S, called the **sequence of partial sums of a**, by $\boldsymbol{S_n = \sum_{k=0}^{n} a_k}$.

A sequence formed this way is called a **series**. Sometimes S converges. When it does its limit may be denoted $\boldsymbol{\sum_{k=0}^{\infty} a_k}$ and the **series is said to converge.**

If S_n does not converge it is said to **diverge**.

If $\sum_{k=0}^{\infty} |\, a_k \,|$ exists the series S is said to **converge absolutely**.

If the series converges but does **not** converge absolutely we say that the series converges **conditionally.**

When discussing the existence of the limit $\sum_{k=0}^{\infty} a_k$, we often say that the symbol $\sum_{k=0}^{\infty} a_k$ itself converges, diverges or converges absolutely or conditionally.

5.3. ***Exercise.*** *(i) If a series converges absolutely then it converges.*

(ii) Suppose $\sum_{k=0}^{\infty} a_k$ converges absolutely, and b is a real-valued sequence. Define for each $k \in \mathbb{N}$ the number $c_k = \sum_{i=0}^{k} a_{k-i} b_i$.

If $\sum_{k=0}^{\infty} b_k$ converges then so too does $\sum_{k=0}^{\infty} c_k$ and

$$\left(\sum_{k=0}^{\infty} a_k\right)\left(\sum_{k=0}^{\infty} b_k\right) = \sum_{k=0}^{\infty} c_k = \sum_{k=0}^{\infty}\left(\sum_{i=0}^{k} a_{k-i} b_i\right).$$

(iii) The series $E_n(x) = \sum_{k=0}^{n} \frac{x^k}{k!}$ converges absolutely for each real x. The limit is denoted e^x. The function $\mathbf{Exp}\colon \mathbb{R} \to (0,\infty)$ defined by $\mathbf{Exp}(\mathbf{x}) = e^x$ is one-to-one and onto $(0,\infty)$. Its inverse is denoted $\mathbf{Ln}$. For each real x and y, $e^{x+y} = e^x e^y$. Exp and Ln are continuous and non-decreasing on their respective domains.

(iv) The series $\sum_{k=0}^{n} x^k$ converges absolutely to $\frac{1}{1-x}$ for each $x \in (-1,1)$.

(v) The series $S_n(x) = \sum_{k=0}^{n} \frac{(-1)^k x^{2k+1}}{(2k+1)!}$ and $C_n(x) = \sum_{k=0}^{n} \frac{(-1)^k x^{2k}}{(2k)!}$ converge absolutely for each real x. Their limits are denoted $\mathbf{Sin}(\mathbf{x})$ and $\mathbf{Cos}(\mathbf{x})$, respectively, and the functions formed from these values are called the **Sine** *and* **Cosine** *functions. They are continuous.*

(vi) If a and b are real-valued sequences define $\Delta a_n = a_{n+1} - a_n$ and $\Delta b_n = b_{n+1} - b_n$ for each $n \in \mathbb{N}$. Then for $0 \le m < n$

$$\sum_{k=m}^{n} a_k\, \Delta b_k = a_{n+1} b_{n+1} - a_m b_m - \sum_{k=m}^{n} b_{k+1}\, \Delta a_k$$

which is called the ***summation by parts formula*** *for series. In case the sequence ab (defined by $(ab)_n = a_n b_n$) converges, the left sequence of partial sums converges exactly when the right sequence of partial sums does.*

(vii) Suppose a and c are real-valued sequences and we want to discover facts about the convergence of $S_n = \sum_{i=0}^{n} a_i c_i$. We define $b_k = \sum_{i=0}^{k} c_i$. Then $\Delta b_{n-1} = c_n$. The following equality of partial sums is called ***Abel's transformation*** *and is useful in several common applications.*

$$S_n = \sum_{k=0}^{n} a_k\, c_k = a_0\, c_0 + \sum_{k=1}^{n} a_k\, \Delta b_{k-1} = a_{n+1} b_n - \sum_{k=0}^{n} b_k\, \Delta a_k.$$

(viii) If the sequence a/b (defined by $(a/b)_n = a_n/b_n$) converges to a nonzero constant L then the series $\sum_{k=0}^{\infty} a_k$ converges exactly when $\sum_{k=0}^{\infty} b_k$ converges.

(ix) Suppose a is a sequence of non-zero numbers. Then $\lim_{n\to\infty} |a_{n+1}| \,/\, |a_n|$ exists exactly when $\lim_{n\to\infty} |a_n|^{1/n}$ exists. In case this common limit exists define

R to be the reciprocal of the limit (if the limit is 0 let $R = \infty$.) For real x the series $\sum_{k=0}^{\infty} a_k x^k$ is called a ***power series*** *and R is called the* ***radius of convergence*** *of the series. This power series converges whenever $|x| < R$.*

(x) Suppose a is a sequence of non-zero numbers and $L = \lim_{n\to\infty} |a_n|^{1/n}$. If $L = 0$ the power series $\sum_{k=0}^{\infty} a_k x^k$ converges absolutely for all x. If $L = \infty$ (that is, if $\lim_{n\to\infty} |1/a_n|^{1/n} = 0$) the power series converges only for $x = 0$. Otherwise, let $R = 1/L$. The power series converges absolutely if $|x| < R$ and diverges if $|x| > R$. This result is called the ***Cauchy-Hadamard Theorem.***

Finally, we get to the issue of specific common representations of real numbers.

If p is an integer bigger than 1, we can represent any real number between 0 and 1 as $\sum_{k=1}^{\infty} \frac{a_k}{p^k}$ where the sequence a consists of integers with $0 \le a_n < p$ for all n.

This representation is not quite unique as stated.

Sequences a that terminate, for some n, with $a_n \neq 0$ and $a_k = 0$ for all $k > n$ and exactly one sequence b with $b_k = p - 1$ for all $k > n$ generate series for the same real number.

However this is the only duplication in the representation, so uniqueness is acquired by forbidding all representations that use sequences b that terminate in $b_k = p - 1$ for all $k > n$ for some n.

With this convention, any real number can be represented uniquely (for each p and some $k \ge 0$) as

$$\pm \left(\sum_{n=0}^{k} \boldsymbol{a_{-n} p^n} + \sum_{n=1}^{\infty} \frac{\boldsymbol{a_n}}{\boldsymbol{p^n}} \right) \qquad \text{where}$$

(*i*) $0 \le a_j < p$ for all $j \ge -k$ and

(*ii*) $a_{-k} \neq 0$ unless $k = 0$ and

(*iii*) the sequence does not terminate with $a_j = p - 1$ for all $j > m$ for any m.

The case of $p = 10$ corresponds to the ordinary **decimal representation** of numbers, while $p = 2$ and $p = 3$ generate the **binary or dyadic and ternary representations**.

We will take one further step in the progression $\varnothing \to 1 \to \mathbb{N} \to \mathbb{Q} \to \mathbb{R}$.

The **complex numbers**, denoted $\mathbb{C}$, consist of the set of all ordered pairs of real numbers with operations of addition and multiplication given by

$$(a, b) + (c, d) = (a + c, b + d) \quad \text{and} \quad (a, b) * (c, d) = (ac - bd, ad + bc).$$

An alternative way of representing an ordered pair of real numbers (a, b) thought of as a complex number is using the symbol $\boldsymbol{a + bi}$.

If $z = a + bi$ is a complex number, a is called its **real part**, and b is called its **imaginary part**. This is purely a notational device: we are associating real number a with ordered pair $(a, 0)$ and bi with $(0, b)$.

$\boldsymbol{\overline{z} = a - bi}$ is called the **conjugate of z**. The **magnitude of z** is $\sqrt{a^2 + b^2}$ and denoted $|\mathbf{z}|$. Note that if $z \neq (0, 0)$ then $(1, 0) = z \left(\frac{\overline{z}}{|z|^2} \right)$.

The map that associates x in $\mathbb{R}$ with $(x, 0)$ in $\mathbb{C}$ preserves the arithmetic operations on $\mathbb{R}$ and sends the multiplicative identity there to the multiplicative identity in $\mathbb{C}$, so the range of this map can (and will) be identified with $\mathbb{R}$.

5.4. ***Exercise.*** *A sequence of complex numbers $z_n = a_n + b_n i$ converges to complex number $w = x + yi$ exactly when both $\lim_{n\to\infty} a_n = x$ and $\lim_{n\to\infty} b_n = y$. This happens exactly when the real sequence $|\, w - z_n \,|$ converges to 0. Adapt Exercise 5.1 wherever necessary to handle series of complex numbers. Then define the series $E_n(z) = \sum_{k=0}^{n} \frac{z^k}{k!}$ and show it converges absolutely for every complex z and define e^z to be the limit. If w and z are complex show that $e^{z+w} = e^z e^w$ and if $z = a+bi$ then*

$$e^z = e^a e^{bi} = e^a \left(Cos(b) + i\, Sin(b) \right).$$

Delete the negative x axis and the origin from the complex plane and define an inverse to a piece of the exponential function there. Call this inverse a logarithm. If you want this logarithm to be continuous, what choices do you have? Could you delete another half-line terminating at the origin and define another logarithm with this domain?

6. An Axiomatic Characterization of $\mathbb{R}$

Let A be any field. A may contain "a copy" $\mathbb{N}_A$ of $\mathbb{N}$. By this we mean that $\mathbb{N}_A$ is subring of A containing the identity of A and which is ring isomorphic to $\mathbb{N}$. Then since A is a field it must also contain "a copy" $\mathbb{Q}_A$ of $\mathbb{Q}$ which contains $\mathbb{N}_A$ as a subring. A is said to **have characteristic 0** when it contains a copy of $\mathbb{N}$.

Generally the additive and multiplicative identities in *any* field are denoted by 0 and 1, respectively. This could, but rarely does, lead to confusion.

If any field A is equipped with a linear order $<$ satisfying

- (i) $\quad x + y > 0$ whenever $\;x, y > 0$
- (ii) $\quad xy > 0$ whenever $\;x, y > 0$
- (iii) $\quad x + z > y + z$ whenever $\;x > y$

we call A an **ordered field**. Both $\mathbb{Q}$ and $\mathbb{R}$ are ordered fields.

If both x and $-x$ were positive (i.e. greater than 0) we would have by (i) that $0 > 0$, contradicting the assumption that our order is a linear order. So if $x \neq 0$ at most one of x or $-x$ is positive.

If $-1 > 0$ then (ii) implies $(-1)(-1) = 1 > 0$, contradicting (i). So $-1 < 0$. Using this in (iii) yields $0 + 1 > -1 + 1$ so $1 > 0$.

Define $\tilde{0} = 0$ and, having defined $\tilde{n}$ for integer n define $\widetilde{n+1} = \tilde{n} + 1$. This recursive definition gives a function from $\mathbb{N}$ to A. Repeated application of (iii) yields $\tilde{n} + 1 > \tilde{n} > 0$ for all positive integers n. In particular, we can never have $\tilde{n} = 0$. So the ordered field properties **imply** that the underlying field has characteristic 0: we do not, actually, need to assume it. There are unique copies $\mathbb{N}_A$ of $\mathbb{N}$ and $\mathbb{Q}_A$ of $\mathbb{Q}$ inside every ordered field.

An ordered field has the quality of **Dedekind completeness** or **DKC** provided that each subset which is bounded above has a least upper bound.

The real numbers as we have built them constitute a Dedekind complete ordered field. Every property of the real numbers used in analysis follows from just a few properties: those which define a field, the properties defining a linear order, (i), (ii), (iii) and DKC.

An ordered field has the **Archimedean order property** or **AOP** if, for each $x, y \in A$ with $0 < x < y$ there is an $n \in \mathbb{N}_A$ so that $y < nx$.

These properties have consequences, a few of which are explored below.

6.1. ***Exercise.*** *We will presume that A is an ordered field as above.*

(i) $x > 0$ exactly when $-x < 0$. *(ii) $x < y$ exactly when $0 < y - x$.*

(iii) $0 < x$ and $0 < y < z$ implies $0 < xy < xz$.

(iv) $x < 0$ and $y < 0$ implies $xy > 0$. *(v) $x < 0$ and $y > 0$ implies $xy < 0$.*

(vi) $x > 0$ exactly when $\frac{1}{x} > 0$. *(vii) $0 < x < y$ exactly when $0 < \frac{1}{y} < \frac{1}{x}$.*

6.2. ***Exercise.*** *Suppose A is an ordered field as above.*

Define $|0| = 0$. If x is nonzero in A, either $x > 0$ or $-x > 0$ but not both. Define $|x|$ to be x or $-x$, chosen so that $|x| > 0$.

(i) For each $x, y \in A$, show that $|\, xy \,| = |x||y|$.

(ii) For each $x, y \in A$, show that $|\, x + y \,| \leq |x| + |y|$.

6.3. ***Exercise.*** *Suppose A is an ordered field as above.*

(i) AOP is equivalent to each of the following three conditions:
For each $x > 0$ there is an $n \in \mathbb{N}_A$ so that $\frac{1}{n} < x$.
For each $x > 0$ there is an $n \in \mathbb{N}_A$ so that $x < n$.
For each $x > 0$ there is a unique $n \in \mathbb{N}_A$ for which $n < x \leq n + 1$.

(ii) DKC implies AOP. (hint: If A does not have AOP then there is a y with $0 < 1 < y$ but $y \geq m$ for all $m \in \mathbb{N}_A$. So $\mathbb{N}_A$ is bounded above. If A had DKC there would be a least upper bound $p \in A$ for $\mathbb{N}_A$. Show that $p - 1$ must also be an upper bound for $\mathbb{N}_A$, a contradiction. So A cannot have DKC.)

(iii) DKC implies that sets in A which are bounded below have infima.

(iv) $\mathbb{Q}$ has AOP but not DKC so AOP does not imply DKC.

6.4. ***Exercise.*** *Suppose A is an ordered field as above with AOP.*

(i) If B is a subset of A for which $s = \sup B$ exists then for each integer $n > 0$ there is a member $t \in B$ with $s - t < \frac{1}{n}$.

(ii) If $r \in A$ then $r = \sup\{\, t \in \mathbb{Q}_A \mid t \leq r \,\}$.

6.5. ***Exercise.*** *If A is a Dedekind complete ordered field then there is a ring isomorphism between A and $\mathbb{R}$. This ring isomorphism is unique, and is an order-isomorphism.*

We have a collection of properties, axioms if you will, satisfied by the real numbers. These axioms are (some of) the axioms of ordinary set theory plus those axioms associated with a Dedekind complete ordered field. The real numbers as we have created them constitute a realization or **model** of the axioms of a Dedekind complete ordered field "inside" ordinary set theory. We have shown by our construction that these axioms are consistent (if the axioms of set theory are consistent) and that was an important finding.

However neither the "Dedekind cut" construction of the real numbers nor the "Cauchy sequence" construction correspond in a compelling way to our simple intuition about real numbers as, for example, "points on a line."

In fact, all properties of the real numbers important to analysts **follow from the axioms mentioned above, not from the details of construction employed in forming our particular realization.**

It is these axioms which capture some of our intuition about real numbers, not any particular construction. The last exercise guarantees that if someone produces a different realization of these axioms, their underlying object shares all essential features with ours. We are free, when that is convenient, to remember the axioms and forget as irrelevant their particular embodiment.

Finally, it is worth noting that the usual identification of the real numbers with **all** the points on a line is not set in stone. It is not implied by the ancient concept of a line, nor by the standard practices of the inventors of calculus who routinely employed "infinitesimals," since replaced by limits.

Practitioners of **nonstandard analysis** use a larger ordered field called the **hyperreal numbers** ${}^*\mathbb{R}$ in place of $\mathbb{R}$. The hyperreal numbers contain positive numbers smaller than any real number, and limit-taking is replaced by hyperreal arithmetic.

The main technical challenges involved in transferring nonstandard results to the standard world were overcome by Abraham Robinson, the creator of this subject, in 1960.

Though conceptually attractive, it is currently unclear if this approach offers net advantages over standard analytic technique.

7. $[-\infty, \infty]^X$ AND $\mathbb{R}^X$

$[-\infty, \infty]$ is called the set of **extended real numbers** and defined to be $\mathbb{R} \cup \{-\infty, \infty\}$, where members of $\mathbb{R}$ have their usual properties and ∞ and $-\infty$ are distinct, not real numbers and have the order, addition and multiplication properties that would seem reasonable for "infinitely large" entities.

For example, $-\infty \leq a \leq \infty \; \forall a \in [-\infty, \infty]$. If $a > 0$ we define $a \cdot \infty = \infty$ $a \cdot (-\infty) = -\infty$ and $a + \infty = \infty$ and $(-a) \cdot \infty = -\infty$ and $(-a) + (-\infty) = -\infty$. We also define $-\infty \cdot 0 = \infty \cdot 0 = 0$. However $-\infty + \infty$ is not defined. The symbols $\pm\infty$ have no multiplicative inverses.

Every set in $[-\infty, \infty]$ is bounded above and below by ∞ and $-\infty$ respectively. We abuse vocabulary and declare a subset of $[-\infty, \infty]$ to be **bounded above or**

below if it is bounded by a real number in the specified sense. With this usage, the bounded sets in $[-\infty,\infty]$ and $\mathbb{R}$ are the same.

$[-\infty,\infty]$ is a compact topological space, where neighborhoods of a point in $\mathbb{R}$ are sets containing an open interval around that point, neighborhoods of $-\infty$ are those sets containing an interval of the form $[-\infty,a)$, and neighborhoods of ∞ are those sets containing an interval of the form $(a,\infty]$.

Suppose J is a directed set, such as $\mathbb{N}$. Recall that for each $j\in J$ the symbol T_j denotes the terminal segment of J consisting of those members n of J for which $n\geq j$.

If $r\colon J\to[-\infty,\infty]$ is a net, each $r\,(T_j)$ is a set of extended real numbers, and any such has both supremum and infimum in $[-\infty,\infty]$. So, for example, both $u(j)=\sup r\,(T_j)$ and $l(j)=\inf r\,(T_j)$ are defined for each $j\in J$ and so form extended real-valued nets l and u defined on J. u and l are are monotone: u is non-increasing while l is non-decreasing.

The reader should investigate the modifications to the definition of limits of real-valued sequences needed to make sense out of notation such as

$$\boldsymbol{\limsup(r)=L}\quad\text{or}\quad\boldsymbol{\liminf(r)=L}\quad\text{or}\quad\boldsymbol{r_\alpha\xrightarrow{\alpha}L}$$

when L is an extended real number and r is a net in $[-\infty,\infty]$. The relationship between these limits and the previously defined limits for real-valued nets (when the former limits existed) must be examined.

For sets X and Y, recall that Y^X is the set of functions from X to Y. When Y has a partial order there is a partial order induced on Y^X given by

$$f\leq g\Leftrightarrow f(a)\leq g(a)\ \forall a\in X.$$

This is called the **pointwise order** on Y^X.

Infima and suprema of indexed sets of functions, such as $\{\,f_\alpha\mid\alpha\in J\,\}\subset Y^X$, are themselves members of Y^X whose values on each $x\in X$ are indicated by:

$$\left(\bigvee_{\alpha\in J}f_\alpha\right)(x)=\bigvee_{\alpha\in J}f_\alpha(x)\quad\text{and}\quad\left(\bigwedge_{\alpha\in J}f_\alpha\right)(x)=\bigwedge_{\alpha\in J}f_\alpha(x)$$

provided, of course, that the "pointwise" infima and suprema exist in Y for every $x\in X$.

These definitions depend on the existence of limits in Y.

If $Y\subset W$, an infimum or supremum might exist in W^X but not in Y^X.

There is a notational issue that should be observed here. If $f_\alpha\in Y^X$, we already have a definition for the infimum and supremum of a function f_α, namely:

$$\bigvee_{x\in X}f_\alpha(x)=\sup\{\,f_\alpha(x)\mid x\in X\,\}\quad\text{and}\quad\bigwedge_{x\in X}f_\alpha(x)=\inf\{\,f_\alpha(x)\mid x\in X\,\}$$

Confusion can arise when there are functions with multiple arguments or if multiple infima and suprema are being calculated if care is not taken in specifying order and arguments. Consider, for example:

$$\bigvee_{\alpha\in J}\left(\bigwedge_{x\in X}f_\alpha(x)\right)\quad\text{and}\quad\bigwedge_{x\in X}\left(\bigvee_{\alpha\in J}f_\alpha\right)(x).$$

There is no reason to think these two limits will be equal.

Note that Y is a lattice $\Leftrightarrow$ Y^X is a lattice.

More generally, infima and suprema always exist in Y^X precisely when such always exist in Y. These always exist if $Y = [-\infty, \infty]$ but not if $Y = \mathbb{R}$.

Suppose $f\colon J \to [-\infty, \infty]^X$, where J is a directed set.

We say f **converges pointwise** to a function $\widehat{f}$ provided

$$f_\alpha(b) \xrightarrow{\alpha} \widehat{f}(b) \ \forall b \in X.$$

To describe this situation and to assert the existence of such a limit we will write

$$\boldsymbol{f_\alpha \xrightarrow{\alpha} \widehat{f}} \quad \text{or, when } J = \mathbb{N}, \text{ we may write} \quad \boldsymbol{\lim_{n\to\infty} f_n = \widehat{f}.}$$

For f and g in $[-\infty, \infty]^X$, we define $\boldsymbol{f \cdot g}$ by $(f \cdot g)(a) = f(a)g(a)$ and $\boldsymbol{f + g}$ by $(f + g)(a) = f(a) + g(a)\ \forall a \in X$.

These are called **pointwise multiplication and addition**.

The multiplication and addition defined above are commutative, and the functions that are constantly one and zero are the multiplicative and additive identities, respectively. $[-\infty, \infty]^X$ is not a real vector space, but only because addition is not defined for all pairs of functions.

For any set X define $\boldsymbol{\chi\colon \mathbb{P}(X) \to 2^X}$ by $\boldsymbol{\chi_A(a)} = \begin{cases} 0 & \text{if } a \notin A; \\ 1 & \text{if } a \in A. \end{cases}$

The map χ is an order-isomorphism.

Each χ_A is called a **step** or **characteristic function** and finite real linear combinations of these are called **simple functions**.

Note that $\chi_A \vee \chi_B = \chi_{A\cup B},\ \chi_A \wedge \chi_B = \chi_{A\cap B} = \chi_A \cdot \chi_B,\ \chi_{A-B} = \chi_A - \chi_{A\cap B}$ and $|\,\chi_A - \chi_B\,| = \chi_{(A-B)\cup(B-A)} = \chi_{A-B} + \chi_{B-A} = \chi_A + \chi_B - 2\chi_{A\cap B}$.

When $\mathbb{G} \subset \mathbb{P}(X)$, we will use $\boldsymbol{\mathcal{S}}(\mathbb{G})$ to denote the set of simple functions constructed from the sets in $\mathbb{G}$.

A function that has constant range value t on its whole domain will sometimes be denoted t, with this usage (and the domain) taken from context. Thus, for example, χ_X is sometimes denoted by 1 and $0\chi_X$ by 0, in yet another use of each of those symbols.

When $\mathbf{H}$ is a subset of $[-\infty, \infty]^X$, we will use $\boldsymbol{\mathcal{B}}(\mathbf{H})$ to denote the bounded members of $\mathbf{H}$; $f \in \boldsymbol{\mathcal{B}}(\mathbf{H}) \Leftrightarrow f \in \mathbf{H}$ and $\exists a \in \mathbb{R}$ with $0 \le a < \infty$ and $-a \le f \le a$.

If X is a topological space, $\boldsymbol{\mathcal{C}}(X)$ denotes the continuous functions from X to $\mathbb{R}$.

$\mathbb{R}^X$, $\boldsymbol{\mathcal{B}}(\mathbb{R}^X)$ and, when X has a topology, $\boldsymbol{\mathcal{C}}(X)$, are all **vector lattices**: real vector spaces and lattices.[3] They are also **commutative rings with multiplicative identity** χ_X.

7.1. ***Exercise.*** $\boldsymbol{\mathcal{S}}(\mathbb{G})$ *is obviously a (possibly empty) vector space. Give conditions on* $\mathbb{G}$ *under which* $\boldsymbol{\mathcal{S}}(\mathbb{G})$ *is a vector lattice and a commutative ring with multiplicative identity* χ_X.

[3] A vector lattice is called, generally, a **Riesz space**. Real function vector lattices are examples.

8. The Axiom of Choice

In this section we introduce another axiom of set theory, the Axiom of Choice.

Every human language has grammar and vocabulary, and people communicate by arranging the objects of the language in patterns. We imagine that our communications evoke similar, or at least related, mental states in others. We also use these patterns to elicit mental states in our "future selves," as reminder of past imaginings so that we can start at a higher level in an ongoing project and not have to recreate each concept from scratch should we return to a task. It is apparent that our brains are built to do this.

But words are all defined in terms of each other. Ultimate meaning, if there is any to be found, is derived from pointing out the window at instances in the world, or from introspection. Very often ambiguity or multiple meaning of a phrase is the point of a given communication, and provides the richness and subtlety characteristic of poetry, for instance, or the beguiling power of political speech.

Set Theory is a language mathematicians have invented to encode mathematics. But unlike most human languages, this language does everything possible to avoid blended meaning, to expose the logical structure of statements and keep the vocabulary of undefined terms to an absolute minimum. Many mathematicians believe what they do is "art." But ambiguity and internal discord is not part of our particular esthetic ensemble.

Most mathematicians believe that, though set theory may be unfinished, it serves its purpose well. Virtually all mathematical structures can be successfully modeled in set theory, to the extent that most mathematicians never think of any other way of speaking or writing.

Together, the collection of axioms (which, along with logical conventions defines the language) normally used by most mathematicians is called the **Zermelo-Fraenkel Axioms**, or simply **ZF** and the set theory that arises from these axioms is called **Zermelo-Fraenkel Set Theory**. You saw explicit mention of two axioms from ZF, the Axiom of Infinity and the Axiom of the Empty Set, in Section 5. We have used others without mention on almost every page. For example we have formed power sets.

> **The Axiom of the Power Set** For any set A there is a set $\mathbb{P}(A)$ consisting of all, and only, the subsets of A.

Asserting the existence of a set with this feature is a dramatic and "non-constructive" thing to do, *particularly* when the underlying set is infinite. We are not told how to create this set. We just have a means of recognizing if a set we have in hand is a member of this power set, or not.

And where, exactly, did that first infinite set come from? The Axiom of Infinity brings it into existence, out of nothing, simply because mathematicians *want infinite sets* and this seems to be a consistent way to produce them.

There is another extremely useful—and arguably even less constructive—axiom which we discuss now.

We will present and presume to be true, wherever convenient, the four equivalent and useful statements below, one of which is called the Axiom of Choice. This axiom is frequently abbreviated to **AC**. The collection of the axioms of standard set theory plus this axiom is frequently denoted **ZFC**.

The discussions regarding equivalence of the Axiom of Choice and the other three statements, and the history associated with them, is a fascinating story which deserves study by every serious student of mathematics.

> **The Axiom of Choice**: If J and X are sets and $A\colon J \to \mathbb{P}(X)$ is an indexed collection of nonempty sets then there is a function $f\colon J \to X$ such that $f(\beta) \in A_\beta \ \forall \beta \in J$. A function with this property is called a **choice function** for A.

Essentially, this axiom states that given any generic set $\mathbb{S}$ of nonempty sets, there is a way of selecting one element from each member of $\mathbb{S}$. The other axioms do not imply that such a selection can be made, unless every member of $\mathbb{S}$ has an element with some unique property, which would allow it to be singled out.

> **Zorn's Lemma**: If S is a set with a partial order and if every chain in S possesses an upper bound in S, then S has a maximal member.
>
> **Zermelo's Theorem**: Every nonempty set can be well-ordered.
>
> **Kuratowski's Lemma**: Each chain in a partially ordered set S is contained in a **maximal chain** in S (that is, a chain in S not contained in any other chain in S.)

Kuratowski's Lemma is also often called **The Hausdorff Maximal Principle.**

That Zorn's Lemma implies Kuratowski's Lemma is immediate. Suppose S is a set with a partial order and and C is a chain in S. Let $\mathbb{W}$ denote the set of all chains in S which contain the chain C, ordered by containment. Any chain in $\mathbb{W}$ is bounded above by the union of the chain, so Zorn's Lemma implies that $\mathbb{W}$ contains a maximal member. That maximal member is a chain in S not properly contained in any other chain in S.

On the other hand, assuming Kuratowski's Lemma to be true, suppose S is a set with a partial order and that every chain in S possesses an upper bound in S. This time let $\mathbb{W}$ denote the set of *all* chains in S. Let X denote a maximal member of $\mathbb{W}$. So X is a chain in S not contained in any other chain. Let M be any upper bound for X. By maximality of X, M must actually be in X and cannot be less than any other member of S: that is, M is maximal in S. So Zorn's Lemma is true.

In the last two paragraphs we have shown that Zorn's Lemma and Kuratowski's Lemma are equivalent statements.

We will now show that Zorn's Lemma implies AC. Suppose $\mathbb{S}$ is any nonempty set of nonempty sets and X is the union of all the sets in $\mathbb{S}$. Let $B = \mathbb{S} \times X$. Now let Q denote the set of all subsets of $\mathbb{P}(B)$ which are choice functions on their domains: that is, $T \in Q$ exactly when T is nonempty and there is at most one ordered pair in T whose first component is any particular member of $\mathbb{S}$, and also $s \in A$ whenever $(A, s) \in T$. These are called "**partial choice functions**." Order Q by containment. The union of any chain in Q is a member of Q so Zorn's Lemma

implies that Q has a maximal member. This maximal member is a choice function on its domain, which must by maximality be all of $\mathbb{S}$.

The fact that Zermelo's Theorem implies AC is also straightforward: given any nonempty set $\mathbb{S}$ of nonempty sets, well-order the set $X = \bigcup_{S\in\mathbb{S}} S$. For each $S \in \mathbb{S}$ let $f(S)$ be the least element of S with respect to this ordering. f is the requisite choice function.

The opposite implication is a bit trickier. It involves using a choice function to create the well-order.

Suppose set A has more than one element and $f\colon \mathbb{P}(A) - \{\varnothing\} \to A$ is a choice function: that is, $f(B) \in B$ whenever $\varnothing \neq B \subset A$.

Let $\mathbb{B}$ denote the set of all nonempty containment-chains in $\mathbb{P}(A) - \{\varnothing\}$ which are well-ordered and satisfy the condition:

> Whenever I_K is an initial segment of one of these chains and if J is the union of all the sets in I_K then $J \neq A$ and $K = J \cup \{f(A - J)\}$.

$\mathbb{B}$ is nonempty: for example, $\{\,\{f(A)\}, \{\,f(A), f(A - \{f(A)\})\,\}\,\}$ is in $\mathbb{B}$.

The condition above implies that each of the chains in $\mathbb{B}$ must start with the set $\{f(A)\}$, and the successor to any set K in such a chain (if, of course, K is not the last set in the chain) has exactly one more member than does K. It also implies directly that if two different chains X and W of this kind have a common initial segment, so that $I_K \subset X$ and $I_G \subset W$ and $I_K = I_G$ then $K = G$. In other words, the least successor of an initial segment is determined by the sets in the initial segment, and *not* by the specific chain within which the initial segment sits.

Suppose that X is one of these chains. We will call S a "starting chunk" of X if $\varnothing \neq S \subset X$ and whenever $B, C \in X$ the condition $B \in S$ and $C \subset B$ implies $C \in S$. Now it might be that a starting chunk is as short as $\{f(A)\}$ or it could, possibly, be all of X. But if it is *not* all of X then because X is well-ordered there is a least member K of X not in S and so S contains all members of X less than K. That is, $S = I_K$ for some $K \in X$. So starting chunks are either initial segments or the entire chain.

Now suppose X and W are unequal chains, members of $\mathbb{B}$. Then one, say X, would contain a least set K not in the other. The initial segment I_K of X is contained in W. If there were a set in W not in I_K but less than some member of I_K then there would be a least member of W of this kind. Call that least member G. But then the initial segment I_G of W would be a starting chunk of X and by the above remark we would have $G \in X$, contrary to its definition.

So there are no missing members of W between members of I_K, which is therefore a starting chunk of W. Since $K \notin W$ we must have $I_K = W$, and conclude that W is an initial segment of X.

To reiterate: for each pair of members of $\mathbb{B}$, one is an initial segment of the other.

Now let S be the union of all the members of $\mathbb{B}$. Each set in S comes from a member of $\mathbb{B}$ and since one of any pair of members of $\mathbb{B}$ is an initial segment of the other we conclude that S itself is a chain, and well-ordered too.

Let J denote the union of all the sets in S. If $J \neq A$ then we could extend S to $S \cup \{J \cup \{f(A-J)\}\}$ which satisfies the conditions for membership in $\mathbb{B}$ but is strictly longer than its longest member, a contradiction. We conclude that $J = A$.

So we can use S to create an order on A. If a and b are members of A there is a least member S_a of S containing a and a least member S_b containing b. Declare $a \leq b$ precisely when $S_a \subset S_b$. If J is the union of the sets in the initial segment determined by S_a then $a \notin J$ so it must be that $a = f(A-J)$. So this relation makes A into a total order. Further, if $\varnothing \neq T \subset A$ then the collection of all of the S_t with $t \in T$ has a least member, which produces a least member of T. So the order on A is a well-order.

We conclude that the existence of a choice function on $\mathbb{P}(A) - \{\varnothing\}$ implies that A can be well-ordered. So AC implies Zermelo's Theorem.

Upon accepting the Axiom of Choice, as we will do throughout this book, well-ordered sets are plentiful and can be used.

At this point we have shown the following implications among the conditions which we claim to be equivalent to the Axiom of Choice.

$$\begin{array}{ccc} \text{Zorn} & \Longleftrightarrow & \text{Kuratowski} \\ \Downarrow & & \\ \text{AC} & \Longleftrightarrow & \text{Zermelo} \end{array}$$

The **Principles of Induction** and **Recursive Definition** are incredibly powerful and useful techniques, extending the idea of Induction on the Integers to many more well-ordered sets and situations more varied than merely checking if an indexed set of propositions are all true. The methods are detailed in Section **??**. It is important to note, and the reader should check, that the proof of the version of Recursive Definition we use here does *not* require AC.

We will now use Induction and Recursive Definition to show that Zermelo's Theorem implies Kurotowski's Lemma, thereby proving that any of the four conditions listed above implies the others. The discussion below is a typical usage of this type of argument. It uses first a recursive definition to deduce that a certain function exists, and then induction to confirm various properties of that function.

We suppose we have a chain in a partially ordered set. We will line up the members of the set not already in the chain and test them one at a time. When it is an element's turn, if it can be added to yield a bigger chain than we have up to that point we select it. Otherwise we discard it. Then we go on to the next element and repeat until we have exhausted the possibilities. The product is a maximal chain. A rigorous justification can be produced after digesting the result in **??**

Assume Zermelo's Theorem to be true, and suppose H is a nonempty chain in set K with partial order $\precsim$. Suppose $B = K - H$ is nonempty. There is a well-order $\leq$ for B. Since we have two orders in hand, we will use prefixes to describe which order is in use. We will let I_β stand for a $\leq$-initial segment for any $\beta \in B$.

Suppose y is a fixed element of H. For the $\leq$-first element α of B, let $P(\alpha)$ equal α if $H \cup \{\,\alpha\,\}$ is a $\precsim$-chain, and let $P(\alpha)$ be y otherwise.

Having found $P(\beta)$ for all $\beta \in B$ with $\alpha \leq \beta < \gamma$ for some $\gamma \in B$ define $P(\gamma)$ to be γ if $H \cup \{\gamma\} \cup P(I_\gamma)$ is a $\precsim$-chain, and let $P(\gamma)$ be y otherwise.

This serves to define $P(\gamma)$ for each $\gamma \in B$.

$H \cup P(B)$ must be a $\precsim$-chain: if not it must contain two $\precsim$-incomparable members s and t, which cannot both be in H. If one of the two, say s, is in H then there is a $\beta \in B$ with $P(\beta) = t = \beta$. But then $H \cup \{\beta\} \cup P(I_\beta)$ is not a chain, violating the defining condition for $P(\beta)$. A similar contradiction occurs if neither s nor t are in H, by examining the point at which the *second* of the two points would have been added. So in fact $H \cup P(B)$ must be a $\precsim$-chain.

No additional members of K can be added to $H \cup P(B)$ without causing the resulting set to fail to be a $\precsim$-chain: once again, letting γ be the $\leq$-least member of B which *could* be added, if any, yields a contradiction. That member *would* have been added at stage γ.

So $A \cup P(B)$ is a maximal $\precsim$-chain in K, and Kuratowski's Theorem holds.

8.1. ***Exercise.*** *Fill in the details of a direct proof using Induction and Recursive Definition that Zermelo's Theorem implies Zorn's Lemma. We assume that K is a set with partial order $\precsim$ for which every chain has an upper bound. We assume also that K has a well-order $\leq$ with $\leq$-first member α.*

We would like to conclude that K has a $\precsim$-maximal element.

Let α denote the $\leq$-first member of K and define $G(\alpha) = \alpha$. Having defined G on $\leq$-initial segment I_β for $\beta > \alpha$ let $G(\beta) = \beta$ if β is a $\precsim$-upper bound for $G(I_\beta)$, and otherwise let $G(\beta) = \alpha$.

Show that $G(K)$ is a chain and that $G(K)$ has a $\precsim$-last member, which is $\precsim$-maximal in K.

8.2. ***Exercise.*** *(i) An axiom equivalent to our Axiom of Choice is produced if we add to that axiom the condition that $A_\alpha \cap A_\beta = \varnothing$ whenever $\alpha \neq \beta$.*

(ii) Consider the statement: "Whenever $\mathbb{B}$ is a nonempty set of nonempty pairwise disjoint sets, there is a set S for which $S \cap x$ contains a single element for each $x \in \mathbb{B}$." Show that this statement is equivalent to the Axiom of Choice.

*(iii) Let $\mathbb{B}$ be a (nonempty) set of sets. $\mathbb{B}$ is said to have **finite character** provided that $A \in \mathbb{B}$ if and only if every finite subset of A is in $\mathbb{B}$. **Tukey's Lemma** states that every set of sets of finite character has a maximal member: a set not contained in any other member. Show that Tukey's Lemma is equivalent to the Axiom of Choice. (hint: To prove that Tukey's Lemma implies the Axiom of Choice examine the set of partial choice functions and note that it satisfies the conditions of Tukey's Lemma.)*

The use of AC in the formation of mathematical arguments has historically been the subject of controversy centered around the nebulous nature of the objects whose existence is being asserted in each case. In applications the axioms of set theory are usually used to affirm the existence of one precisely defined set whose elements share an explicit property. That is less obviously the case when AC is invoked.

Applications which require less than the full strength of AC are common. In an effort to control, or at least record, how the axiom is being used, weaker variants have been created. Some mathematicians award "style points" to proofs using one of these, or which avoid AC altogether. We list two of these weaker versions of AC below.

> **The Axiom of Dependent Choice**: If X is a nonempty set and $R \subset X \times X$ is a binary relation with domain all of X, then there is a sequence $r\colon \mathbb{N} \to X$ for which $(r_k, r_{k+1}) \in R\ \forall k \in \mathbb{N}$.
>
> **The Axiom of Countable Choice**: If X is a nonempty set and $r\colon \mathbb{N} \to \mathbb{P}(X)$ is a sequence of nonempty subsets of X then there is a sequence $f\colon \mathbb{N} \to X$ such that $f(n) \in A_n\ \forall n \in \mathbb{N}$.

These axioms are frequently abbreviated to **DC** and $\mathbf{AC}_\omega$, respectively.

8.3. ***Exercise.*** *(i) Prove the implications $AC \Rightarrow DC \Rightarrow AC_\omega$.*

(ii) Suppose X is infinite. For each $k \in \mathbb{N}$ let S_k denote the set of all subsets of X which have 2^k elements. ZF alone implies that S_k is nonempty for each k, and you may assume this. Let S denote the set of all the S_k. Use AC_ω twice to prove that there is a one-to-one function $f\colon Y \to \mathbb{N}$ for an infinite subset Y of X. Any set Y (infinite or not) for which there is a one-to-one function $f\colon Y \to \mathbb{N}$ is called ***countable****, and the result here may be paraphrased as "Any infinite set has an infinite countable subset in ZF+AC_ω."*

(iii) Sometimes the use of an axiom, particularly a variant of the Axiom of Choice, is hard to spot in an argument. It seems so reasonable, it is hard to see you are assuming anything. The theorem that "The union of a countable set of countable sets is countable." is an example.

Suppose A is a countable set of countable sets, and let B denote the union of all the members of A. Because A is countable, there exists one-to-one $T\colon A \to \mathbb{N}$. Because each member of A is countable, for each nonempty set $S \in A$ there is a nonempty set F_S consisting of all one-to-one functions from S to $\mathbb{N}$. Using T, this collection of sets of functions is seen to be countable, so AC_ω guarantees that we can pick a function from each. It is easy to overlook this step, and merely assert "Because each member of A is countable there exists one-to-one $G_S\colon S \to \mathbb{N}$ for each $S \in A$." and get on with the discussion using these selected functions. But it is AC_ω which endorses this selection.

To finish the argument, for each $x \in B$ we let $A_x = \{\, S \in A \mid x \in S \,\}$ and define i_x to be the least integer in $T(A_x)$. We define W_x to be that member of A_x with $T(W_x) = i_x$. The function $H\colon B \to \mathbb{N}$ given by

$$H(x) = 2^{i_x} \cdot 3^{G_{W_x}(x)}$$

is one-to-one, so B is countable.

8.4. ***Exercise.*** *(i) Any chain in a tree is contained in a branch.*

(ii) Prove ***König's Tree Lemma****: If S is an infinite rooted tree but each $t \in S$ is the immediate predecessor of only finitely many members of S then S has an infinite branch. (hint: Let K denote those members of S with an infinite number*

of successors and for each $t \in K$ let $M_t = T_t \cap K - \{t\}$. Let f denote a choice function for these sets: $f(t) \in M_t\ \forall t \in K$. Use induction on $\mathbb{N}$ to create an infinite chain.)

The next section contains another important consequence of the Axiom of Choice. Many more can be found scattered in appendices and chapters throughout this book.

Those who want a slightly more detailed look at the ZF axioms can find them listed in Sections **??** and **??**. The discussions there are rudimentary but, I hope, a practical guide providing a taste of modern set theory.

9. Nets and Filters

Suppose $r\colon J \to X$ is a net. Recall that this means that J is pre-ordered and there is an upper bound in J for each two-element subset of J.

If $A \subset X,\ r$ is said to be **in** A if $r(J) \subset A$. r is said to be **eventually in** A if there is a terminal segment $T_\alpha \subset J$ such that $r(T_\alpha) \subset A$.

r is said to be **frequently in** A if $r(T_\alpha) \cap A \neq \varnothing\ \forall$ terminal segments T_α in J.

Obviously, if r is eventually in A then r is frequently in A.

A **subnet of** r is a net $s\colon K \to X$ such that $\exists f\colon K \to J$ for which $s = r \circ f$ and $\forall m \in J\ \exists n \in K$ such that $f(T_n) \subset T_m$. Note that f is not presumed to be non-decreasing. It is simply eventually in any terminal segment of J. A subnet of a subnet is also a subnet of the original net.

A net in a set X is called **universal** if the net is eventually in A or eventually in A^c for all $A \in \mathbb{P}(X)$.

9.1. ***Proposition.*** *Each net $r\colon D \to X$ has a universal subnet.*

Proof. Let $\mathbb{M} \subset \mathbb{P}^2(X) = \mathbb{P}(\mathbb{P}(X))$ be the set of all those $\mathbb{G} \subset \mathbb{P}(X)$ such that r is frequently in each member of $\mathbb{G}$ and also if $A, B \in \mathbb{G}$ then $A \cap B \in \mathbb{G}$.

Obviously $\{X\} \in \mathbb{M}$ so $\mathbb{M} \neq \varnothing$, and chains in $\mathbb{M}$ ordered by inclusion have upper bounds in $\mathbb{M}$ (the union of the chain) so $\mathbb{M}$ contains a maximal member $\mathbb{K}$.

If r is eventually in A or eventually in A^c then the maximality of $\mathbb{K}$ guarantees that one or the other is in $\mathbb{K}$. It remains to consider the case where r is frequently in A but $A \notin \mathbb{K}$. By maximality of $\mathbb{K}$ there must be some $S \in \mathbb{K}$ so that r is not frequently in $A \cap S$: that is, r is eventually in $(A \cap S)^c$. Now, if T is any member of $\mathbb{K},\ r$ is frequently in $T \cap S = (T \cap S \cap A) \cup (T \cap S \cap A^c)$ so r must be frequently in $T \cap S \cap A^c \subset T \cap A^c$. This is true for any $T \in \mathbb{K}$ so by maximality of $\mathbb{K},\ A^c \in \mathbb{K}$.

We have just shown that either A or $A^c \in \mathbb{K}\ \forall A \in \mathbb{P}(X)$.

Now let $E = \{\, (\alpha, B) \mid \alpha \in D,\ B \in \mathbb{K} \text{ and } r(\alpha) \in B \,\}$ directed by $(\alpha, B) \leq (\beta, C)$ precisely when $\alpha \leq \beta$ and $B \supset C$. The net $s\colon E \to X$ defined by $s((\alpha, B)) = r(\alpha)$ is a subnet of r and universal by construction. □

We now move on to the next idea of this section.

A nonempty subset $\mathbb{F}$ of $\mathbb{P}(X)$ is called a **filterbase on** X if

$$(a) \qquad \varnothing \notin \mathbb{F} \qquad \text{and}$$
$$(b) \qquad A, B \in \mathbb{F} \Rightarrow A \cap B \in \mathbb{F}.$$

If the additional condition

$$(c) \qquad A \in \mathbb{P}(X),\ B \in \mathbb{F} \Rightarrow A \cup B \in \mathbb{F}$$

holds, $\mathbb{F}$ is called a **filter on** X .

Given any nonempty subset $\mathbb{F}$ of $\mathbb{P}(X)$ for which finite intersections of members of $\mathbb{F}$ are nonempty there is a unique smallest filterbase containing $\mathbb{F}$. Each filterbase is contained in a unique smallest filter. This filterbase and this filter are said to be **generated by** $\mathbb{F}$.

The most common example of a filterbase is the collection of all open sets containing a particular point of a topological space. A filter containing this filterbase would be the set of all neighborhoods of that point.

Another filterbase would be $\{\, (0, a) \subset (0, \infty) \mid a > 0 \,\}$.

Yet another example is given by the following: Let $r\colon D \to X$ be a net in X. Let $\mathbb{F} = \{\, r(T_d) \mid d \in D \,\}$, where each T_d is a terminal segment of D. $\mathbb{F}$ is a filterbase. The collection of all sets containing any terminal segment, $\mathbb{G} = \{\, A \in \mathbb{P}(X) \mid r(T_d) \subset A \text{ for some } d \in D \,\}$, is the smallest filter containing $\mathbb{F}$.

Let $\boldsymbol{\mathcal{F}}$ denote the set of filters on X. $\boldsymbol{\mathcal{F}}$ is partially ordered by containment. If $\{\, \mathbb{F}_\alpha \mid \alpha \in J \,\}$ is any chain of filters then $\bigcup_{\alpha \in J} \mathbb{F}_\alpha$ is also a filter and an upper bound for the chain. So $\boldsymbol{\mathcal{F}}$ possesses maximal members called **ultrafilters.**

When $\mathbb{G}$ is a filterbase, $\{\, \mathbb{F} \in \boldsymbol{\mathcal{F}} \mid \mathbb{F} \supset \mathbb{G} \,\}$ is nonempty and possesses maximal members, which are maximal in $\boldsymbol{\mathcal{F}}$ as well. So any filterbase is contained in an ultrafilter.

It is not hard to show that a filter $\mathbb{F}$ on X is an ultrafilter if and only if whenever $A \in \mathbb{P}(X)$ then $A \in \mathbb{F}$ or $A^c \in \mathbb{F}$.

This provides a link between universal nets and ultrafilters.

If $\mathbb{F}$ is the filterbase on X formed from the net r as above, let $s\colon E \to X$ be a universal subnet of r. Let $\mathbb{K} = \{\, A \in \mathbb{P}(X) \mid s(T_d) \subset A \text{ for some } d \in E \,\}$. Since s is universal, either A or A^c is in $\mathbb{K}$ $\forall A \in \mathbb{P}(X)$. $\mathbb{K}$ is an ultrafilter containing $\mathbb{F}$.

Alternatively, suppose $\mathbb{F}$ is any filter and $\mathbb{G}$ is the ultrafilter generated by $\mathbb{F}$. Let $J = \{\, (x, A) \mid x \in A \in \mathbb{F} \,\}$ and $K = \{\, (x, A) \mid x \in A \in \mathbb{G} \,\}$. Direct J and K by $(x, A) \leq (y, B)$ if and only if $A \supset B$. We define $r\colon J \to X$ by $r((x, A)) = x$ and $s\colon K \to X$ by $s((x, A)) = x$. The filters $\mathbb{F}$ and $\mathbb{G}$ are precisely the sets formed from terminal segments of J and K by r and s, respectively. If we define $f\colon K \to J$ by $f((x, A) = (x, X)$, then $s = r \circ f$ and it follows that s is a subnet of r. Moreover, s is a universal net.

Suppose X is a nonempty set and $p \in X$. Let $\mathbb{F}_p$ denote the collection of all subsets of X containing p. $\mathbb{F}_p$ is an ultrafilter, and ultrafilters of this type are called **principal**. Other kinds of ultrafilters are called **free**.

If X is nonempty let $\mathbb{K}$ denote the set of **cofinite** subsets of X: that is, all subsets S of X for which $X - S$ is a finite set. If X is finite, $\mathbb{K} = \mathbb{P}(X)$. But if X is infinite, $\mathbb{K}$ is a filter on X, the **filter of cofinite subsets of X**.

9.2. ***Exercise.*** *(i) If $V_1, V_2, \ldots, V_n$ is a finite partition of X and $\mathbb{F}$ is an ultrafilter on X then $\mathbb{F}$ contains exactly one of the V_i.*

(ii) If an ultrafilter on X contains a finite set it contains a one point set, and is principal.

(iii) Suppose $\mathbb{U}$ is an ultrafilter on infinite X. $\mathbb{U}$ is free exactly when $\mathbb{U}$ contains all cofinite subsets of X.

(iv) There is a free ultrafilter $\mathbb{U}$ on $\mathbb{N}$ containing the set of even natural numbers. There is another containing the set of odd natural numbers. In fact if A is any infinite subset of $\mathbb{N}$ there is a free ultrafilter on $\mathbb{N}$ containing A.

10. Rings and Algebras of Sets

Consider $\mathbb{P}(X)$, the power set on the set X. When there is no danger of ambiguity and $A \subset X$, the notation A^c is often seen in place of $X - A$. $\mathbb{P}(X)$ is partially ordered by containment. $\mathbb{P}(X)$ is a lattice, with $A \wedge B = A \cap B$ and $A \vee B = A \cup B$. There is also additional structure on subsets of $\mathbb{P}(X)$.

$\mathbb{G} \subset \mathbb{P}(X)$ will be referred to as a **ring in X** if

(i) $\quad \varnothing \in \mathbb{G}$

(ii) $\quad A, B \in \mathbb{G} \Rightarrow A - B \in \mathbb{G}$ $\quad$ and

(iii) $\quad A, B \in \mathbb{G} \Rightarrow A \cup B \in \mathbb{G}$.

The last two items can be rephrased by saying that $\mathbb{G}$ is **closed** with respect to the operations $\cup$ and $-$.

$\mathbb{G} \subset \mathbb{P}(X)$ will be referred to as an **algebra on X** if, in addition

(iv) $\quad X \in \mathbb{G}$

Items (ii) and (iv) imply that $\mathbb{G}$ is **closed** with respect to the operations $\cup$ and ^{c}. In the presence of (iii), this last statement implies (ii).

It is apparent that item (i) is redundant in the presence of (ii) and (iv). Also, if $\mathbb{G}$ is a ring in X and A and B are in $\mathbb{G}$ then so is $A \cap B$. In fact, item (iii) could be replaced by "if A and B are in $\mathbb{G}$ then so is $A \cap B$" to yield equivalent definitions for a ring in a set.

10.1. ***Exercise.*** *(i) Show that the smallest algebra on X containing a topology for X consists of all sets $A \cap B$ or $A \cup B$ where A is an open set and B is a closed set.*

(ii) If $\mathbb{G}$ is a ring in X then both $\{ A \in \mathbb{P}(X) \mid A \in \mathbb{G}$ or $A^c \in \mathbb{G} \}$ and $\{ A \in \mathbb{P}(X) \mid A \cap B \in \mathbb{G}$ whenever $B \in \mathbb{G} \}$ are algebras on X.

*(iii) The set of "**clopen sets**" (that is, sets that are both open and closed) in a topology for X constitutes an algebra on X.*

10.2. ***Exercise.*** *(i) Suppose $\mathbb{G}$ is a ring in X. Define multiplication in $\mathbb{G}$ by $A \cdot B = A \cap B$ and addition by* ***symmetric difference****:*

$$A \triangle B = (A - B) \cup (B - A).$$

Show that $\mathbb{G}$ is a commutative (algebraic) ring with these operations. This ring has identity when the union of all sets in $\mathbb{G}$ is a member of $\mathbb{G}$. An additive subgroup $\mathbb{S}$ of this ring is an ideal exactly when $A \subset B$, $A \in \mathbb{G}$ and $B \in \mathbb{S}$ imply $A \in \mathbb{S}$.

(ii) Suppose X is infinite and $\mathbb{G}$ is a ring in X. Let $\mathbb{S}$ denote the finite members of $\mathbb{G}$. Then $\mathbb{S}$ is an ideal.

When thinking of rings and algebras of sets, bear in mind the following two.

All finite unions of bounded subintervals of $\mathbb{R}$ constitute a ring in $\mathbb{R}$.

An algebra on $\mathbb{R}$, obviously closely related to this ring, would be all finite unions of subintervals (bounded or not) of $\mathbb{R}$.

Apart from its raw defining qualities, an algebra on a set has useful properties which will be used throughout this work. Turn to Section 31 on Boolean Algebras and Rings to find out how some of these properties, when extracted and studied on their own, necessarily return to their roots as an algebra on a set.

Because of the way we handle the material of later chapters, rings in a set will be less common than algebras on a set.

Algebra April 22, 2020

This appendix constitutes a condensed introduction to a rather large fraction of an undergraduate abstract algebra course. To explore individual topics further (and see some of what was left out) the reader is invited to peruse Atiyah and MacDonald, *Introduction to Commutative Algebra* [**?**], Hungerford, T. W. *Algebra* [**?**], Lang, S., *Algebra* [**?**] and Dixon, J. D., *Problems in Group Theory* [**?**].

11. Groups

Suppose G is a nonempty set. A function $\otimes\colon G \times G \to G$ is called a **binary operation on** G. The notation $f \otimes g$ is used in this context in preference to $\otimes(f, g)$.

$\otimes$ is called **associative** if $f \otimes (g \otimes h) = (f \otimes g) \otimes h$ for all f, g and h in G.

A **semigroup** is a nonempty set G together with an associative binary operation $\otimes$ on G. The classic example is the set of positive integers with ordinary addition. Another is the set of positive integers with ordinary multiplication.

When there is more than one semigroup or operation around we will sometimes refer to a semigroup as an ordered pair such as $(G, \otimes)$, though this usage can be awkward and we will more often simply refer to "the semigroup G" or "a semigroup G with operation $\otimes$."

A **subsemigroup of** $(G, \otimes)$ is a semigroup $(H, \odot)$ where H is a subset of G and $f \otimes g = f \odot g$ for every f, g in H. In other words, $\odot$ agrees with $\otimes$ on members of H. Because of this similarity, when H is a subsemigroup of G we will usually use the same symbol for the two binary operations. Example: the even positive integers form a subsemigroup of the positive integers with either addition or multiplication.

In case $f \otimes g = g \otimes f$ the elements f and g are said to **commute with respect to the binary operation** $\otimes$.

$\otimes$ is called **commutative** if all pairs of elements commute with respect to $\otimes$. A semigroup is called **abelian** if $\otimes$ is commutative.

An element $\mathbf{e}_\otimes \in G$ is called an **identity for** $\otimes$ if $f \otimes e_\otimes = e_\otimes \otimes f = f$ for all f in G.

A semigroup with identity is called a **monoid**. A **submonoid of** of a monoid $(G, \otimes)$ is a subsemigroup which contains the identity of G.

As an example, $[0, \infty]$ is a monoid with both addition and multiplication.

If a binary operation $\otimes$ on G has an identity $e_\otimes$, an element f of G is called a **$\otimes$-inverse to the element** h of G if $f \otimes h = h \otimes f = e_\otimes$. Sometimes the inverse of an element h is denoted $-h$ and sometimes h^{-1}, depending on context and the customs involving the specific binary operation.

$(0, \infty)$ is the subset of $[0, \infty]$ of those elements with multiplicative inverses. Elements of $(0, \infty]$ have no additive inverses.

A **group** is a monoid $(G, \otimes)$ for which every member of G has a $\otimes$-inverse.

11.1. ***Exercise.*** *(i) There can be at most one identity in a semigroup.*

(ii) An element of a semigroup can have at most one inverse.

(iii) Both elements a and b of a semigroup have inverses if and only if $a \otimes b$ does. When defined, $(a \otimes b)^{-1} = b^{-1} \otimes a^{-1}$.

(iv) Suppose G is a semigroup and there is an element e_L in G so that $e_L \otimes g = g\ \forall g \in G$ and also for each $g \in G$ there is an element $g_L \in G$ for which $g_L \otimes g = e_L$. Then G is a group. What we are saying here is that if there is an element that acts like a "left identity" in a semigroup, and also if "left inverses" always exist corresponding to this "left identity" then a "left inverse" is also a right inverse, and the "left identity" is also a right identity. The same result holds with the word "right" replacing "left" above. (First show that $g \otimes g = g$ implies $g = e_L$. Then examine $g \otimes g_L \otimes g \otimes g_L$ and $g \otimes g_L \otimes g$.)

A **subgroup of** a group $(G, \otimes)$ is a group $(H, \odot)$ which is a submonoid of $(G, \otimes)$.

A subset H of a group $(G, \otimes)$ is a subgroup with the induced operation provided $g \otimes h^{-1}$ is in H whenever g and h are in H.

Every group is a subgroup of itself, and so is the set containing the identity alone. These are not very interesting subgroups. The identity alone is called the **trivial subgroup**. A subgroup other than G itself is called a **proper subgroup**. Mostly we will want to know about nontrivial, proper subgroups.

We now introduce a handy notation which will be used elsewhere in the text.

Suppose $(G, \otimes)$ is a commutative semigroup. We will need a notation for a specified extended "product" or "sum" of a finite number of elements of G which might be denoted $g_1 \otimes \cdots \otimes g_n$. Commutativity and associativity of $\otimes$ guarantee that an extended combination of elements of G of this kind does not depend on order in any way.

Let $f\colon A \to G$ and suppose $\widetilde{A} = \{\ a \in A \mid f(a) \neq e_\otimes\ \}$ is finite and nonempty. If $\otimes$ has no identity this means that A itself is finite. Let $a_1, \ldots, a_n$ be a listing of the n elements of $\widetilde{A}$.

We define both $\prod_{\mathbf{a}\in\mathbf{A}} \mathbf{f}(\mathbf{a})$ and $\sum_{\mathbf{a}\in\mathbf{A}} \mathbf{f}(\mathbf{a})$ to be the combination of the n elements of G indicated as $f(a_1) \otimes \cdots \otimes f(a_n)$. The $\prod$ notation is used when the operation "looks like" multiplication, while the $\sum$ notation is customarily used when the operation "looks like" addition.

When $\widetilde{A}$ is empty and if $e_\otimes$ exists it is customary to define an empty sum or product to be $e_\otimes$.

11.2. ***Exercise.*** *What additional structure must A possess and how would you use that structure to define an extended product notation similar to that given above but for nonabelian semigroups?*

Examples of groups and semigroups abound. We will use sets of numbers and matrices and the familiar operations on them to provide a variety of examples of groups with different properties.

If $(G, \otimes)$ is a group, any intersection of subgroups of G is a subgroup of G. Also, the union of any chain (ordered by containment) of subgroups of G is a subgroup of G.

If S is a subset of G, the intersection of all subgroups of G containing S is a subgroup of G, called the **subgroup generated by S**. As an example, for $g \in G$ let $\mathbf{Cyclic}_\otimes(\mathbf{g})$ be the intersection of all subgroups of G containing g. If there is only one group operation around, we will usually denote this group $Cyclic(g)$. If n is a positive integer, there are two common notations for an element g combined

with itself n times using the operation $\otimes$. If $\otimes$ "looks like" addition we write $ng = g \otimes g \otimes \cdots \otimes g$. If $\otimes$ "looks like" multiplication we usually write g^n for the same combination. In the first case, $0g$ indicates $e_\otimes$ while in the second $g^0 = e_\otimes$ is used. If n is a negative integer, we write $ng = (-n)(-g)$ or $g^n = (g^{-1})^{-n}$. Using the multiplicative version, $Cyclic(g) = \{\ g^n \mid n \in \mathbb{Z}\ \}$. Using the additive version, $Cyclic(g) = \{\ ng \mid n \in \mathbb{Z}\ \}$. Whichever notation is used, $Cyclic(g)$ is an abelian subgroup of G, called the **cyclic subgroup generated by g.** A group G is called **cyclic** if $G = Cyclic(g)$ for some $g \in G$.

11.3. ***Exercise.*** *If G is any finite group (that is, as a set G has finite cardinality) then there is an integer N for which $g^N = e$, where e is the group identity, for all $g \in G$. (hint: Since G is finite the list $e, g, g^2, \ldots$ must begin to repeat. Deduce first that for each g there is a least nonnegative integer n_g for which $g^{n_g} = e$.)*

11.4. ***Exercise.*** *Suppose G is a finite group and that the cardinality of the group is divisible by 2. Fill in the argument below to show that there must be at least two members of G whose square is e, the identity of the group.*

Let S denote the set of all sets of the form $S_g = \{\, g, g^{-1}\,\}$ for $g \in G$. Every member of G is in exactly one of these sets, so S is a partition of G. So the cardinality of G is the sum of the cardinalities of the distinct classes. Each class has cardinality 1 or cardinality 2. At least one class has cardinality 1, namely S_e. If all the rest had cardinality 2 we would conclude that G had odd cardinality, contrary to assumption. So there is at least one member g of G other than e with $g = g^{-1}$ and so $g^2 = e$. (Exercise 16.10 outlines a generalization of this method.)

If $(G, \otimes)$ and $(H, \oplus)$ are two semigroups, define a binary operation $\odot$ on $G \times H$ by $(g, h) \odot (a, b) = (g \otimes a, h \oplus b)$. This operation is a semigroup operation. With this operation, $G \times H$ is called the **external direct product, or sometimes just the direct product, of the semigroups G and H**.

More generally, suppose A is a nonempty set and $(G_a, \otimes_a)$ is a semigroup for each $a \in A$. Let $H = \cup_{a \in A} G_a$ and define $\prod_{\mathbf{a \in A}} \mathbf{G_a}$ to be the set of all functions $f\colon A \to H$ with $f(a) \in G_a\ \forall a \in A$. Define operation $\otimes$ on $\prod_{a \in A} G_a$ by $(f \otimes g)(a) = f(a) \otimes_a g(a)\ \forall a \in A$. $\prod_{a \in A} G_a$ is a semigroup with this operation, called the **external direct product, or sometimes just the direct product, of the $\mathbf{G_a}$.**

The direct product is a group exactly when every one of the semigroups G_a is a group. If $(G_a, \otimes_a) = (G, \otimes)$ for all $a \in A$ then, as a set, $\prod_{a \in A} G_a = G^A$.

The subset $\sum_{\mathbf{a \in A}} \mathbf{G_a}$ of $\prod_{a \in A} G_a$ consists of those members of $\prod_{a \in A} G_a$ which are $e_{\otimes_a}$ except at finitely many $a \in A$. This set will be empty unless all but finitely many of the G_a actually has an identity. If nontrivial, $\sum_{a \in A} G_a$ with the operation inherited from the direct product, is called the **direct sum of the $\mathbf{G_a}$**, and is a subsemigroup of the direct product. Obviously, if A is finite, direct product and direct sum are the same concept.

A direct product or sum is abelian if and only if each G_a is abelian. A direct product or sum has an identity exactly when every G_a has an identity.

11.5. ***Exercise.*** *$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ with ordinary addition are abelian groups. Each of these is a subgroup of the next. $\sqrt{2}\mathbb{Q}$, the rational multiples of $\sqrt{2}$, forms an abelian group with addition. For fixed integer n let $\mathbf{n}\mathbb{Z}$ denote the set of all integer multiples*

of n. It forms an abelian group with addition. $\mathbb{Q}(\sqrt{2}) = \{\, p+q\sqrt{2} \mid p, q \in \mathbb{Q} \,\}$ forms an abelian group with addition.

11.6. ***Exercise.*** *If S is a nonempty set and* $\mathbf{Perm(S)}$ *is the set of all one-to-one and onto functions $P\colon S \to S$ then $Perm(S)$ is a group with composition. It is called the* ***group of permutations of*** $\mathbf{S}$*, or sometimes the* ***symmetric group on*** $\mathbf{S}$*. The set of permutations on the first n positive integers, a common case, will usually be denoted* $\boldsymbol{\mathfrak{S}_n}$*.*

If T is a subset of S define $\mathbf{Perm_T(S)}$ *to be the set of those permutations P of S for which $P(s) = s$ except possibly when $s \in T$. $Perm_T(S)$ is a subgroup of $Perm(S)$. Also, let* $\mathbf{Finite(S)}$ *denote the set of those permutations P for which $P(s) = s$ except for finitely many $s \in S$. If S is a finite set, $Perm(S) = Finite(S)$, but otherwise $Finite(S)$ is a distinct subgroup of $Perm(S)$. If T is finite $Perm_T(S)$ is a subgroup of $Finite(S)$.*

11.7. ***Exercise.*** *Suppose G is a semigroup with operation $\oplus$ and let m and n be positive integers. Meditate on the similarities among the sets G^{mn}, $(G^n)^m$ and $(G^m)^n$ and use $\oplus$ to define a semigroup operation on each set. Which of these three would you like to call "the set of m by n matrices with entries in G?"*

11.8. ***Exercise.*** *Let* $\mathbf{M_n(A)}$ *be the set of n by n matrices with entries in the nonempty set A, where n is a positive integer. The sets of matrices $M_n(\mathbb{Z})$, $M_n(\mathbb{Q})$, $M_n(\mathbb{R})$ and $M_n(\mathbb{C})$ with ordinary matrix addition are abelian groups. Each of these is a subgroup of the next. Each of these is a monoid with matrix multiplication as operation. Unless n is 1, matrix multiplication involving these matrices is not commutative.*

11.9. ***Exercise.*** *$\{1\}$, $\{-1, 1\}$, $\mathbb{Q} - \{0\}$, $\mathbb{Q}(\sqrt{2}) - \{0\}$, $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$ with the usual multiplications are abelian groups. Each of these is a subgroup of the next. The complex numbers of magnitude 1 form an abelian group with complex multiplication. If z is a complex number of magnitude 1 its multiplicative inverse is just $\overline{z}$, the complex conjugate of z, which also has magnitude 1. The positive rational numbers and the positive real numbers are abelian groups with multiplication.*

Consider the four matrices from $M_2(\mathbb{R})$:

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{and} \quad c = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

We will have occasion to refer to these matrices numerous times in important examples in this appendix. *In the context of 2 by 2 matrices, these symbols will be reserved.* You will note that

$$a^2 = -e \quad \text{and} \quad b^2 = c^2 = e$$

$$\text{while} \quad ab = -ba = c \quad \text{and} \quad cb = -bc = a \quad \text{and} \quad ca = -ac = b.$$

Using this "multiplication table" you can avoid matrix multiplications as you work with these examples.

11.10. ***Exercise.*** *The four matrices $\{\, e,\ -e,\ a,\ -a \,\}$ from $M_2(\mathbb{R})$ form an abelian group with matrix multiplication.*

More generally, if n is a positive integer the n matrices from $M_2(\mathbb{R})$:

$$\cos\left(\frac{2k\pi}{n}\right)e + \sin\left(\frac{2k\pi}{n}\right)a = \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) & -\sin\left(\frac{2k\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right) & \cos\left(\frac{2k\pi}{n}\right) \end{pmatrix} \text{ for } k = 0 \ldots n-1$$

form an abelian group with matrix multiplication. These matrices represent counterclockwise rotations of the plane by angles which are multiples of $2\pi/n$ and for particular n we will refer to this group as $\mathbf{Rot_n}$*,* ***the rotation group*** *by angle $2\pi/n$. At most two members of Rot_n satisfy $x^2 = e$, where e is the identity matrix of this group. Rot_n is cyclic.*

11.11. ***Exercise.*** *The eight matrices $\{\, e,\ -e,\ a,\ -a,\ b,\ -b,\ c,\ -c \,\}$ form a group with matrix multiplication. It is not abelian. We will call it* **SquareSym**. *It is the* ***group of symmetries of the square*** *in the following sense. Draw a picture of a square centered at the origin of the XY plane with corners on the coordinate axes. All of the ways of rigidly mapping this square to itself, sending corners to corners (including reflection across the diagonal) can be obtained by multiplying all coordinates of the points in the square by a matrix from $SquareSym$.*

We recall from above that six of the eight members of $SquareSym$ satisfy $x^2 = e$, where e is the identity matrix of this group, while two satisfy $x^2 = -e$.

The eight matrices $\{\, e,\ -e,\ a,\ -a,\ ib,\ -ib,\ ic,\ -ic \,\}$ from $M_2(\mathbb{C})$ also form a group with matrix multiplication. It too fails to be abelian. We will refer to it as **Quat**. *See Exercise 21.16 for the genesis of this name.*

Six of the eight members of $Quat$ satisfy $x^2 = -e$, while only two satisfy $x^2 = e$.

Recall (or look up) the following facts about square matrices. A square matrix with complex entries has a multiplicative inverse provided that its **determinant** is nonzero. Determinants are formed as sums and differences of products of the entries of a matrix. If a matrix B is obtained from a matrix A by multiplying all entries in one row or one column of A by the complex number c, the determinant of B is c times the determinant of A. If you switch two rows or two columns of a square matrix the determinant of the new matrix is -1 times the former determinant. If you add a multiple of a row of a matrix to a different row, or a multiple of a column of a matrix to a different column, the determinant of the new matrix is unchanged. If A and B are two compatible square matrices then the determinant of AB is the product of the determinants of A and B separately. Finally, **Cramer's Rule** gives a formula for the entries of the multiplicative inverse of an invertible matrix A, explicitly, as a ratio of determinants involving the entries of A.

If $m < n$, an m by m matrix can be "fit inside" an n by n matrix—put the smaller matrix in the upper left block of the larger one, with zeros outside this block. That means that $M_m(\mathbb{C})$ looks a lot like a subset of $M_n(\mathbb{C})$. Abstracting certain features of this situation, we have the following exercises.

11.12. ***Exercise.*** *(i) Let H denote the set of all the matrices of $M_2(\mathbb{C})$ "fit inside" $M_3(\mathbb{C})$ as described above. H is a subgroup of $M_3(\mathbb{C})$ with matrix addition, and matrix addition in H "agrees with" matrix addition in $M_2(\mathbb{C})$.*

(ii) Let K denote the two matrices comprising Rot_2 "placed inside" $M_3(\mathbb{C})$ as described above. K is a group with matrix multiplication, and the matrix multiplication on members of K "agrees with" matrix multiplication in Rot_2. K is a monoid and a subsemigroup of the monoid $M_3(\mathbb{C})$ with matrix multiplication. But K does not contain the multiplicative identity of $M_3(\mathbb{C})$. It is not a submonoid (or subgroup) of $M_3(\mathbb{C})$ for this reason.

11.13. ***Exercise.*** *Suppose J is a directed set and G_i is a semigroup with operation $\oplus_i$ for each $i \in J$. Suppose further that whenever $i \leq j$ then G_i with $\oplus_i$ is a subsemigroup of G_j with $\oplus_j$. Show that the operations involved here can be used to define a semigroup operation on $\bigcup_{j\in J} G_j$.*

If, further, each of these semigroups G_j with $\oplus_j$ is a group with identity e_j, is $\bigcup_{j\in J} G_j$ necessarily a group with this induced operation? (Note: we are not assuming that G_i with $\oplus_i$ is a subgroup of G_j with $\oplus_j$ when $i \leq j$.)

11.14. ***Exercise.*** *Define $\mathbf{M}_\infty(\,[\mathbf{0},\infty]\,)$ to be the set of nonnegative extended real valued functions defined on ordered pairs of positive integers*

$$f\colon \{\,1,2,\dots\,\}\times\{\,1,2,\dots\,\}\to[0,\infty].$$

(i) It is easy to show that $M_\infty(\,[0,\infty]\,)$ is a monoid with addition of functions, and harder to show (but true) that it is a monoid with multiplication given by

$$(fg)_{i,j}=\sum_{n=1}^{\infty} f_{i,n}g_{n,j}.$$

Prove these facts.

(ii) Is $M_n(\,[0,\infty)\,)$ a submonoid of $M_\infty(\,[0,\infty]\,)$ with matrix addition? What about matrix multiplication?

(iii) Let S be the subset of those members of $M_\infty(\,[0,\infty]\,)$ with the property that "each row and each column" is square summable. Specifically,

$$\sum_{n=1}^{\infty} f_{n,k}^2<\infty \quad \textit{and} \quad \sum_{n=1}^{\infty} f_{k,n}^2<\infty \quad \forall k.$$

If f and g are in S, is $f+g\in S$? What about fg, with multiplication inherited from $M_\infty(\,[0,\infty]\,)$? (hint: Tracking down techniques for this part of the exercise might take you out of the world of groups.)

If A is a matrix, $\mathbf{A^t}$ denotes the **transpose** of A: the matrix obtained by switching the row and column designations on the entries of A. $\mathbf{A}^*$ denotes the **conjugate transpose** of A: the matrix obtained by taking conjugates of the entries of A and then switching the row and column designations. The determinant of A^t is the same as the determinant of A.

A square matrix A is called **hermitian** if $A = A^*$. It is called **skew hermitian** if $-A = A^*$. It is called **symmetric** if $A = A^t$ and **skew symmetric** if $-A = A^t$.

The **trace** of a square matrix is the sum of the diagonal entries of the matrix.

So the trace of any skew symmetric matrix is 0. The trace of any hermitian matrix is real. The trace of any skew hermitian matrix is purely complex: it is the sum of real multiples of i.

With these facts in hand we define certain subsets of $M_n(\mathbb{C})$.

11.15. ***Exercise.*** *The following sets of matrices are abelian groups with matrix addition, where H is $\mathbb{C}$ or $\mathbb{R}$ or or $\mathbb{Q}$. (Note: not all these groups are distinct.)*

$\mathbf{M}_{\mathbf{H}}^{traceless} = \{A \in M_n(H) \mid A \text{ has trace } 0\}$

$\mathbf{M}_{\mathbf{H}}^{sym} = \{A \in M_n(H) \mid A \text{ is symmetric }\}$

$\mathbf{M}_{\mathbf{H}}^{skewsym} = \{A \in M_n(H) \mid A \text{ is skew symmetric }\}$

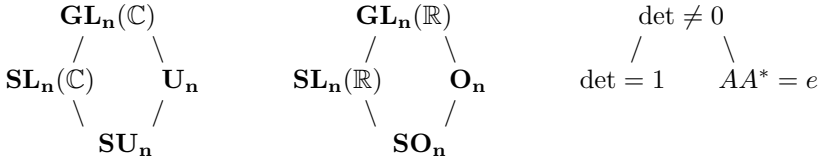
$\mathbf{M}_{\mathbf{H}}^{hermitian} = \{A \in M_n(H) \mid A \text{ is hermitian }\}$

$\mathbf{M}_{\mathbf{H}}^{skewherm} = \{A \in M_n(H) \mid A \text{ is skew hermitian }\}$.

If $A \in M_n(\mathbb{C})$ define $\mathbb{R}A$ to be the set of all real multiples of the matrix A and define $\mathbb{C}A$ similarly. These sets of matrices are always abelian subgroups of $M_n(\mathbb{C})$ with matrix addition. Members of one of these additive subgroups commute with each other with matrix multiplication too. Give conditions on A so that $\mathbb{R}A$ or $\mathbb{C}A$ is an additive subgroup of one of the ten groups listed above.

Here are some more.

- $\mathbf{GL_n}(\mathbb{C})$: the set of matrices in $M_n(\mathbb{C})$ with nonzero determinant. This set is called the **complex general linear group** of n by n matrices.
- $\mathbf{GL_n}(\mathbb{R})$: the set of matrices in $M_n(\mathbb{R})$ with nonzero determinant. This set is called the **real general linear group** of n by n matrices.
- $\mathbf{SL_n}(\mathbb{C})$: the set of matrices in $M_n(\mathbb{C})$ with determinant 1. This set is called the **complex special linear group** of n by n matrices.
- $\mathbf{SL_n}(\mathbb{R})$: the set of matrices in $M_n(\mathbb{R})$ with determinant 1. This set is called the **real special linear group** of n by n matrices.
- $\mathbf{U_n}$: the set of matrices A in $M_n(\mathbb{C})$ with $AA^* = e$ where e is the identity matrix. This implies the determinant of A has magnitude 1. This set is called the **unitary group** of n by n matrices.
- $\mathbf{O_n}$: the set of matrices A in $M_n(\mathbb{R})$ with $AA^t = e$. This implies the determinant of A is ± 1. This set is called the **orthogonal group** of n by n matrices.
- $\mathbf{SU_n} = U_n \cap SL_n(\mathbb{C})$. This set is called the **special unitary group** of n by n matrices.
- $\mathbf{SO_n} = O_n \cap SL_n(\mathbb{R})$. This set is called the **special orthogonal group** of n by n matrices.



11.16. ***Exercise.*** *Show that the sets of matrices described above are in fact multiplicative groups, as are the similar sets of matrices with rational number entries.*

11.17. ***Exercise.*** *When $A \in M_n(\mathbb{C})$ for $n \geq 1$ and m exceeds the maximum magnitude of all entries in A one can show by induction that the maximum magnitude of any entry of A^k cannot exceed $n^{k-1}m^k$ for any positive integer k. Defining A^0 to be the identity matrix, it follows that the entries of*

$$e^A = \sum_{k=0}^{\infty} \frac{A^k}{k!}$$

are absolutely convergent series and if matrices A and B commute then $e^A e^B = e^{A+B}$.

If G is any additive semigroup formed from members of $M_n(\mathbb{C})$ which commute with each other under matrix multiplication then $e^G = \{\, e^A \mid A \in G \,\}$ is a commutative semigroup with matrix multiplication. If G is a group, so is e^G.

(Though we will not pursue the matter in these notes, the exponential map defined here links the additive matrix groups explored in Exercise 11.15 with the multiplicative groups of matrices listed after that exercise.)

Suppose $f(x) = \sum_{k=0}^{\infty} a_k x^k$ is a power series and there is a real number $c < 1$ with $\left|\frac{a_{k+1}}{a_k}\right| \leq \frac{c}{nm}$ for sufficiently large k. Define $f(A)$.

11.18. ***Exercise.*** *Let $\mathbf{X}(\mathbf{A})$ be the set of members of $M_2(A)$ of the form*

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix} = x\,e + y\,a \quad \text{with } x \text{ and } y \text{ in } A \text{ and matrices } e \text{ and } a \text{ from page 40.}$$

$X(\mathbb{Z})$, $X(\mathbb{Q})$, $X(\mathbb{R})$ and $X(\mathbb{C})$ are all abelian groups with matrix addition. If you delete the zero matrix, the last three are also abelian groups with matrix multiplication.

12. Counting with Cosets

If g is a member of a semigroup $(G, \otimes)$ and A a nonempty subset of G we define $\mathbf{g} \otimes \mathbf{A} = \{\, g \otimes h \in G \mid h \in A \,\}$ and $\mathbf{A} \otimes \mathbf{g} = \{\, h \otimes g \in G \mid h \in A \,\}$. Similarly, if B is another nonempty subset of G we define $\mathbf{A} \otimes \mathbf{B} = \{\, h \otimes k \mid h \in A,\ k \in B \,\}$. When the binary operation "looks like" multiplication the operation is often left out of the notation, and these sets are denoted simply gA, Ag or AB and an element $h \otimes k$ is denoted hk.

When A and B are groups, and in case the set AB is a group too, it is sometimes called the **internal direct product of A and B**.

If G is a group with subgroup H and nonempty subset A the **centralizer of A in H** is denoted $\mathbf{C}(\mathbf{A}, \mathbf{H})$ and defined to be $\{\, h \in H \mid gh = hg\ \forall g \in A \,\} = \{\, g \in G \mid hgh^{-1} = g\ \forall g \in A \,\}$. It is the set of elements of H which commute with every element of A, and it is a subgroup of H. $C(A, H)$ need not be abelian. The **center of G** is denoted $\mathbf{Z}(\mathbf{G})$ and is defined to be $C(G, G)$. The center of a group *is* abelian. A group G is abelian if and only if $Z(G) = G$.

The **normalizer of A in H** is denoted $\mathbf{N}(\mathbf{A}, \mathbf{H})$ and defined to be $\{\, h \in H \mid hA = Ah \,\} = \{\, h \in H \mid hAh^{-1} = A \,\}$. Membership in $N(A, H)$ is less restrictive than membership in $C(A, H)$: an element h of $N(A, H)$ need not commute with every element of A. hgh^{-1} need only be *in* A for each $g \in A$. $N(A, H)$ is a subgroup of H.

If A has a single element x the centralizer and normalizer are the same, and both are denoted $\mathbf{N(x, H)}$.

For the next few paragraphs we will suppose that H and K are subgroups of a group G.

The set **gH** is called the **left coset of the subgroup H generated by g** and the set **Hg** is called the **right coset of the subgroup H generated by g**.

We will let $|\mathbf{S}|$ denote the cardinal number of a set S. In our discussions below, finite cardinalities will be our main interest and you may restrict your attention to those cases if you wish, at least on first reading.

If G is a group, the cardinal number $|G|$ is called the **order** of the group. The **order of an element** g of a group is the order of $Cyclic(g)$. In this case the notation $\mathbf{o(g)} = |Cyclic(g)|$ is used. If finite, it is the least positive integer n for which $g^n = e$.

12.1. ***Exercise.*** *Suppose G is a group and K and H are subgroups of G. Let C denote the collection of sets $\{\ hK \mid h \in H\ \}$ produced by members of H and K and let D denote the collection of sets $\{\ Kh \mid h \in H\ \}$.*

(i) Show that $|gK| = |Kh|\ \forall h, g \in G$.

(ii) $|C| = |D|$.

(iii) C and D are partitions of HK and KH, respectively.

(iv) $|HK| = |KH|$.

(v) $HK = KH$ if and only if HK is a subgroup of G.

When A is any subset of G that can be formed as HK for *subgroups* H and K of G define $[\mathbf{A} : \mathbf{K}]$ to be the cardinal number of the set of left cosets of K generated by the members of H. We call this cardinal number the **index of K in A.** We make special note that there may be a variety of ways that A can be represented as HK. The index, however, does not depend on the representation: only on the fact that one exists. If K is a subgroup of H, we have $H = HK$ as a special case.

12.2. ***Exercise.*** *If $A = HK$ for subgroups H and K of G there is a subset B of H with the following property: $BK = A$ and whenever $QK = A$ with $Q \subset B$ then $Q = B$. Moreover, $|B| = [A : K]$. (B, of course, will not usually be a subgroup of G: it can be a selection of one member of H in each distinct coset.)*

12.3. ***Exercise.*** *Suppose H and K are subgroups of G and let C denote the set of left cosets of K in HK.*

(i) $\quad |HK| = |C \times K| \quad$ *so* $\quad |HK| = [HK : K]|K|$.

(ii) $\quad [H : H \cap K] = [HK : K] \quad$ *and* $\quad |H \times K| = |H||K| = |HK||H \cap K|$.

(iii)
$$\begin{aligned}[G : H \cap K] &= [G : H][H : H \cap K] = [G : H][HK : K] \\ &\leq [G : H][G : K] \text{ with equality only when } HK = G.\end{aligned}$$

(iv) If $g \in G$ and $o(g)$ is finite then $g^{o(g)} = e$, where e is the identity in G and

$$Cyclic(g) = \{\ g^k \mid 1 \leq k \leq o(g)\ \}.$$

Further, if $n > 0$ and $g^n = e$ then $o(g)$ divides n.

*(v) $GK = G$ so, from (i), if G is finite we know $|G|$ is an integer multiple of $|K|$. In particular (**Lagrange's Theorem**), the order of each element of G is a factor of the order of G. So $g^{|G|} = e$ $\forall g \in G$.*

(vi) If $|H|$ and $|K|$ are finite and share no common factor then $H \cap K = \{ e \}$.

An element a of any group G is said to be a **torsion element** if there is an integer n for which $a^n = e$, the group identity. If every element has finite order, the group is called, synonymously, a **periodic group** or a **torsion group**. If every element except the identity has infinite order, the group is called **torsion free**.

The least positive n for which $a^n = e$ for every $a \in G$, if any, is called the **exponent** of the group. If it exists, it is the least common multiple of the orders of the elements of G. It is easy to produce (infinite) torsion groups with no exponent. See Exercise 20.6 for an example. But every finite group has an exponent. It is a divisor of the order of the group.

The **torsion set** (the set of torsion elements) will *not*, in general, form a subgroup. See Exercise 20.7 for an example. The torsion set of an abelian group, however, *is* a subgroup.

If A is a nonempty subset of a group G we define a **conjugate of A in G** to be a set of the form gAg^{-1} for some $g \in G$.

12.4. ***Exercise.*** *(i) If A is a subgroup of G so is each gAg^{-1}, and in any case $|A| = |gAg^{-1}|$.*

(ii) With H a subgroup of G, let S denote the set of conjugates of A by members of H. Specifically, $S = \{\ hAh^{-1} \mid h \in H\ \}$.

Then $|S| = [H : N(A, H)]$. This means

$$|H| = [H : N(A, H)]|N(A, H)| = |S||N(A, H)|$$

and, in particular, if H is finite then $|S|$ is a factor of the order of H.

(iii) Again suppose H is a subgroup of G but this time let S be the set of all conjugates of H in G. As a special case of (ii) we have $|S| = [G : N(H, G)]$. Since $[G : H] = [G : N(H, G)][N(H, G) : H]$, the number of conjugates of H in G is a divisor of the number of left cosets of H in G. Their numbers are equal only when there is no subgroup between H and G within which H is normal.

12.5. ***Exercise.*** *Suppose H is a proper subgroup of finite group G. Then G cannot be the union of conjugates of H. (hint: If H has only one conjugate in G the result is obvious. But if H has more, the number of conjugates is $[G : N(H, G)]$ and each conjugate has cardinality $|H|$. Each conjugate shares with the others, at least, the identity. Now examine $|G| = [G : N(H, G)]|N(H, G)|$.)*

Suppose H and K are subgroups of a group G. A set of the form

$$\mathbf{HxK} = \{\ hxk \mid h \in H, k \in K\ \} \text{ for } x \in G$$

is called a **double coset of H and K** (in that order.)

12.6. ***Exercise.*** *Suppose H and K are subgroups of a group G.*

(i) The set $S = \{HxK \mid x \in G\}$ of double cosets forms a partition of G.

(ii) There is a subset B of G with the following property: $G = \bigcup_{b\in B} HbK$ and whenever $Q \subset B$ with $G = \bigcup_{q\in Q} HqK$ then $Q = B$. Moreover, $|B| = |S|$. (B is a selection of one member from each distinct double coset.)

(iii) $|HxK|\,|H \cap xKx^{-1}| = |HxKx^{-1}|\,|H \cap xKx^{-1}| = |H|\,|xKx^{-1}| = |H|\,|K|$.

When $|H \cap xKx^{-1}|$ is finite this becomes

$$|HxK| = \frac{|H|\ |K|}{|H \cap xKx^{-1}|}.$$

(iv) If $|H||K|$ exceeds $|G|$ then H and K have nontrivial intersection.

12.7. ***Exercise.*** *Suppose H is a subgroup of a finite group G.*

(v) $H \cap xHx^{-1} = H$ if and only if $x \in N(H, G)$. So $|HxH|$, which is a multiple of $|H|$, is equal to $|H|$ if and only if $x \in N(H, G)$

(vi) $x \in N(H, G)$ if and only if $HxH \subset N(H, G)$. So any double coset of this form intersecting $N(H, G)$ at all is entirely in $N(H, G)$, and these double cosets form a partition of $N(H, G)$. For these particular cosets $HxH = xH$, so the number of these double cosets (which are actually left cosets) is $[N(H, G) : H]$.

13. Homomorphisms and Normal Subgroups

If H is a subgroup of G and $N(H, G) = G$ we call H a **normal subgroup of G**. Normal subgroups have only one conjugate in G. Left cosets and right cosets of H are the same when H is normal. H is always normal as a subgroup of $N(H, G)$, and in fact $N(H, G)$ is the largest subgroup of G within which H is normal.

13.1. ***Exercise.*** *Suppose H and N are subgroups of G, and e is the identity in G.*

(i) Suppose $N \cap H = \{\, e \,\}$. If $xh = yg$ for certain $x, y \in N$ and $h, g \in H$ then $y^{-1}x = gh^{-1} = e$. So in this case every member w of NH has a unique representation as $w = xh$ for $x \in N$ and $h \in H$.

(ii) If N is normal in G then $NH = HN$ so NH is a subgroup of G.

(iii) Suppose both N and H are normal and $N \cap H = \{\, e \,\}$ then $xhx^{-1}h^{-1} = e$ for $x \in N$ and $h \in H$ so every member of N commutes with every member of H. (Note: this does not imply that HK is abelian.)

The **normal core of a subgroup H of a group G** is the intersection of all the conjugates of H in G. It is denoted $\mathbf{core_G(H)}$.

13.2. ***Exercise.*** *(i) $core_G(H)$ is the largest subgroup of H which is normal in G.*

(ii) If $[G : H]$ is finite so is $[G : core_G(H)]$. (hint: If $[G : H]$ is finite so is the cardinality of the set of conjugates of H. Apply Exercise 12.3 (iii) repeatedly.)

When H is a normal subgroup of the group $(G, \otimes)$ the set of cosets of H is denoted $\mathbf{G/H}$. It is made into a group by the binary operation $\widetilde{\otimes}$ defined by $gH\widetilde{\otimes}fH = (g\otimes h)H$. This group is called the **quotient group or, synonymously, the factor group of G by H.**

13.3. ***Exercise.*** *Verify that when H is normal the operation $\widetilde{\otimes}$ is well defined and the cosets of H form a group with this operation.*

If $(G, \otimes)$ and $(H, \odot)$ are any two groups a function $w\colon G \to H$ is called a **group homomorphism** provided $w(f \otimes g) = w(f) \odot w(g)$ for all f and g in G.

If w is a homomorphism $w(e_\otimes)e_\odot = w(e_\otimes e_\otimes) = w(e_\otimes)w(e_\otimes)$ and left cancellation (that is, multiplying both sides on the left by $w(e_\otimes)^{-1}$) shows that $w(e_\otimes) = e_\odot$. We find similarly that $w(g^{-1})$ is always $w(g)^{-1}$.

The set of all homomorphisms between these groups is denoted $\mathbf{Hom}(\mathbf{G}, \mathbf{H})$. The more precise notation $Hom((G, \otimes), (H, \odot))$ is avoided when possible. Even more, it is not unheard of to use the same symbol or even juxtaposition to indicate the binary operation in G and H, leaving the reader to determine which operation is intended from context. Using this convention, the main defining property of a homomorphism would be simply $w(fg) = w(f)w(g)$ for all f and g in G.

Homomorphisms are a rich source of subgroups.

For instance if $w \in Hom(G, G)$ the set $\mathbf{Fixed_w} = \{\, g \mid w(g) = g \,\}$ is a subgroup of G, called the group of **fixed points of w**.

Suppose $w \in Hom(G, H)$. $\mathbf{Ker(w)}$ is defined to be $w^{-1}(e_\odot)$ and called the **kernel of w**. It too is a subgroup of G.

13.4. ***Exercise.*** *(i) With w as above, $Ker(w)$ is normal in G.*

(ii) If K is any subgroup of H then $w^{-1}(K) = \{\, w^{-1}(f) \mid f \in K \,\}$ is a subgroup of G containing $Ker(w)$.

(iii) Whenever K is normal in H then $w^{-1}(K)$ is normal in G.

(iv) On the other hand, if J is a subgroup of G then $w(J) = \{\, w(g) \mid g \in J \,\}$ is a subgroup of H. $\mathbf{Image(w)}$*, defined to be the range $w(G)$ of the function w, is an important case. The range is usually called, in this context, the* ***image of*** *w.*

(v) If w is onto H (that is, $Image(w) = H$) then $w(J)$ is normal in H whenever J is normal in G and contains $Ker(w)$. So if w is onto H it provides a correspondence between normal subgroups of H and those normal subgroups of G which contain $Ker(w)$.

(vi) If w has an inverse function then the inverse is also a homomorphism. In that case w is called a ***group isomorphism.*** *The groups involved, $(G, \otimes)$ and $(H, \odot)$, are called* ***isomorphic groups*** *by virtue of the existence of a group isomorphism between them.*

(vii) If w is any homomorphism onto H, w is an isomorphism if and only if $Ker(w) = \{e_\otimes\}$.

(viii) If H is a subgroup of G and $g \in G$ then gHg^{-1} is isomorphic to H. In particular, if $g, h \in G$ then $Cyclic(g)$ is isomorphic to $h\,Cyclic(g)\,h^{-1} = Cyclic(hgh^{-1})$.

(ix) If w is a homomorphism, the factor group $G/Ker(w)$ is isomorphic to $Image(w)$.

(x) Also, if N is any normal subgroup of G then the function $w\colon G \to G/N$ defined by $w(g) = gN$ is a homomorphism and $Ker(w) = N$. This means that normal subgroups are precisely the kernels of group homomorphisms.

(xi) If N is a normal subgroup of G and $\widetilde{K}$ is a subgroup of G/N then the union of the members of $\widetilde{K}$ is a subgroup K of G and $|K| = |N|\,|\widetilde{K}|$.

(xii) If N is a normal subgroup of G and K is any subgroup of G containing N then N is normal in K and $\widetilde{K} = K/N$ is a subgroup G/N.

(xiii) If N and K are both normal subgroups of G and $N \cap K = \{ e \}$ we saw in Exercise 13.1 that every element of N commutes with every element of K (though the group NK need not be abelian.) Show that under these conditions $N \times K$ is isomorphic to NK.

Collecting some results from above we have, for homomorphism $w\colon G \to H$, and any subgroup K of G containing the kernel of w

$$|G| = |Ker(w)|\,|Image(w)| = [G : K]\,|K| = [G : K]\,|Ker(w)|\,|w(K)|.$$

13.5. ***Exercise.*** *Consider Exercises 12.5, 13.2 and 13.4 (xii) and conclude that if subgroup K has finite index in group G then G is not the union of conjugates of K.*

13.6. ***Exercise.*** *It is possible for A to be normal in B and B to be normal in C but with A not normal in C. An example of this is provided in SquareSym:*

$$A = \{ e, c \} \qquad \text{and} \qquad B = \{ e, -e, c, -c \}.$$

SquareSym and B also provide an example of the following phenomenon: B is abelian and normal in SquareSym and SquareSym/B is abelian but SquareSym itself is not abelian.

13.7. ***Exercise.*** *Suppose M and N are normal subgroups of the group G and $M \subset N \subset G$. Then M is normal in N and N/M is normal in G/M and $(G/M)/(N/M)$ is isomorphic to G/N.*

13.8. ***Exercise.*** *Let G be the abelian product group with set $(\mathbb{R} - \{0\}) \times (\mathbb{R} - \{0\})$ and ordinary multiplication on each factor. Let N be the subgroup $(0, \infty) \times (0, \infty)$. Let $M = \{\big(x, \frac{1}{x}\big) \mid x \in (0, \infty)\}$. Show that G/N is isomorphic to the subgroup $\{(1, 1),\ (-1, 1),\ (1, -1),\ (-1, -1)\}$ of G. Can you identify subgroups of G to which G/M and N/M are isomorphic? (hint: $\{(x, y) \in G \mid y = \pm x\}$ is a subgroup of G.)*

A group is called **simple** if it has no nontrivial proper normal subgroups. A simple group only has two types of homomorphisms: those that are one-to-one, and therefore isomorphisms onto their image, and the constant homomorphisms.

13.9. ***Exercise.*** *(i) If G is a group, $Hom(G, G)$ is a monoid with composition as the operation.*

(ii) If G is a group and $(H, +)$ an abelian group, $Hom(G, H)$ is itself a group with operation, also denoted $+$, given by $(f + g)(a) = f(a) + g(a)$ for each $f, g \in Hom(G, H)$ and $a \in G$.

If G is a group let $\mathbf{Aut(G)} = Perm(G) \cap Hom(G, G)$. This is the set of group isomorphisms of G onto G. Members of $Aut(G)$ are called **automorphisms of G**.

13.10. ***Exercise.*** *Show that $Aut(G)$ is a group with composition.*

For $g \in G$ define $\theta_{\mathbf{g}}$ to be the function $\theta_g\colon G \to G$ given by $\theta_g(h) = ghg^{-1}$. Show that $\theta_g \in Auto(G)$. Automorphisms of this kind are called **inner automorphisms.** The set of all these inner automorphisms is denoted $\mathbf{Inner(G)}$.

13.11. ***Exercise.*** *$Inner(G)$ is a normal subgroup of $Aut(G)$.*

Outer automorphisms are nontrivial members of the group $Aut(G)/Inner(G)$.

A subset S of a group G is called a **characteristic subset of G** if it is invariant under all automorphisms of G: that is, $\phi(S) = S\ \forall \phi \in Aut(G)$. If S is a subgroup and also characteristic it is called a **characteristic subgroup of G**. Since normal subgroups are precisely those invariant under all inner automorphisms, all characteristic subgroups are normal.

13.12. ***Exercise.*** *(i) Any subgroup that is the only subgroup of its order is a characteristic subgroup. The center of a group and the commutator subgroup are both characteristic subgroups. The smallest group containing all the torsion elements of a group is characteristic, as is the set of torsion elements itself. The set of elements which have a particular order is characteristic, as is the set of elements of infinite order.*

(ii) Show that Quat has a characteristic subgroup of order 2*. It has cyclic subgroups of order* 4*, which are normal but not characteristic.*

(iii) Suppose N is normal in finite group G and that $|N|$ and $|G/N|$ share no common factor. Then N is characteristic, and if H is any subgroup of G for which $|G/N| = |H|$ then $G = NH$.

13.13. ***Exercise.*** *Suppose H is a subgroup of G.*

(i) If $gHg^{-1} \subset H\ \forall g \in G$ then H is normal in G.

(ii) If H is finite and $gHg^{-1} \subset H$ for some $g \in G$ then $gHg^{-1} = H$.

(iii) Let $G = Perm(\mathbb{Z})$ and define, for $i \in \mathbb{Z}$, the set H_i to be those members ϕ of G for which $\phi(n) = n\ \forall n \geq i$. In other words, a permutation is in H_i exactly when it fixes all integers from i onward. Clearly, each H_i is a subgroup of G and H_i is properly contained in H_{i+1} for every i.

Let σ be the right shift permutation defined by $\sigma(n) = n + 1$ for all $n \in \mathbb{Z}$.

If $\phi \in H_1$ and $n \geq 0$ then

$$\sigma^{-1} \circ \phi \circ \sigma(n) = \sigma^{-1} \circ \phi(n+1) = \sigma^{-1}(n+1) = n.$$

This means $\sigma^{-1} \circ \phi \circ \sigma \in H_0$.

Conclude that (ii) is false without the finiteness condition on H.

14. Central Series

If G is a group, recall that $Z(G)$ is the center of G. Define $\mathbf{C_0(G)} = \{\, e \,\}$ and $\mathbf{C_1(G)} = Z(G)$. $C_1(G)$ is normal in G. The group $G/C_1(G)$ itself has center $Z\left(G/C_1(G)\right)$. Define $\mathbf{C_2(G)}$ to be the union of the cosets comprising this normal subgroup of $G/C_1(G)$. So $C_2(G)$ is itself normal. In general, having found $C_i(G)$ define $\mathbf{C_{i+1}(G)}$ to be the union of those cosets comprising $Z\left(G/C_i(G)\right)$. This serves to define $C_i(G)$ for each integer $i \geq 0$.

The sequence of normal subgroups of G formed in this way is called the **upper or (synonymously) ascending central series** and the groups themselves are referred to as **the second center of G**, **the third center of G** and so on.

$$C_0(G) \subset C_1(G) \subset \cdots \subset C_i(G) \subset \cdots$$

If G is finite this process must terminate after a finite number of steps. If it terminates at G the group is said to be **nilpotent**.

If G is a group, let $\mathbf{G^{(0)}} = G$ and for $i \geq 0$ let $\mathbf{G^{(i+1)}}$ denote the smallest subgroup containing all finite products of elements $aba^{-1}b^{-1}$ for $a, b \in G^{(i)}$.

$G^{(1)}$ is called the **commutator subgroup of G**. The sequence of these subgroups is called the **derived series of G**.

Let $G_{(i)} = G^{(i)}$ and for $i = 0$ and $i = 1$ and for $i > 1$ let $G_{(i)}$ be the subgroup generated by all $aba^{-1}b^{-1}$ for $b \in G_{(i-1)}$ and $a \in G$.

The sequence of these $G_{(i)}$ called the **lower central or, synonymously, the descending central series of G**.

14.1. ***Exercise.*** *(i) $G^{(i)} \subset G_{(i)}$ and $G_{(i+1)} \subset G_{(i)}$ and $G^{(i+1)} \subset G^{(i)}$ for each i.*

(ii) Each $G^{(i)}$ is normal in G. Each $G_{(i)}$ is normal in G.

(iii) If H is normal in G, the group G/H is abelian exactly when $G^{(1)} \subset H$.

From the last exercise, we see that both $G^{(i)}/G^{(i+1)}$ and $G_{(i)}/G_{(i+1)}$ are always abelian and, in particular, $G/G^{(1)}$ is abelian, called the **abelianization of G**.

G is said to be **solvable** if $G^{(i)} = \{e\}$ for some i.

14.2. ***Exercise.*** *Suppose G is a finite group. If G is abelian and simple it must be of prime order. If G is nonabelian and simple it has trivial center and $G^{(1)} = G$.*

Solvability and nilpotency (and simplicity) are core building blocks for the classification scheme for all finite groups. Though we do not dwell on it in these notes, the complete description of the finite simple groups is one of the major achievements of group theory, and of mathematics as a whole.

14.3. ***Exercise.*** *(i) $G_{(i)} = \{e\}$ for some i if and only if G is nilpotent.*

(ii) Every nilpotent group is solvable. However the converse is not true. No nontrivial group with trivial center can be nilpotent, so any "centerless" solvable group provides a counterexample. See Exercise 17.2.

***Nilpotent: each sbgp properly contained in normalizer, all finite nilpotent are direct prod of sylow subgps

15. An Excursion into Arithmetic

15.1. ***Exercise.*** *We suppose n is an integer, and not equal to $0, 1$ or -1.*

*(i) $n\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$ with addition and $\mathbb{Z}/(n\mathbb{Z})$ is isomorphic to Rot_n for each integer $n \geq 2$. The group $\mathbb{Z}/(n\mathbb{Z})$ is also denoted $\mathbb{Z}_\mathbf{n}$, called the **integers mod n**. The group operation is called **addition mod n.** When $a + n\mathbb{Z} = b + n\mathbb{Z}$ the notation $\mathbf{a \equiv b \bmod n}$ is sometimes used. If $a \equiv b \bmod n$, the integer a is said to be **congruent to b mod n**.*

*(ii) Define multiplication in $\mathbb{Z}_n$ by $(s + n\mathbb{Z})(t + n\mathbb{Z}) = st + n\mathbb{Z}$. Show that this operation is well defined and makes $\mathbb{Z}_n$ into a monoid. This operation is called **multiplication mod n.***

*(iii) A nonzero integer k is called a **factor** of a nonzero integer n if there is an integer j with $n = jk$. An integer $n > 1$ is called a **prime integer** if whenever*

m is an integer and $1 < m < n$ there are integers j and k with $jm + kn = 1$. An integer $n > 1$ is called ***composite*** *if it is not prime.*

Two nonzero integers m and n are called ***relatively prime*** *if there are integers j and k so that $jm + kn = 1$.*

Suppose m and n are positive integers. Let $H = \{\ jm + kn \mid j, k \in \mathbb{Z}\ \}$. H is an additive group. H contains a least positive member r. r must be a factor of every nonzero member of H including m and n. Show that $H = r\mathbb{Z}$. Note: m and n can have no larger common factor. r is the greatest common factor of m and n.

(iv) Show that two nonzero integers are relatively prime if and only if they have no common factor other than ± 1. (hint: Use induction on n for $1 < m < n$.) So a positive integer is prime if and only if it has no positive factors except itself and 1. Composite numbers, on the other hand, have nontrivial factorizations.

(v) If n is any integer bigger than 1 show that there is a unique positive integer k and a unique list of primes $p_1, \ldots, p_k$ with $p_i \leq p_{i+1}$ for $i = 1, \ldots, k-1$ and $n = p_1 \cdots p_k$. In words, any integer bigger than 1 can be factored in one and only one way as a product of prime numbers of nondecreasing size. (hint: Use induction on n.)

(vi) Conclude from (v) that if n is any integer bigger than 1 there is a unique positive integer L and a unique list of positive integers $k_1, \ldots, k_L$ and a unique list of primes $p_1, \ldots, p_L$ with $p_i < p_{i+1}$ for $i = 1, \ldots, L-1$ and $n = (p_1)^{k_1} \cdots (p_L)^{k_L}$.

15.2. ***Exercise.*** *(i) For fixed $n > 1$, let $j_1, \ldots, j_{\phi(n)}$ denote the list, in order, of all positive integers less than n and relatively prime to n. This list is not "empty:" at least 1 is on the list. Let $\mathbf{RelPrime_n}$ denote $\{\ j_k + n\mathbb{Z} \mid 1 \leq k \leq \phi(n)\ \}$. Show that $RelPrime_n$ is an abelian group of order $\phi(n)$ with multiplication mod n. The function ϕ is called the* ***Euler ϕ function*** *and pops up in surprising places.*

(ii) We conclude from Lagrange's Theorem that if m and n are relatively prime integers and if $n > 1$ then $m^{\phi(n)} \equiv 1$ mod n. This result is called ***Euler's Theorem****. The special case of prime n is called* ***Fermat's Little Theorem****.*

(iii) Suppose m and n are relatively prime integers and $n > 1$. Let $j_1, \ldots, j_{\phi(n)}$ denote the list, in order, of the positive integers less than n and relatively prime to n. Then $RelPrime_n = \{\ mj_k + n\mathbb{Z} \mid 1 \leq k \leq \phi(n)\ \}$.

15.3. ***Exercise.*** *(i) If p is prime show that $\phi(p) = p - 1$ and $\phi(p^2) = p(p-1)$. More generally, show that $\phi(p^k) = p^k - p^{k-1}$ for integer $k \geq 1$.*

(ii) For relatively prime numbers m, n both bigger than 1 show that $\phi(mn) = \phi(m)\phi(n)$. (hint: consider the case where m is a prime power.)

(iii) For integer n bigger than 1 let $n = (p_1)^{k_1} \cdots (p_L)^{k_L}$ for positive integers $k_1, \ldots, k_L$ and primes $p_1, \ldots, p_L$ with $p_i < p_{i+1}$ for $i = 1, \ldots, L-1$. Show that

$$\phi(n) = \left((p_1)^{k_1} - (p_1)^{k_1 - 1}\right) \cdots \left((p_L)^{k_L} - (p_L)^{k_L - 1}\right).$$

15.4. ***Exercise.*** *This exercise constitutes a tiny introduction to* ***public key cryptography****.*

There are several of these systems in use, and they are designed to conceal data from unauthorized access particularly during the transmission of this data from

one place or time to another. We discuss some of the ideas used in the ***RSA cryptosystem****.*

The flavor of this exercise will be quite different from other exercises you have seen in these notes. In particular, terms such as "random," "high probability" and "unlikely," upon whose meaning the security of these systems hinge, are left undefined.

(i) To get started, we must produce two large prime numbers p and q. The level of security in the encryption scheme is dependent on their size, so we require them both to have binary representation longer than some predetermined number of binary digits. A candidate prime j of proper size is ***randomly*** *selected. If j is prime then $m^j \equiv m \bmod j$ for all m with $2 \leq m < j$. Even if j is not prime, it still could happen that $m^j \equiv m \bmod j$ for any, or even all of, these values of m. But this is* ***very unlikely*** *if j is large and this probability can be estimated. Candidate primes j are tested one after another until one is found that "passes this test," called the* ***Fermat Test****, for a sufficient number of different prime numbers m. When that happens j is simply assumed to be prime: an "Industrial Grade Prime" if not an actual prime. It is nowadays not hard to produce numbers with binary representation having length beyond a thousand digits and which have an* ***extremely high probability*** *of being prime. We will choose for purposes of illustration $p = 101$ and $q = 107$.*

(ii) Multiply these: $n = pq$ and calculate $\phi(n) = (p-1)(q-1)$. In our case $n = 10807$ and $\phi(10807) = 10600$.

(iii) Select any w with $0 < w < \phi(n)$ and with w and $\phi(n)$ relatively prime. That means there are integers d and k with $wd + k\phi(n) = 1$. So $wd \equiv 1 \bmod \phi(n)$. We can (and do) require that $0 < d < \phi(n)$. For our example, we pick $w = 11$ and calculate $d = 2891$. At this point the key creator destroys all record of p, q, k and $\phi(n)$.

(iv) The key creator gives the ***private key*** *d to the intended recipient of the message* ***only*** *and makes public the* ***public key*** *consisting of the two numbers w and n. The key creator, if different from the private key holder, should then destroy all record of d.*

If the public could factorize n it would know $\phi(n)$ and therefore the private key d. The key to the security of this system is ***only the apparently intractable problem of factoring large integers****. It seems that no one knows how to factorize n without exhaustively examining the entire* ***keyspace*** *to determine factors: all numbers, essentially, up to $\sqrt{n}$. To factorize an integer without small factors whose binary representation contains 128 digits would seem to require around six months if potential factors were checked at a rate of 10^{12} per second. Using 2048 digits creates a keyspace more than 10^{250} times larger. The "exhaustion" method of factorization, I think it is safe to say, cannot crack such an integer during the lifetime of our species. However no one has proven that factorization cannot be accomplished by some alternative, faster, method. This would break the RSA cryptosystem. If you discover such a method you are well advised to consider carefully who to tell, and how to tell them.*

(v) Let's suppose we want to send a secret message to the holder of the private key. For convenience suppose the secret message is the positive integer m with m

less than the minimum size restriction we have for p and q. So m and n are relatively prime. This means that $m^{\phi(n)} \equiv 1$ mod n. Any message can be converted by a non-secure encoding method into an integer and broken up into pieces, if necessary, where each piece is small enough to satisfy this condition. The number m is called the ***plaintext*** *and it is the goal of the cryptographic system to protect the plaintext from public exposure but allow the holder of the private key to recover the plaintext. For our purposes let $m = 100$.*

(vi) Calculate a number c with $c \equiv m^w$ mod n. The number c is called the ***ciphertext*** *and is sent openly to the recipient. We can (and do) require that $0 < c < n$. This process is called* ***encryption****. In our case $c = 2120 \equiv 100^{11}$ mod 10807.*

(vii) The holder of the private key d takes c and calculates a number $\overline{m}$ with $0 < \overline{m} < n$ and $\overline{m} \equiv c^d$ mod n.

$\overline{m} \equiv c^d$ mod n so $\overline{m} \equiv m^{wd}$ mod n so $\overline{m} \equiv m^{-k\phi(n)+1}$ mod n so $\overline{m} \equiv m$ mod n.

This means $\overline{m} = m$ and the message is recovered by its intended recipient. This process is called ***decryption****. In our example 100 is the smallest positive integer with $100 \equiv 2120^{2891}$ mod 10807.*

We should note that there are fast methods to perform all of the necessary calculations above for integers whose lengths are well beyond a thousand binary digits.

(viii) How would you calculate 2120^{2891} mod 10807 on an ordinary scientific calculator? (hint: $2891 = 1 + 2 + 8 + 64 + 256 + 512 + 2048$. If set up properly, the calculation can be performed in fewer than twenty manual "mod" operations on a calculator, each taking around thirty seconds.)

(ix) There is complete symmetry between private and public key. In the example above we used a public key to encrypt information only one private key can decrypt. But a private key could be used to encrypt information that only the paired public key could decrypt. You as a ciphertext recipient want to be sure the message you decrypt actually came from the right person, and is not a fake message. After all, anyone can use your public key to create a message only you can decrypt. How would you modify the encryption system so you can be sure only the expected person could have sent it? This is the process of creating a ***digital signature*** *to verify the authenticity of documents, and is a vital part of any cryptosystem. (hint: You may create another key pair for your confederate.)*

16. Action

Sometimes a one-to-one homomorphism $f\colon G \to H$ is called an **embedding**: specifically, an **embedding of G in H**. One usually uses this vocabulary to encourage identification of G with $Image(f)$, a subgroup of H. In the following exercise we see that any group can be embedded in a permutation group.

16.1. ***Exercise.*** *If G is a group and $g \in G$ define $\lambda_g \in Perm(G)$ by $\lambda_g(h) = gh$ $\forall h \in G$. λ_g is called the* ***left action of*** **g** ***on*** **G.** *We will denote the set of all permutations formed in this way by Λ_G. This set is a group with composition, a subgroup of $Perm(G)$.* ***Cayley's Theorem*** *asserts that G and Λ_G are isomorphic groups. The point is that any group is isomorphic to a subgroup of a permutation group. Prove Cayley's Theorem.*

More generally, an **action of a group H on a nonempty set S** is a function $\odot : H \times S \to S$ for which $e \odot x = x$ and $f \odot (g \odot x) = (fg) \odot x \ \forall x \in S$ and $f, g \in H$, and where e is the identity in H. Given an action, H is said to **act on S**.

$\odot$ can be associated in a unique way with a homomorphism $\phi\colon H \to Perm(S)$ defined by $\phi(h)(s) = h \odot s$, and any homomorphism of this kind can be used to produce a unique action by the reverse process.

Any such homomorphism is called a **representation of H on S**.

If the kernel of this homomorphism is trivial (it contains only the identity) the representation is called **faithful**. Any faithful representation provides an embedding of H in $Perm(S)$.

We have already seen and used several representations, though we did not use the vocabulary. The connection will be explored in several of the exercises below.

16.2. ***Exercise.*** *If G is a group the function $\odot\colon \mathbb{Z} \times G \to G$ defined by $n \odot g = g^n$ is an action of $\mathbb{Z}$ (with addition) on G. If G has any element of infinite order this representation is faithful. If G has finite order the associated representation is not faithful. But if G is finite there is a least positive integer k for which $g^k = e$ for all $g \in G$, and then $\otimes\colon \mathbb{Z}_k \times G \to G$ given by $(n + k\mathbb{Z}) \otimes g = g^n$ is well defined, an action, and the induced representation of the additive group $\mathbb{Z}_k$ is faithful.*

16.3. ***Exercise.*** *Create an action of $Inner(G)$ on a group G. More generally, show that if S is a set and H is any subgroup of $Perm(S)$ then H can be made to act on S in a natural way. The associated representation is faithful.*

For any action of a group H on a set S and any $x \in S$ define the **orbit of x** to be $\mathbf{Orbit}_{\odot}(\mathbf{x}) = \{\ g \odot x \mid g \in H\ \}$ and the **stabilizer of x** to be $\mathbf{Stabilizer}_{\odot}(\mathbf{x}) = \{\ g \in H \mid g \odot x = x\}$. Sometimes $Stabilizer_{\odot}(x)$ is called the **isotropy group of x**. The kernel of the representation induced by the action is the intersection of all these isotropy groups.

Let $\mathbf{Orbits}_{\odot} = \{\ Orbit_{\odot}(x) \mid x \in S\ \}$ and $\mathbf{Single}_{\odot} = \{\ Orbit_{\odot}(x) \mid x \in S$ and $Orbit_{\odot}(x) = \{x\}\ \}$ and $\mathbf{Multiple}_{\odot} = \{\ Orbit_{\odot}(x) \mid x \in S$ and $Orbit_{\odot}(x) \neq \{x\}\ \}$.

$x \in S$ is called a **fixed point** for the action if $Orbit(x)$ contains only x.

As usual, when there is only one action around the "$\odot$" subscript will be suppressed. An example of this convention in use is the following sentence: $Single \cup Multiple = Orbits$ is a partition of S and each $Stabilizer(x)$ is a subgroup of H.

16.4. ***Exercise.*** *Verify that $Single \cup Multiple$ is a partition of S and each $Stabilizer(x)$ is a subgroup of H. Then show that $[H : Stabilizer(x)] = |Orbit(x)|$.*

An action is called **transitive** if for some (and hence every) $x \in S$, $Orbit(x) = S$.

Members of the intersection of the isotropy groups of all the elements in a specified orbit are precisely those members of H that act as the identity on the orbit, though they may well move members of S *not* in this orbit. This subgroup is

$$\{\ g \in H \mid ghx = hx\ \forall h \in H\ \} = \{\ g \in H \mid h^{-1}ghx = x\ \forall h \in H\ \}$$

On the other hand, the normal core of $Stabilizer(x)$ is the intersection of all conjugates of $Stabilizer(x)$. This intersection is

$$\begin{aligned} core_H(\, Stabilizer(x)\,) &= \{\, g \in H \mid g \in h\, Stabilizer(x)\, h^{-1} \ \forall h \in H \,\} \\ &= \{\, g \in H \mid h^{-1}gh \in Stabilizer(x) \ \forall h \in H \,\} \end{aligned}$$

These two subgroups are the same: the normal core of $Stabilizer(x)$ is exactly those group members that act as the identity on $Orbit(x)$.

In particular, for a transitive action, the normal core of *the* isotropy group (there is only one in this case) is the kernel of the representation of H given by this action.

An action can be used to induce another action on a set smaller than S. If T is any orbit, or any union of orbits, the restriction of $\odot : H \times S \to S$ to domain $H \times T$ is onto T and also an action. Isotropy groups do not change, but the kernel of the new representation might be bigger (there are fewer isotropy groups when $T \neq S$) so "faithfullness" need not be preserved.

16.5. ***Exercise.*** *If A is a nonempty subset of a group G let $S = \{\ gA \mid g \in G\}$. Suppose H is a subgroup of G.*

Then $h \odot (gA) = (hg)A$ defines an action of H on S. The associated representation need not be faithful.

16.6. ***Exercise.*** *If H is any subgroup of G then $h \odot g = hg$ is a transitive action of H on G. H is said to act on G by* ***translation.*** *The associated representation is faithful.*

16.7. ***Exercise.*** *Suppose H is a subgroup of group G and S is the set of left cosets of H in G. For each $x \in G$ define $\phi(x) \in Perm(S)$ by $\phi(x)(cH) = xcH$ for all $cH \in S$.*

(i) Show that this actually defines a function on S and that this function is in $Perm(S)$ (that is, show $xcH = xdH$ if and only if $cH = dH$, and also that each $\phi(x)$ is onto S.)

(ii) ϕ is a representation of G.

(iii) $Ker(\phi) = \{x \mid xcH = cH \ \forall c \in G\} = \{x \mid c^{-1}xcH = H \ \forall c \in G\}$. This set is the intersection of all conjugates of H in G. It is $core_G(H)$, the largest normal subgroup of G contained in H. So the representation of G is faithful exactly when H contains no subgroups normal in G other than $\{e\}$. If G happens to be simple, this is guaranteed.

Cayley's Theorem follows from the case $H = \{e\}$. Finding larger H with no nontrivial subgroups normal in ***finite*** *G provides an embedding of G in a permutation group smaller than $Perm(G)$.*

(iv) $|G| = |Ker(\phi)|\,|Image(\phi)|$. $Ker(\phi)$ is a subgroup of H and $Image(\phi)$ is a subgroup of $Perm(S)$. So if G is finite $|Ker(\phi)|$ divides $|H|$ and also $|Image(\phi)|$ divides $|Perm(S)| = [G : H]\,!$.

If $|G| > [G : H]\,!$ we can use this to deduce that there is a nontrivial subgroup of H which is normal in G.

A bit less crudely, if $|G|$ has prime power factor p^m exceeding the largest power p^j of p dividing $[G : H]\,!$ we can deduce that there is a nontrivial subgroup K of H

which is normal in G and which has cardinality divisible by p^{m-j}. This conclusion holds (for the same K) for each prime power divisor of $|G|$.

(v) Suppose $|G| = 99$ and $|H| = 11$. Since 99 is not a factor of $9\,!$ we know that H must have a nontrivial subgroup normal in G. Since 11 is prime, that means $|H|$ itself is normal.

(vii) If G is finite with subgroup H and $[G : H] = p$ where p is the smallest prime which is a factor of $|G|$ then H is normal. So, for instance, if G has a subgroup H of index 2 then H is normal.

16.8. ***Exercise.*** *If H and K are subgroups of G let $S = \{\ gKg^{-1} \mid g \in G\}$.*

Then $h \odot (gKg^{-1}) = (hg)K(hg)^{-1} = hgKg^{-1}h^{-1}$ is an action of H on S. H is said to ***act on*** **S** ***by conjugation.***

We will denote the corresponding representation by $\mu\colon H \to Perm(S)$. An element h of H is in the kernel of the representation exactly when

$$\begin{aligned} hg\,K\,g^{-1}h^{-1} = gKg^{-1} \quad \forall g \in G \\ \text{which is equivalent to} \quad g^{-1}hg\,K\,g^{-1}h^{-1}g = K \quad \forall g \in G \\ \text{which means} \quad g^{-1}hg \in N(K,G) \quad \forall g \in G \\ \text{or, equivalently,} \quad h \in g\,N(K,G)\,g^{-1} \quad \forall g \in G. \end{aligned}$$

So $Ker(\mu) = H \cap core_G(N(K,G))$. The representation is faithful when H contains no members (other than e) of the normal core of $N(K,G)$.

Recall that $|S| = [G : N(K,G)]$ and $|H| = |Ker(\mu)|\,|Image(\mu)|$. We see that $Ker(\mu)$ must divide both $|H|$ and $|core_G(N(K,G))|$, the latter divides $|N(K,G)|$ and $|Image(\mu)|$ divides $|Perm(S)| = [G : N(K,G)]\,!$.

16.9. ***Exercise.*** *(i) If H is a subgroup of G then $h \odot g = hgh^{-1}$ for $h \in H$ and $g \in G$ prescribes an action of H on G.*

H is said to ***act on*** **G** ***by conjugation.***

The kernel of the corresponding representation is $H \cap Z$ where $Z = Z(G)$ is the center of G. The representation is ***trivial*** *(that is, its kernel is H) if $G = C(H,G)$. The representation is faithful if no element of H except e commutes with every member of G. Let $\mu\colon H \to Perm(G)$ denote this representation.*

(ii) With H and G and Z as above, let $S = \{\, k\,Z \mid k \in H\,\}$. Recall that $|S| = [HZ : Z] = [H : H \cap Z]$ which may be, possibly, much smaller than $|G|$.

The action defined for k and h in H by $h \otimes k\,Z = hk\,Z$ induces a representation $\theta\colon H \to Perm(S)$. Find $Ker(\theta)$.

(iii) Prove that $Image(\theta)$ is isomorphic to $Image(\mu)$.

The following exercise expands on the method of Exercise 11.4 and presages some of the discussions of the Class Equation and Cauchy's Theorem found below.

16.10. ***Exercise.*** *Suppose $|G|$ is finite and divisible by 3. Complete the argument below to conclude that there are at least three members of G whose cube is e.*

Let S denote the set of all members of $G \times G \times G$ of the form $(g, h, h^{-1}g^{-1})$. So $|S| = |G|^2$ and, in particular, $|S|$ is divisible by 3. Consider sets of the form

$K(g,h) = \{\,(g,h,h^{-1}g^{-1}),\,(h,h^{-1}g^{-1},g),\,(h^{-1}g^{-1},g,h)\,\}$ for $h,g \in G$. It is possible that $K(g,h)$ contains a single ordered triple: for instance $K(e,e)$ does. By examining cases we can see that if $K(g,h)$ does not contain 3 distinct ordered triples then $g = h$ and $g = g^{-2}$ so $g^3 = e$ and it has but one. It is also easy to show that, for any $K(g,h)$ and $K(a,b)$ either $K(g,h) = K(a,b)$ or $K(g,h) \cap K(a,b) = \varnothing$. So these sets form a partition of S and each has cardinality 1 or 3. At least one class has cardinality 1. If all the rest had cardinality 3 we would conclude that the cardinality of G had remainder 1 after division by 3, contrary to assumption. So there are at least three classes of cardinality 1. So there is a member g of G other than e with $g^3 = e$. For any such g, the member g^2 of G is another.

Suppose S is a finite set and G is a group acting on S. Let A denote a set consisting of a selection of one element of each member of $Multiple$ and let B denote the set of fixed points for the action. Then

$$\begin{aligned} |S| &= \sum_{x\in A\cup B} |Orbit(x)| \\ &= \sum_{x\in A\cup B} [G : Stabilizer(x)] \\ &= |Single| + \sum_{x\in A} [G : Stabilizer(x)] \end{aligned}$$

where every summand in the sum on the far right in the last line exceeds one and, if $|G|$ is finite, is a factor of $|G|$. This decomposition of $|S|$ into the sum of the cardinal numbers of its orbit classes under an action is very useful. Some of the most basic structure and classification theorems for finite groups use this decomposition repeatedly. It is called the **Class Equation.**

16.11. ***Exercise.*** *Suppose G is a finite group of order p^n for prime p acting on any finite set S. So*

$$|S| - |Single| = \sum_{x\in A} [G : Stabilizer(x)]$$

where A is formed as a selection of one member from each class in $Multiple$. Since p divides every term in the sum on the right, we conclude: $|Single| \equiv |S| \bmod p$. So if p does not divide $|S|$ the action has fixed points.

Let H be a subgroup of the group G, and let S consist of all the subgroups of G conjugate to H: that is, $S = \{\, gHg^{-1} \mid g \in G \,\}$.

Let G act on S by conjugation. This action is transitive. $Stabilizer(H) = \{\, g \in G \mid gHg^{-1} = H \,\} = N(H,G)$. The Class Equation now gives the number of groups conjugate to H as

$$|S| = |Orbit(H)| = [G : Stabilizer(H)] = [G : N(H,G)]$$

reprising a result from Exercise 12.4. Note that $H \subset N(H,G)$ so if G is finite, the number of conjugates is $\frac{|G|}{|N(H,G)|}$ which cannot exceed $\frac{|G|}{|H|}$.

Let the finite group G act on itself by conjugation. So each $Stabilizer(x) = N(x,G)$, the set of members of G which commute with x. The set of fixed points for this action is precisely the center $Z(G)$ of G. The Class Equation gives

$$|G| = |Z(G)| + \sum_{x\in A} |Orbit(x)| = |Z(G)| + \sum_{x\in A} [G : N(x,G)] = |Z(G)| + \sum_{x\in A} \frac{|G|}{|N(x,G)|}$$

where A is a selection of one element of each member of $Multiple$, if any.

16.12. ***Exercise.*** *(i) Use the equation above to show that if $|G| = p^n$ for some prime number p and positive integer n then G has nontrivial center.*

(ii) If $|G| = p^2$ then G is abelian. (hint: if G is not then $|Z(G)| = p$ so there is x in G with $x \notin Z(G)$. But then the fact that $Z(G) \subset N(x, G)$ implies $N(x, G) = G$, contradicting choice of x.)

The very short proof presented here of the classic result below was created by **J. H. McKay** in 1959.

16.13. ***Proposition.*** ***(Cauchy's Theorem)*** *Suppose G has finite order n, which has prime factor p. Then the number of distinct elements in G whose pth power is the identity of G is a positive integer multiple of p.*

Proof. Let $H = Cyclic(\sigma)$, the subgroup of the permutation group $\mathcal{S}_p$ generated by the permutation σ defined by $\sigma(i) = i + 1$ for $i = 1, \ldots, p - 1$ and $\sigma(p) = 1$. So $|H| = p$.

Consider $W = G \times \cdots \times G$, the product of G with itself p times. A member $x \in W$ has the form $x = (x_1, x_2, \ldots, x_p)$. Let S be the set of those members of W with $x \in S$ if and only if $(x_p)^{-1} = x_1 x_2 \cdots x_{p-1}$. In other words, the last component is the inverse of the product of the first $p - 1$ components. So $|S| = n^{p-1}$, and p is a factor of this number since it is a factor of n.

If $x = (x_1, x_2, \ldots, x_p) \in S$ then σx, which we define to be

$$\sigma x = (x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(p)}) = (x_2, \ldots, x_p, x_1)$$

is in S too, as seen in the following calculation:

$$(x_2 \cdots x_p)^{-1} = x_p^{-1} x_{p-1}^{-1} \cdots x_2^{-1} = x_1 x_2 \cdots x_{p-1} x_{p-1}^{-1} \cdots x_2^{-1} = x_1.$$

By extension to powers of σ, we have an action of H on S. By the remark above, $|Single| \equiv |S| \ mod\ p$ where $Single$ consists the orbits of the fixed points of this action. Since p is a factor of $|S|$ it is a factor of $|Single|$.

But $Single$ is not empty: $\{(e, e, \ldots, e)\} \in Single$, at least, where e is the identity in G, so the cardinality of $Single$ is a positive integer multiple of p. Any orbit $\{x\}$ in $Single$ is of the form $\{(a, a, \ldots, a)\}$ and the product of the entries of *any* member of S is e: that is, $a^p = e$. □

17. Facts about Permutations

Let's examine permutation groups a bit more closely. A **cycle** is a permutation P of nonempty set S for which there is a finite list of *distinct* elements $s_1, \ldots, s_n$ with $P(s_i) = s_{i+1}$ for $i = 1, \ldots, n - 1$ and $P(s_n) = s_1$ but with $P(s) = s$ for all other elements of S. Since this particular cycle involves n elements of S it is called an n-cycle. It is often represented in the form $(s_1, s_2, \ldots, s_{n-1}, s_n)$. This representation is not unique: $(s_2, \ldots, s_{n-1}, s_n, s_1)$ is the same cycle. Of particular importance here are 2-cycles, also known as **transpositions**. The cycle shown here is the product (that is, the composition) of 2-cycles

$$(s_1, s_2, \ldots, s_n) = (s_1, s_n)(s_1, s_{n-1}) \cdots (s_1, s_3)(s_1, s_2).$$

So any n-cycle can be represented as a product of n of these 2-cycles.

Two cycles are called **disjoint** if they do not involve any of the same members of S.

We now suppose P is any permutation on S. The group $Cyclic(P)$ acts on S in the obvious way. *Orbits* constitutes a partition of S.

When $Orbit(t)$ is finite then there is a least positive integer n for which $Orbit(t) = \{\, P^k(t) \mid k = 0, \ldots n-1 \,\}$. $P^j(t)$ can never equal $P^k(t)$ for distinct j and k between 0 and $n-1$ and $P^n(t) = t$.

We now restrict attention to $P \in Finite(S)$ and, to avoid triviality, we suppose P is not the identity. Let T be the set of those elements of S for which $Orbit(t) \neq \{t\}$. $Multiple$ is a partition of T. Select t_i for $i = 1, \ldots, m$ so that $Orbit(t_i) \neq Orbit(t_j)$ unless $i = j$ and so that $Multiple = \{\, Orbit(t_i) \mid i = 1, \ldots, m \,\}$. Let $n_i = |Orbit(t_i)|$. Then P can be represented as the product of mutually disjoint cycles:

$$(t_1, P(t_1), \ldots, P^{n_1-1}(t_1))\,(t_2, P(t_2), \ldots, P^{n_2-1}(t_2)) \cdots (t_m, P(t_m), \ldots, P^{n_m-1}(t_m)).$$

This representation is unique except for order of these cycles, which commute with each other because they involve no common members of T. You will also note that P can be represented as the product of $n_1 + n_2 + \cdots + n_m$ 2-cycles.

So *any* member of $Finite(S)$ can be written as a product of 2-cycles.

An **even permutation** is a permutation which can be represented as a product of an even number of 2-cycles. An **odd permutation** is a permutation which can be represented as a product of an odd number of 2-cycles.

17.1. ***Proposition.*** *A member of $Finite(S)$ is odd or even but cannot be both.*

Proof. The shortest proof of this fact that I have seen involves the introduction of a rather odd polynomial, but before we do that let's simplify things a bit.

Suppose A is any finite subset of $Finite(S)$. Let $\widetilde{S}$ denote those members of S moved by *any* of the permutations from A. The set $\widetilde{S}$ is itself finite with, say, n elements.

Let B denote the restrictions of the members of A to the set $\widetilde{S}$. For any product of members of A we can form a corresponding product of members of B in the obvious way.

Further, by listing the members $s_1, s_2, \ldots, s_n$ of $\widetilde{S}$ we can identify each s_i with integer i so each permutation in B (and hence A) corresponds to a unique permutation in $\mathcal{S}_n$.

The point of all this is that *if* we could write some permutation $P \in Finite(S)$ as a product of 2-cycles in two different ways

$$P = P_1 \ldots P_k = Q_1 \ldots Q_j$$

with k even and j odd we could let A consist of P together with all these 2-cycles

$$A = \{\, P, P_1, \ldots, P_k, Q_1, \ldots Q_j \,\}$$

and reproduce this same situation in $\mathcal{S}_n$.

So we will consider all permutations below to be from $\mathcal{S}_n$.

Define the polynomial W in the n distinct variables $x_1, \ldots, x_n$ by

$$W = \prod_{(j,k) \in \{ \ (a,b) \ | \ 1 \leq a < b \leq n \ \}} (x_j - x_k).$$

There are $\frac{n(n-1)}{2}$ terms in this product.

If Q is any permutation define QW by:

$$QW = \prod_{(j,k) \in \{ \ (a,b) \ | \ 1 \leq a < b \leq n \ \}} (x_{Q(j)} - x_{Q(k)}).$$

It is fairly easy to show that $QW = \pm W$.

Define $sgn(Q)$ to be 1 if $QW = W$ and $sgn(Q)$ to be -1 if $QW = -W$.

It is not too hard to show that if Q_1 and Q_2 are permutations then

$$(Q_1 Q_2)W = sgn(Q_2) Q_1 W.$$

It follows that the function **sgn**, called the **signum function**, is a group homomorphism from $\mathcal{S}_n$ to the multiplicative group $\{-1, 1\}$.

It is obvious that if Q is a 2-cycle that $sgn(Q) = -1$.

So if P can be written as a product of an odd number j of 2-cycles then $sgn(P) = (-1)^j = -1$, while if P can be written as a product of an even number k of 2-cycles then $sgn(P) = (-1)^k = 1$. It can't be both.

This, combined with the observation from above that any member of $Finite(S)$ can be written as a product of 2-cycles, finishes the argument. □

Purists might object to this proof, since we have not defined the word "polynomial" nor have we proved anything about the properties of polynomials. The reader is invited to look for these facts as they are developed, later in the notes.

Define **Alt(S)** to be the set of even permutations of a nonempty set S. $Alt(S)$ is a group. Sometimes $Alt(S)$ is called the **alternating group on S**.

The alternating group on the first n positive integers will be denoted $\boldsymbol{\mathcal{A}lt_n}$.

17.2. ***Exercise.*** *The commutator subgroup $\mathcal{S}_3^{(1)}$ of $\mathcal{S}_3$ is $\mathcal{A}lt_3$. The second commutator subgroup $\mathcal{S}_3^{(2)}$ is trivial. So $\mathcal{S}_3$ is solvable, but has trivial center so cannot be nilpotent.*

17.3. ***Exercise.*** *If $|S| \geq 4$ then $Alt(S)$ is not abelian. Show that $Alt(S)$ and $Finite(S)$ are normal in $Perm(S)$. Show $Perm_T(S)$ will not be normal in $Perm(S)$ unless $T = S$ or T is empty. Show $Finite(S)/Alt(S)$ is isomorphic to $\{-1, 1\}$ with multiplication. Consider $Perm(S)/Finite(S)$ when S is infinite. Under what conditions on permutations τ and ϕ are the elements $\tau Finite(S)$ and $\phi Finite(S)$ of $Perm(S)/Finite(S)$ equal?*

17.4. ***Exercise.*** *Let e_i denote the matrix with n rows and 1 column having 1 in the ith row and 0 elsewhere, for integer $n \geq 1$ and $1 \leq i \leq n$. For $\sigma \in \mathcal{S}_n$ define $f(\sigma)$ to be the n by n matrix with columns $e_{\sigma(1)}, \ldots, e_{\sigma(n)}$, in that order. We will call these **permutation matrices**.*

(i) $f(\sigma)e_i = e_{\sigma(i)}$ so the matrix $f(\sigma)$ permutes the column matrices $e_1, \ldots, e_n$, via matrix multiplication on the left, in the same way that σ permutes $1, \ldots, n$.

(ii) Show that f is an embedding of $\mathcal{S}_n$ with composition into $GL_n(\mathbb{R})$ with matrix multiplication. The image of f consists exactly of all those matrices having all 0 entries except for a single 1 in each column, and for which no two columns are repeated. The image of f also consists of exactly all those matrices having all 0 entries except for a single 1 in each row, and for which no two rows are repeated.

(iii) Show that $\det(f(\sigma)) = sgn(\sigma)$.

(iv) If you know (somehow) that switching two columns in a square matrix introduces a minus sign in the determinant, you can argue that any permutation is even or odd, but not both. (Typically, however, determinants are defined using permutations and the signum function.)

(v) Conclude that every finite group with n elements is isomorphic to a group of n by n permutation matrices with matrix multiplication.

18. The Sylow Theorems

An element g of any group G is called a **p-element** if $g^{p^k} = e$, the identity, for some integer $k \geq 0$. Any group H is called a **p-group** if every element of H is a p-element. If H is a p-group and a subgroup of G it is called a **p-subgroup of G**. Note that $\{e\}$ is a p-subgroup of G for any prime p. If H is a p-subgroup of G so is any conjugate xHx^{-1} for any $x \in G$.

Since the union of a chain of p-subgroups is a p-subgroup, the set of p-subgroups of G ordered by containment has maximal members called **Sylow p-subgroups of G**.

We will suppose throughout this section that G is a finite group of order $n = tp^i$ for prime p and integer t. We will suppose p is not a factor of t, and will be concerned with the nontrivial case $i > 0$.

Because of Cauchy's Theorem, the order of any p-subgroup of G is a power of p, and G does have at least one nontrivial p-subgroup. Also, any subgroup of G of p-power order is a p-group.

We start with a preliminary lemma.

18.1. ***Lemma.*** *Suppose H is a p-subgroup of finite group G and for $i > 0$ we have $|H| = p^{i-1}$ and $|G| = p^i t$. Then $N(H, G)$ is strictly larger than H and, in fact, p is a factor of $[N(H, G) : H]$.*

Proof. Let S be the partition of G into double cosets HxH. In Exercise 12.7 we saw that these double cosets can be divided into those contained in $N(H, G)$ and those which do not intersect $N(H, G)$. There are $[N(H, G) : H]$ double cosets in $N(H, G)$. Let A be a choice of one member from each class involving $N(H, G)$, and B a selection of one member from each remaining class. Then

$$p^i t = |G| = \sum_{x \in A} |HxH| + \sum_{x \in B} |HxH| = |A|\ p^{i-1} + \sum_{x \in B} \frac{|H|\ |xHx^{-1}|}{|H \cap xHx^{-1}|}.$$

Each term on the far right is $p^i p^{t_x}$ for certain nonnegative integers t_x because $H \cap xHx^{-1}$ can never be H for any of those terms. So

$$p^i t = [N(H, G) : H]\ p^{i-1} + p^i \sum_{x \in B} p^{t_x}.$$

The result follows. □

18.2. ***Theorem. First Sylow Theorem*** *Suppose G is a finite group of order $p^i t$ where prime p is not a factor of t. If $A_1 \subset A_2 \subset \cdots \subset A_L$ is any chain of p-subgroups of G then there is a chain of p-subgroups $P_1 \subset P_2 \subset \cdots \subset P_i$ of G so that all the A_j appear on the list and $|P_j| = p^j$ for $1 \leq j \leq i$ and with P_j normal in P_{j+1} for $1 \leq j \leq i-1$.*

Proof. Suppose $|A_1| > p$ and pick element a of order p in A_1. By Lemma 18.1 $N((a), A_1)$ is larger than $P_1 = (a)$. So $N((a), A_1)/(a)$ has an element of order p and so the subgroup $\widetilde{H}$ of $N((a), A_1)/(a)$ generated by this element has order p. The union P_2 of the classes in this cyclic subgroup of $N((a), A_1)/(a)$ is a subgroup of $N((a), A_1)$ and has order p^2. Also $P_1 = (a)$ is normal in P_2. Carry on with this procedure with P_2 in place of P_1 until you arrive at some stage at $P_{j_1} = A_1$. Continue the construction in A_2 until you arrive at $P_{j_2} = A_2$.

The procedure terminates when all p powers of G are exhausted. □

This theorem implies, among other things, that any Sylow p-group of G has order p^i, the maximum p power which is a factor of $|G|$.

18.3. ***Theorem. Second Sylow Theorem*** *The conjugates of any one Sylow p-subgroup of a finite group G form the set of all Sylow p-subgroups of G.*

Proof. Let H and K be two Sylow p-subgroups of order p^i in G. So if A is a selection of one member of each distinct double coset HxK we have

$$|G| = \sum_{x \in A} |HxK| = \sum_{x \in A} \frac{|H|\ |K|}{|H \cap xKx^{-1}|} = \sum_{x \in A} \frac{p^{2i}}{|H \cap xKx^{-1}|}.$$

Each denominator in the sum is a power of p no greater than p^i. At least one denominator in the sum must actually be p^i or we would have p^{i+1} a factor of $|G|$. So for the x corresponding to that term, $H = xKx^{-1}$. □

18.4. ***Corollary.*** *The number of Sylow p-subgroups of a finite group G is a factor of t, where $|G| = tp^i$ and p is not a factor of t.*

Proof. Because of Theorem 18.2 we know that the number of Sylow p-subgroups is the number of conjugates of any one of them. That number is

$$[G : N(H, G)] = \frac{|G|}{|N(H, G)|}$$

where H is any Sylow p-subgroup. □

We also have the following result along these lines.

18.5. ***Theorem. Third Sylow Theorem*** *The number of Sylow p-subgroups of finite group G is congruent to 1 mod p.*

Proof. Consider the partition of G formed by double cosets HxH where H is a Sylow p-subgroup of order p^i. Let A be a selection of one member of each double coset contained in $N(H, G)$ and let B be a selection of one member of each remaining double coset.

We saw In Exercise 12.7 that $\sum_{x \in A} |HxH| = \sum_{x \in A} |xH| = |N(H, G)|$.

Also, for each $x \in B$ we have

$$|HxH| = \frac{|H|\ |xHx^{-1}|}{|H \cap xHx^{-1}|} = p^{i+1}p^{t_x}$$

for certain nonnegative integers t_x because $H \cap xHx^{-1}$ cannot be H for $x \in B$. So

$$|G| = \sum_{x\in A} |HxH| + \sum_{x\in B} |HxH| = |N(H,G)| + p^{i+1}\sum_{x\in B} p^{t_x}.$$

Let $s = \sum_{x\in B} p^{t_x}$. Since $N(H,G)$ is a subgroup of G its order divides the order of G. The first two out of three of the terms listed below

$$\frac{|G|}{|N(H,G)|} = 1 + \frac{p^{i+1}s}{|N(H,G)|}$$

are integers, so the last must be as well. Further, the last must be a multiple of p since $|N(H,G)|$ has only i factors of p.

Since $\frac{|G|}{|N(H,G)|}$ is the number of distinct conjugates of H, we have the result. □

18.6. ***Exercise.*** *(i) If H is a normal p group, and a subgroup of finite group G then H is a subgroup of every Sylow p-subgroup of G.*

(ii) Suppose $|G| = p^n$ for $n \geq 3$ and G is not abelian. G has both a nontrivial center and exactly one subgroup H of order p^{n-1}, which must be normal. The center of G must be contained in H.

19. Semidirect Products

Suppose H and N are groups and $\alpha\colon H \to Aut(N)$ is a representation of H. Recall that this means $\alpha(e_H)$ is the identity automorphism, where e_H is the identity of H, and also that

$$\alpha(xy)(n) = \alpha(x)\circ\alpha(y)(n) = \alpha(x)(\alpha(y)(n)) \quad \forall x, y \in H \ \text{ and } \ n \in N.$$

We define the **semidirect product $\mathbf{N} \rtimes_\alpha \mathbf{H}$** to be the set $N \times H$ together with operation given by

$$(x,i)(y,j) = (\, x\,\alpha(i)(y)\,,\, ij\,).$$

A calculation shows that this operation is associative with identity (e_N, e_H), where e_N is the identity of the group N. Also,

$$\left(\,\alpha\left(i^{-1}\right)(x^{-1})\,,\, i^{-1}\,\right)(\,x\,,\,i\,) = \left(\,\alpha\left(i^{-1}\right)(x^{-1})\alpha\left(i^{-1}\right)(x)\,,\, i^{-1}i\,\right) = (e_N, e_H).$$

So $N \rtimes_\alpha H$ is a group with this operation, of order $|N|\,|H|$.

If the representation is trivial, so that $Ker(\alpha) = H$, then $N \rtimes_\alpha H = N \times H$, but otherwise these groups are different.

The center of $N \rtimes_\alpha H$ consists of those points (x,i) where i is in the center of H, x is in the center of N and also a fixed point for the action (that is, $\alpha(j)(x) = x$ for all $j \in H$) and, finally, $\alpha(i)$ is the inner automorphism $\theta_x^{-1} = \theta_{x^{-1}}$.

Defining $\widetilde{N}$ to be $N \times \{\, e_H \,\}$ we see that

$$\begin{aligned}(x,i)\,(y,e_H)\,\left(\,\alpha\left(i^{-1}\right)(x^{-1})\,,\, i^{-1}\,\right) \ &= \ (x,i)\,\left(\,y\,\alpha\left(i^{-1}\right)(x^{-1})\,,\, i^{-1}\,\right)\\ &= \ \left(\,x\,\alpha(i)(y)\,x^{-1}\,,\, e_H\,\right) \ \in \ \widetilde{N}.\end{aligned}$$

So $\widetilde{N}$, which is isomorphic to N, is normal in $N \rtimes_\alpha H$.

On the other hand, the subgroup $\widetilde{H} = \{ e_N \} \times H$, which is isomorphic to H, will not be normal unless α is trivial, as seen by the calculation

$$(x, e_H)\,(e_N, j)\,\left(x^{-1}, e_H\right) = (x, j)\,\left(x^{-1}, e_H\right) = \left(x\,\alpha(j)\,\left(x^{-1}\right), j\right).$$

Recall Exercise 13.1 and suppose H and N are subgroups of G, $H \cap N = \{ e \}$, N is normal in G and $G = NH$.

Let elements of H act on N by conjugation θ. So $\theta_h(n) = hnh^{-1}$ for all $h \in H$, $n \in N$.

Define $f\colon N \rtimes_\theta H \to G$ by $f(n, h) = nh$.

According to that exercise, f is one-to-one and f is onto by assumption. Also, f is a homomorphism:

$$f\,(\,(x,h)\,(y,j)\,) = f\,\left(\,\left(xhyh^{-1}, hj\,\right)\,\right) = xhyh^{-1}hj = xhyj = f(\,(x,h)\,)\,f(\,(y,j)\,).$$

Our conclusion: The (internal) product of a normal subgroup with another subgroup with which it has trivial intersection is (isomorphic to) this particular semidirect product.

19.1. ***Exercise.*** *Let G be a group of finite order $n > 1$. Let T be a member of $Aut(G)$ other than the identity. This requires that n be at least 3. $Aut(G)$ is a subgroup of $Perm(G)$, so T has some finite order m which divides $n!$.*

Let $\mathbf{G_T}$ denote the set $G \times Cyclic(T)$ together with semidirect product multiplication

$$(g, T^j)(h, T^k) = (\, g\,T^j(h)\,,\ T^{j+k}\ ).$$

If e is the identity on G, (e, T^0) is the identity, and $(\ T^{-j}(h^{-1}), T^{-j}\ )$ is inverse to (h, T^j). G_T is a group of order $mn \geq 6$.

Each member (g, T^j) of G_T can be factorized as

$$(g, T^j) = (g, T^0)(e, T^j) \quad \textit{and note that} \quad (e, T^j)(g, T^0) = (T^j(g), T^j).$$

So this group is not abelian under our condition on T.

In fact, the center of G_T consists only of the points (g, T^j) where g is a fixed point of T and T^j is the inner automorphism $\theta_g^{-1} = \theta_{g^{-1}}$. This will include the points (g, T^0) where g is both in the center of G and a fixed point of T.

Examine what (if anything) must be modified to create similar structures for infinite G.

19.2. ***Exercise.*** *(i) If G is an infinite cyclic group then $|Aut(G)| = 2$.*

(ii) If G is a finite cyclic group of order n then $|Aut(G)| = \phi(n)$ where ϕ is the Euler ϕ function.

(iii) G is abelian if and only if the function $f\colon G \to G$ given by $f(x) = x^{-1}$ is an automorphism, which in that case has order 2.

(iv) If $a \in G$ is not in the center of G and $a^2 = e$ then the inner automorphism θ_a has order 2.

The groups referred in the cases above all have an automorphism of order 2.

When $m = 2$ and G is cyclic the groups G_T defined above are called dihedral groups, and any group isomorphic to one of these is also called a **dihedral group.** When G is finite of order n the order of G_T is $2n$.

19.3. ***Exercise.*** *(i) Let T be the member of $Aut(Rot_3)$ defined by $T(a) = a^{-1} = a^2$. $Cyclic(T)$ has order 2 so the group as defined above on $Rot_3 \times Cyclic(T)$ with operation given by $(a, T^i)(b, T^j) = (aT^i(b), T^{i+j})$ has order 6. Show that this group is isomorphic to $Perm\{1, 2, 3\}$.*

(ii) Let T be the member of $Aut(Rot_4)$ defined by $T(a) = a^{-1} = a^3$. $Cyclic(T)$ has order 2 so the group as defined above on $Rot_4 \times Cyclic(T)$ with operation given by $(a, T^i)(b, T^j) = (aT^i(b), T^{i+j})$ has order 8. Show that this group is isomorphic to $SquareSym$.

(iii) Let T be the member of $Aut(Rot_5)$ defined by $T(a) = a^{-1} = a^4$. $Cyclic(T)$ has order 2 so the group as defined above on $Rot_5 \times Cyclic(T)$ with operation given by $(a, T^i)(b, T^j) = (aT^i(b), T^{i+j})$ has order 10.

19.4. ***Exercise.*** *Suppose G is a finite group of order $2p$ for prime $p > 2$ and suppose G is not abelian. Let a be an element of order 2 generating subgroup A and b an element of order p generating subgroup B.*

(i) B is normal in G and $G = AB$.

(ii) $a^{-1}ba = b^M$ for some unique M with $1 < M < p$. ($M \neq 1$ because G is not abelian.)

(iii) So $T\colon B \to B$ defined by $T(b^k) = a^{-1}b^k a = b^{kM}$ for each k is an isomorphism and not the identity. Also $T^2(b^k) = a^{-2}b^k a^2 = b^k$ so $Cyclic(T)$ has order 2.

(iv) Let B_T denote the group with set $B \times Cyclic(T)$ and group operation defined in Exercise 19.3. Define $\mu\colon B_T \to G$ by $\mu(b^k, T^i) = b^k a^i$ for $i = 0$ or 1 and $0 \leq k < p$.

Show that μ is an isomorphism and conclude that any nonabelian group of order $2p$ is isomorphic to the dihedral group B_T.

20. More Examples of Finite Groups

We have assembled quite a few examples of groups (finite and otherwise, abelian and not) and quite a bit of information about them. For instance Rot_n provides abelian groups of all finite orders, while $\mathcal{S}_n$ provides nonabelian groups of order $n!$ for $n > 2$. $\mathcal{A}lt_n$ is nonabelian of order $(n!)/2$ when $n > 3$. The dihedral groups provide nonabelian groups of order $2n$ for any $n > 2$. We will now consider a few more, and some of their properties and subgroups.

Define for integer $n > 1$ $\mathbf{Aff_n}$, the **affine group on** $\mathbb{Z}_n$ to be the semidirect product $\mathbb{Z}_n \rtimes_\alpha RelPrime_n$ where the action, α, connotes multiplication:

$$(a, r)(b, s) = (a + rb, rs).$$

This group is nonabelian if $n > 2$ and its order is $n\phi(n)$, where ϕ is the Euler ϕ function, the number of integers among 1, 2, ..., $n - 1$ which are relatively prime to n.

$$|Aff_2| = 2, \quad |Aff_3| = 6, \quad |Aff_4| = 8, \quad |Aff_5| = 25 \quad \text{and} \quad |Aff_6| = 12.$$

20.1. ***Exercise.*** *Find all subgroups of $\mathcal{A}lt_n$ and $\mathcal{S}_n$ for $n = 1, 2$ and 3 and identify them as normal or characteristic. Find $Aut(\mathcal{S}_n)$ and $Aut(\mathcal{A}lt_n)$ for $n = 1, 2$ and 3.*

20.2. ***Exercise.*** *See how many of the following facts you can prove, and look up (or accept) the rest. We restrict attention in this exercise to $\mathcal{S}_n$ and $\mathcal{A}lt_n$ for $n \geq 4$.*

(i) $\mathcal{S}_4$ has only 2 nontrivial proper normal subgroups: $\mathcal{A}lt_4$ and

$$\{\, e,\ (1,\,2)(3,\,4),\ (1,\,3)(2,\,4),\ (1,\,4)(2,\,3)\,\}.$$

(ii) $\mathcal{A}lt_n$ is the only subgroup of index 2 in $\mathcal{S}_n$ for $n \geq 4$.

(iii) $\mathcal{A}lt_n$ is the only nontrivial proper normal subgroup of $\mathcal{S}_n$ for $n > 4$.

(iv) $\mathcal{A}lt_n$ is simple for $n > 4$.

(v) $\mathcal{S}_n$ is the internal direct product of its normal subgroup $\mathcal{A}lt_n$ with the subgroup T generated by any transposition for $n \geq 4$, and isomorphic to semidirect product $\mathcal{A}lt_n \rtimes_\alpha T$ where the action is given by inner automorphism.

(vi) $Aut(\mathcal{S}_n)$ and $Aut(\mathcal{A}lt_n)$ are isomorphic to $\mathcal{S}_n$ for $n = 4, 5$ and $n > 6$. The automorphisms can all be given as inner automorphisms by the members of $\mathcal{S}_n$.

(vii) Both $Aut(\mathcal{S}_6)$ and $Aut(\mathcal{A}lt_6)$ are isomorphic to a semidirect product of $\mathcal{S}_6$ with the subgroup generated by a transposition, with inner automorphism as the action on $\mathcal{S}_6$. So $Outer\,(\mathcal{S}_6)$ is isomorphic to $\mathbb{Z}_2$, while $Outer\,(\mathcal{A}lt_6)$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, also known as the ***Klein Four Group****.*

20.3. ***Exercise.*** *Consider the matrices e, a, b and c (see page 40) from $M_2(\mathbb{R})$.*

(i) For positive integer n the set of matrices of the form

$$\cos\left(\frac{2\pi k}{n}\right) e + \sin\left(\frac{2\pi k}{n}\right) a \qquad or \qquad \cos\left(\frac{2\pi k}{n}\right) b + \sin\left(\frac{2\pi k}{n}\right) c$$

for integer k values form a nonabelian group of order $2n$ with matrix multiplication.

The matrices on the left are the rotation matrices, Rot_n, and each will rotate a regular n-gon, the collection of points of the unit circle placed at angles $\frac{2\pi k}{n}$ starting with a point on the positive X axis, onto each other. The matrices on the right represent reflections of these n points across an axis of symmetry, and will represent the remaining types of "rigid motion" of the n-gon onto itself, sending vertices to vertices.

If n is even there are two kinds of reflections. The first kind is a reflection across a line from vertex to vertex, and leaves these two corners fixed. The second is a reflection across the middle of two sides, and moves all vertices.

On the other hand, if n is odd there is only one kind of reflection, that across a line from the center of an edge to the opposite vertex.

The reflections, including b and c themselves, are of order 2. Rot_n is a normal subgroup.

For each n these $2n$ matrices form a group isomorphic to the dihedral group described in Section 19. This embodiment of the dihedral group of order $2n$ is denoted $\mathbf{Dih_n}$.

If n is even the center of Dih_n is $\{\, e, -e \,\}$, and if n is odd the center is trivial.

By analogy with $SquareSym$, we might refer to Dih_3, Dih_5 and Dih_6 as **TriSym**, **PentSym** *and* **HexSym**, *respectively.*

(ii) Draw a picture of a regular triangle centered at the origin of the XY plane with one vertex on the X axis. Interpret the meaning of the elements of $TriSym$ by examining how the action when they left-multiply the coordinates of these points. Do the same, by analogy, with the groups $SquareSym$ and $PentSym$ and $HexSym$.

20.4. ***Exercise.*** *Try to show that $Aut\,(Dih_n)$ is isomorphic to Aff_n. Try to show that for n even, $Inner\,(Dih_n)$ has order n, while for n odd, $Inner\,(Dih_n)$ has order $2n$. So, except for $n = 3$, $Outer\,(Dih_n)$ is nontrivial. Interpret the effect of these outer automorphisms.*

20.5. ***Exercise.*** *(i) For positive integer n the set of matrices from $M_2(\mathbb{C})$ of the form*

$$\cos\left(\frac{\pi k}{n}\right) e + \sin\left(\frac{\pi k}{n}\right) a \qquad or \qquad \cos\left(\frac{\pi k}{n}\right) ib + \sin\left(\frac{\pi k}{n}\right) ic$$

for integer k values form a nonabelian group of order $4n$ with matrix multiplication.

For given n, the group is called the ***dicyclic group of order*** $\mathbf{4n}$, *denoted* $\mathbf{Dic_n}$.

Note that $Dic_2 = Quat$. The center of Dic_n is $\{\, e, -e \,\}$. The element $-e$ is the only ***involution*** *(that is, the only element of order 2) in Dic_n.*

(ii) Dih_{2n} has the same order as Dic_n, and each contains Rot_{2n} as a (normal) subgroup of index 2. At least half the members of Dic_n (those not in Rot_{2n}) have order 4, while the members of Dih_{2n} not in Rot_{2n} all have order 2.

(iii) Show that $Dic_n/\{\, e, -e \,\}$ is isomorphic to Dih_n.

(iv) Are $Quat/\{\, -e, e \,\}$ and $SquareSym/\{\, -e, e \,\}$ isomorphic?

20.6. ***Exercise.*** *Show that $\bigcup_{n=1}^{\infty} Dih_n$ is a group. What about $\bigcup_{n=1}^{\infty} Dic_n$?*

20.7. ***Exercise.*** *(i) Consider the semidirect product $\mathbb{Z}_T$ where T is the automorphism $T(n) = -n$ for $n \in \mathbb{Z}$. So $T^2 = e$, the identity automorphism. This is a dihedral group, sometimes denoted $\mathbf{Dih}_\infty$. Note that*

$$(n, T)(n, T) = (n + T(n), T^2) = (n - n, e) = (0, e)$$

for every n. So every element of this form is a torsion element of exponent 2 in this dihedral group. However

$$(n, T)(m, T) = (n + T(m), T^2) = (n - m, e)$$

which is an element of infinite order. The set of torsion elements of this dihedral group is not closed under the group operation so, among other things, they do not form a subgroup of $\mathbb{Z}_T$.

(ii) We refer to the notation of Exercise 20.3. The set of matrices of the form

$$\cos\left(\sqrt{2}\pi k\right) e + \sin\left(\sqrt{2}\pi k\right) a \qquad or \qquad \cos\left(\sqrt{2}\pi k\right) b + \sin\left(\sqrt{2}\pi k\right) c$$

for $k \in \mathbb{Z}$ forms a group isomorphic to $\mathbf{Dih}_\infty$.

(iii) Again, with reference to Exercise 20.3, show that the set of matrices of the form

$$\cos\left(\sqrt{2}\pi k\right) e + \sin\left(\sqrt{2}\pi k\right) a \qquad or \qquad \cos\left(\sqrt{2}\pi k\right) ib + \sin\left(\sqrt{2}\pi k\right) ic$$

for $k \in \mathbb{Z}$ forms a group. Is it isomorphic to $\mathbf{Dih}_\infty$?

20.8. ***Exercise.*** *The symmetry groups of the regular tetrahedron and the cube have orders 12 and 24 respectively. They represent the ways that these three dimensional objects can be rotated in space so that vertices align with vertices. These groups can be regarded as subgroups of $\mathcal{S}_4$ and $\mathcal{S}_8$, respectively. Identify these groups.*

20.9. ***Exercise.*** *Suppose G is an **abelian** finite group of order $n = p_1^{n_1} \cdots p_L^{n_L}$ for distinct primes p_i and positive integers n_i.*

(i) There is a unique list of integers $r_1, \ldots, r_k$ with $r_1 > 1$ and r_i a factor of r_{i+1} for $i = 1, \ldots, k-1$ and with $n = r_1 \cdots r_k$ so that G is isomorphic to $\prod_{i=1}^k \mathbb{Z}_{r_i}$.

(ii) There are positive integers $k_{i,j}$ for $j = 1, \ldots, m_i$ and $i = 1, \ldots, L$ where for each i, $m_i \geq 1$ and $\sum_{j=1}^{m_i} k_{i,j} = n_i$ and so that G is isomorphic to $\prod_{i,j} \mathbb{Z}_{p_i^{k_{i,j}}}$.

*If W is a positive integer, let $\pi(\mathbf{W})$ denote the number of ways that W can be represented as the sum of one or more positive integers, where order does not matter in any such sum. So $\pi(3) = 3$ because $3,\ 1+2,\ 1+1+1$ is a complete list of sums of the required type. π is called the **partition function for positive integers**. There is a big literature concerned with the properties of the partition function.*

(iii) If p is prime and W is positive show that any abelian group of order p^W is isomorphic to exactly one of $\pi(W)$ nonisomorphic (to each other) groups of the form $\prod_i \mathbb{Z}_{p^{k_i}}$ where the k_i are positive and add to W. How many abelian groups (up to isomorphism) are there of order $n = p_1^{n_1} \cdots p_L^{n_L}$ as in part (ii)?

(iv) If m divides the order of abelian G there is a subgroup of G of order m. However $\mathcal{A}lt_4$, which has order 12, has no subgroup of order 6. So this result cannot hold without the commutativity condition on G.

20.10. ***Exercise.*** *There is, essentially, only one group of prime order for each prime p and that group is abelian, and there are two groups of order p^2, which also must be abelian. Also if G is an abelian group of order n and $n = p_1 \cdots p_k$ is a factorization of the positive integer n as a product of distinct primes then G is isomorphic to $\mathbb{Z}_n$.*

We have also defined groups of various non-prime orders:
Order 4: $\mathbb{Z}_4$, Dih_2 and the Klein Four Group
Order 6: $\mathbb{Z}_6$, Aff_3, $\mathcal{S}_3$ and $TriSym$
Order 8: $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, Aff_4, $Quat$ and $SquareSym$
Order 9: $\mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$
Order 10: $\mathbb{Z}_{10}$ and $PentSym$
Order 12: $\mathbb{Z}_{12}$, $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathcal{A}lt_4$, Aff_6, $HexSym$ and Dic_3
Order 14: $\mathbb{Z}_{14}$ and Dih_7
Order 15: $\mathbb{Z}_{15}$

Are any of these isomorphic to any others? Are there any groups of these orders not isomorphic to one of those listed above? How many nonisomorphic groups can you find of order 16? (Hint: There are fourteen, five abelian and nine not. At least seven are easy to find.) How about higher orders?

21. Rings

Sometimes a set has more than one binary operation defined on it, the classic example being the integers with addition and multiplication.

A **ring** is a triple $(R, +, \cdot)$ where $(R, +)$ is an abelian group and $(R, \cdot)$ is a semigroup and the **left and right distributive laws** $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ hold for all a, b and c in R. As a notational convenience we use the conventional order of operations (powers first, then multiplication and last addition) and the previous sentence is an example of this in action.

A ring is called **nontrivial** if it contains more than a single element. Otherwise it is called **trivial**.

Two elements h and g in a ring are said to **commute** if they commute with respect to the multiplication in the ring. If $\cdot$ is a commutative operation we call the ring a **commutative ring.**

If $(R, \cdot)$ is a monoid the ring is called a **ring with identity.**

We will usually denote e_+ by 0 and $e_\cdot$, if it exists, by 1. We denote the additive inverse of an element r of R by $-r$ and a multiplicative inverse, when it exists, by r^{-1}. Obviously these notational simplifications fail when there are several ring structures on the same set, but that won't happen very often in these notes.

21.1. ***Exercise.*** *If $(R, +)$ is a group and $(R, \cdot)$ is a monoid and the left and right distributive laws hold it follows that $(R, +)$ is abelian and $(R, +, \cdot)$ is therefore a ring with identity. (hint: Expand $(1 + a) \cdot (1 + b)$ two ways.)*

21.2. ***Exercise.*** *(i) Suppose $(R, +, \cdot)$ is a ring. Then $(-g) \cdot h = -(g \cdot h) = g \cdot (-h)$ for every g and h in R.*

(ii) Further, if the elements h and g commute (with respect to multiplication, of course) then h commutes with $-g$ too. In the event that h^{-1} exists we find that h^{-1} commutes with g and $-g$ as well.

A **zero divisor** in a ring $(R, +, \cdot)$ is a nonzero member a of R for which $ab = 0$ or $ba = 0$ for some nonzero b in R. An element with a multiplicative inverse is called a **unit.** The units in a ring, if any, form a group with multiplication.

21.3. ***Exercise.*** *A ring has no zero divisors if and only if **left and right cancellation laws** are valid in the ring: that is, (**right cancellation**) $ax = bx$ implies $x = 0$ or $a = b$ and (**left cancellation**) $xa = xb$ implies $x = 0$ or $a = b$.*

If $(R - \{0\}, \cdot)$ is a group (that is, all nonzero members of R are units) we call the ring a **division ring**. A commutative division ring is called a **field.**

The integers $\mathbb{Z}$ and $X(\mathbb{Z})$ (see Exercise 11.18) form rings with identity. $n\mathbb{Z}$ where n is any fixed integer is a ring. $X(\mathbb{Q})$, $X(\mathbb{R})$, $X(\mathbb{C})$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Q}(\sqrt{2})$ are all fields.

$M_n(\mathbb{Z})$, $M_n(\mathbb{Q})$, $M_n(\mathbb{R})$ and $M_n(\mathbb{C})$ are very important rings.

21.4. ***Exercise.*** *Show directly that a member A of $M_2(\mathbb{R})$ is a zero divisor if and only if $det(A) = 0$.*

A **subring** of a ring R is a subset S of R containing the additive identity from R and which is itself a ring whose binary operations are given by the restriction of the binary operations in R. The additive identity of S will agree with that from R, but multiplicative identities need not agree. Indeed, S can have one while R does not or conversely. They can each have different multiplicative identities.

21.5. ***Exercise.*** *Let R be the set of matrices of the form*

$$\begin{pmatrix} m & 0 \\ 0 & 2n \end{pmatrix} \quad \text{for} \quad m, n \in \mathbb{Z}.$$

This set is a ring with matrix addition and multiplication. Find a subring of R with an identity and show that R itself does not.

21.6. ***Exercise.*** *If $\mathbf{R}[\mathbf{x}]$ is the set of all polynomials of finite degree in the variable x with coefficients in the ring R then $R[x]$ is a ring.*

$R[x]$ can be realized as the set consisting of those functions in $R^{\mathbb{Z}}$ whose values are 0 except for finitely many nonnegative members of the domain $\mathbb{Z}$. We will use subscript to indicate evaluation of such a function at one of its integer domain members. If $r \in R$ the polynomial rx^k for nonnegative k is identified with the function $f\colon \mathbb{Z} \to R$ which is 0 for all values of $\mathbb{Z}$ except k and for which $f_k = r$. In case R has an identity and $k = 1$ and $r = 1$ we identify x itself with this function.

$R[x]$ is closely related to the additive group $\sum_{n\in\mathbb{N}} R$ and is distinguished from that group by context and the existence of a multiplication defined for $f, g \in R[x]$ by $(fg)_k = \sum_{n\in\mathbb{Z}} f_n g_{k-n}$. Show that $R[x]$ is a ring with this operation and the obvious addition. The ring $R[x]$ has an identity precisely when R has one.

*For any $f \in R[x]$ and $k \in \mathbb{Z}$ the member $f_k \in R$ is called the **coefficient of $\mathbf{x^k}$ in $\mathbf{f}$**. The coefficient of x^0 is called the **constant term of $\mathbf{f}$**. f itself is called **constant** if $f_k = 0$ for $k > 0$. The **degree** of a constant polynomial is defined to be 0 if it is not the 0 polynomial, degree is not defined for the 0 polynomial, and for other polynomials the degree is the largest k for which $f_k \neq 0$.*

The "variable" x seems irrelevant, but will be used to distinguish different instances of the polynomial ring, and to label the instance to which a polynomial belongs. In these notes we take the point of view that notations such as $p(x)$ and $p(y)$ indicate polynomials which are closely related but not the same, even though they have the same coefficients. One is from $R[x]$ and the other from $R[y]$. The reader is invited to invent some other scheme to avoid ambiguity in cases where that might be an issue. The notation $p(x)$, mimicking as it does the usual function evaluation notation, is misleading. p is actually a function defined on $\mathbb{Z}$ with values in R (the coefficients), and $p(x)$ serves as a reminder that $p \in R[x]$. The problem will be further compounded when we define an evaluation of a polynomial at a member r of R in Exercise 21.11 using notation $p(r)$. In context, the correct meaning is usually clear and we rely on the reader's (no doubt) extensive experience with polynomial manipulation to keep it all straight.

The set of all polynomials of finite degree in the two variables x followed by y with coefficients in the ring R is denoted $\mathbf{R}[\mathbf{x}, \mathbf{y}]$ and defined to be $R[x][y]$. It too is a ring. Note: $R[x, y] \neq R[y, x]$.

Suppose that H is a subring of the ring R. Then $H[x]$ is a subring of $R[x]$ and $H[x, y]$ is a subring of $R[x, y]$.

If R_i is a ring for each integer $i = 1, \ldots, n$ the **product ring, denoted** $\mathbf{R_1 \times \cdots \times R_n}$, is the ring with product group addition and ring multiplication defined by $(r_1, \ldots, r_n) \cdot (s_1, \ldots, s_n) = (r_1 s_1, \ldots, r_n s_n)$.

21.7. ***Exercise.*** *Satisfy yourself that the operations defined above make $R_1 \times \cdots \times R_n$ into a ring. How might you extend the definition to a product of rings defined over an arbitrary nonempty index set A, rather than just a finite set of integers $\{1, \ldots, n\}$?*

21.8. ***Exercise.*** *With multiplication and addition mod n, $\mathbb{Z}_n$ is a commutative ring with identity called* ***the ring of integers mod*** $\mathbf{n}$*. The units of this ring are the members of $RelPrime_n$. $\mathbb{Z}_n$ is a field precisely when n is prime.*

The **quaternion** structure, defined below, is a way of making $\mathbb{R}^4$ into a division ring, and was discovered by Hamilton. They were used to study rotations in three dimensions, among other things, until they were supplanted (hastily, perhaps) by matrix reformulations. Applications in Engineering and Physics are plentiful.

A member $u = (w, x, y, z)$ of $\mathbb{R}^4$ is also denoted in this context

$$u = w + x\mathbf{i} + y\mathbf{j} + z\mathbf{k}$$

for historical reasons and by analogy with the complex numbers. Quaternion addition is defined by $(w_1, x_1, y_1, z_1)+(w_2, x_2, y_2, z_2) = (w_1+w_2, x_1+x_2, y_1+y_2, z_1+z_2)$, the usual addition in $\mathbb{R}^4$. Quaternion multiplication is associative but not commutative and is defined by

$$\begin{aligned}(w_1,&x_1, y_1, z_1) \cdot (w_2, x_2, y_2, z_2)\\ &= (w_1w_2 - x_1x_2 - y_1y_2 - z_1z_2,\ w_1x_2 + x_1w_2 + y_1z_2 - z_1y_2,\\ &\qquad\qquad w_1y_2 + y_1w_2 + z_1x_2 - x_1z_2,\ w_1z_2 + z_1w_2 + x_1y_2 - y_1x_2).\end{aligned}$$

If $u = (w, x, y, z)$ is a nonzero quaternion the notation $\overline{u}$ denotes the **conjugate quaternion** $(w, -x, -y, -z)$, while $|u| = \sqrt{w^2 + x^2 + y^2 + z^2}$ is the **magnitude of the quaternion,** the ordinary magnitude of u as a member of $\mathbb{R}^4$. The multiplicative inverse of u is $\overline{u}/|u|^2$.

A messy but direct calculation shows that if u and t are two quaternions, $\overline{ut} = \overline{t}\,\overline{u}$ and $|ut| = |u|\,|t|$.

The Quaternions (that is, the ring consisting of $\mathbb{R}^4$ with this addition and multiplication) will be denoted $\mathbb{H}$.

Quaternion multiplication can be calculated in a manner similar to the usual method of working out complex products by taking advantage of the relations:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1 \qquad \mathbf{ij} = -\mathbf{ji} = \mathbf{k} \qquad \mathbf{jk} = -\mathbf{kj} = \mathbf{i} \qquad \mathbf{ki} = -\mathbf{ik} = \mathbf{j}.$$

Because quaternions are not commutative care must be taken to preserve the order of the products while multiplying $w_1 + x_1\mathbf{i} + y_1\mathbf{j} + z_1\mathbf{k}$ by $w_2 + x_2\mathbf{i} + y_2\mathbf{j} + z_2\mathbf{k}$.

21.9. ***Exercise.*** *Verify that the quaternions form a division ring.*

A subring S of a generic ring R is called a **left ideal of R** if $xS \subset S\ \forall x \in R$. A subring S of R is called a **right ideal of R** if $Sx \subset S\ \forall x \in R$. A subring S of R is called an **ideal of R** if it is both a left and right ideal.

Suppose S is an ideal in a ring R. Because R, as an additive group, is abelian the subgroup S is a normal subgroup of R so we can form the additive quotient group R/S. Because S is an ideal the multiplication given by $(r+S)\cdot(t+S) = (rt)+S$ is well defined and it is also associative. So $\mathbf{R/S}$ with these operations is a ring too, called the **quotient ring of R by S**. When $a+S = b+S$ the notation $\mathbf{a \equiv b \bmod S}$ is sometimes used, and a is said to be **congruent to b mod S**.

21.10. ***Exercise.*** *Show that the multiplication given above on R/S is well defined and associative.*

21.11. ***Exercise.*** *Suppose that R is a ring with identity and $g, h \in R$ and $hg = gh$. $\mathbb{Z}[x]$ and $\mathbb{Z}[x,y]$ are the polynomial rings with coefficients in $\mathbb{Z}$. If $P \in \mathbb{Z}[x]$ we define $P(g)$ in the obvious way, with the understanding that an additive constant term in a polynomial is to be interpreted as a multiple of the multiplicative identity in R. Define $\mathbb{Z}(g) = \{\, P(g) \mid P \in \mathbb{Z}[x] \,\}$ and $\mathbb{Z}(g,h) = \{\, P(g,h) \mid P \in \mathbb{Z}[x,y] \,\}$ and show that these two sets are commutative rings and subrings of R, and $\mathbb{Z}(g,h) = \mathbb{Z}(h,g)$.*

*The subring $\mathbb{Z}(i)$ of $\mathbb{C}$, called the **ring of Gaussian integers**, is an example. The previously seen $\mathbb{Q}(\sqrt{2})$ is another. The **Eisenstein integers**, $\mathbb{Z}(\omega)$, where $\omega = \left(-1+i\sqrt{3}\right)/2$, is a third.*

21.12. ***Exercise.*** *If H is an ideal in a ring R then $H[x]$ is an ideal in the ring $R[x]$ and $H[x,y]$ is an ideal in the ring $R[x,y]$.*

Suppose that R is a commutative ring with identity and $f, g \in R$ and H is a subring of R. Then both $\mathbf{H(g)} = \{\, P(g) \mid P \in H[x] \,\}$ and $\mathbf{H(g,h)} = \{\, P(g,h) \mid P \in H[x,y] \,\}$ are subrings of R and $H(g,h) = H(h,g)$. If H is an ideal so are $H(g)$ and $H(g,h)$ and in that case $H(g) \subset H(g,h) \subset H$.

A **ring homomorphism** from a ring R to a ring S is a function $w\colon R \to S$ which is in $Hom(R,S)$ where R and S are thought of as additive groups but with the additional property that $w(rt) = w(r)w(t)\ \forall r,t \in R$. If a ring homomorphism has an inverse that inverse is also a ring homomorphism and w is called a **ring isomorphism**. R and S are called **isomorphic rings** by virtue of the existence of a ring isomorphism between them.

21.13. ***Exercise.*** *Suppose R is a commutative ring with identity. Define an addition and multiplication on the set S of all functions $\sigma\colon \mathbb{N}\times\mathbb{N} \to R$ which are nonzero at only finitely many domain values so that S is ring isomorphic to $R[x][y]$. Create a means of "evaluating" σ at a pair (f,g) of elements of R so that $R(f,g) = \{\sigma(f,g) \mid \sigma \in S\}$.*

The set of all ring homomorphisms from the ring R to the ring S is denoted $\mathbf{Hom_{ring}(R,S)}$.

Since addition is always commutative in a ring, $Hom(R,S)$ will be a group with addition of homomorphisms. However $Hom_{ring}(R,S)$ will not be a subgroup of $Hom(R,S)$ with this operation because the sum of ring homomorphisms need not (usually will not) be a ring homomorphism.

If R is a ring $\mathbf{Aut_{ring}(R)}$ is defined to be $Perm(R) \cap Hom_{ring}(R,R)$, the **ring automorphisms of R**. $Aut_{ring}(R)$ is a subgroup of $Aut(R)$ with composition.

21.14. ***Exercise.*** *When $(G,+)$ is an abelian group then $Hom(G,G)$ is a ring with addition and composition.*

21.15. ***Exercise.*** *We suppose $w \in Hom_{ring}(R,S)$.*

(i) $Ker(w)$ is an ideal in R and $Image(w)$ is a subring of S.

(ii) If H is any subring of S then $w^{-1}(H)$ is a subring of R containing $Ker(w)$.

(iii) If T is a subring of R then $w(T)$ is a subring of S.

(iv) If w is onto S then w provides a correspondence between subrings of S and subrings of R containing $Ker(w)$.

(v) If H is any ideal in S then $w^{-1}(H)$ is an ideal in R containing $Ker(w)$.

(vi) If T is an ideal of R then $w(T)$ is an ideal in the ring $Image(S)$. So if w is onto S then $w(T)$ is an ideal of S.

(vii) If w is onto S then w provides a correspondence between ideals in S and ideals in R containing $Ker(w)$.

(viii) $Image(w)$ is ring isomorphic to $R/Ker(w)$.

(ix) If S is an ideal in R the function $w\colon R \to R/S$ defined by $w(t) = t+S$ $\forall t \in R$ is a ring homomorphism and $S = Ker(w)$.

(x) If w is onto S then w is a ring isomorphism if and only if $Ker(w) = \{0\}$.

21.16. ***Exercise.*** *Recall the matrices*

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \textit{and} \quad a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \textit{and} \quad b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \textit{and} \quad c = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

defined originally on page 40.

(i) If R is a subring of $\mathbb{C}$ then $X(R) = \{\, xe + ya \mid x, y \in R \,\}$ is ring isomorphic to the subring $R(i)$ of $\mathbb{C}$. In particular, $X(\mathbb{R})$ is ring isomorphic to $\mathbb{C}$ itself.

(ii) Consider the set of all matrices in $M_2(\mathbb{C})$ which can be written as a sum

$$w\,e + x\,a + y\,ib + z\,ic = \begin{pmatrix} w+iy & -x+iz \\ x+iz & w-iy \end{pmatrix}$$

with real w, x, y and z. This set with matrix operations is ring isomorphic to $\mathbb{H}$, the quaternions.

(iii) Commonly, one sees the quaternions represented as the set of all matrices in $M_2(\mathbb{C})$ which can be written as a combination, with real w, x, y and z,

$$w\,e + x\,ib + y\,(-a) + z\,ic = \begin{pmatrix} w+ix & y+iz \\ -y+iz & w-ix \end{pmatrix}.$$

Satisfy yourself that this is a convenient alternative to that given in (ii).

(iv) Define matrices

$$\sigma_0 = e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \textit{and} \quad \sigma_1 = c = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$\textit{and} \quad \sigma_2 = ia = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \textit{and} \quad \sigma_3 = b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

We have:

$$\sigma_1\sigma_2 = i\sigma_3 \quad \textit{and} \quad \sigma_2\sigma_3 = i\sigma_1 \quad \textit{and} \quad \sigma_3\sigma_1 = i\sigma_2$$
$$\textit{and} \quad \sigma_1^2 = \sigma_2^2 = \sigma_3^2 = \sigma_0 = e.$$

$$\textit{Also} \quad \sigma_k\sigma_m = -\sigma_m\sigma_k \quad \textit{for unequal nonzero } m \textit{ and } k.$$

The group consisting of the sixteen matrices

$$\{\, \pm\sigma_0,\, \pm i\sigma_0,\, \pm\sigma_1,\, \pm i\sigma_1,\, \pm\sigma_2,\, \pm i\sigma_2,\, \pm\sigma_3,\, \pm i\sigma_3 \,\}$$

contains both $SquareSym = Dih_4$ *and* $Quat = Dic_2$ *as subgroups.*

The matrices σ_1, σ_2 *and* σ_3 *are called* ***Pauli spin matrices****. They are hermitian (and so correspond to "observables") and represent spin with respect to the coordinate axes in quantum mechanical descriptions of certain particles. Any* 2 *by* 2 *hermitian matrix can be found (in one way) as a combination*

$$w\,\sigma_0 + x\,\sigma_1 + y\,\sigma_2 + z\,\sigma_3 \;=\; \begin{pmatrix} w+z & x-iy \\ x+iy & w-z \end{pmatrix}$$

with real w, x, y *and* z*.*

Show that

$$w\,\sigma_0 + x\,(-i\sigma_1) + y\,(-i\sigma_2) + z\,(-i\sigma_3) \;=\; \begin{pmatrix} w-zi & -xi-y \\ -xi+y & w+zi \end{pmatrix}$$

with real w, x, y *and* z *provides yet another way of realizing the quaternions, this time in terms of the Pauli spin matrices.*

(v) Consider the product set $\mathbb{C}\times\mathbb{C}$ *with obvious addition but with multiplication*

$$(u_1, v_1) * (u_2, v_2) = (\; u_1u_2 \;-\; \overline{v_1}\; v_2,\; v_1u_2 \;+\; \overline{u_1}\; v_2 \;).$$

The multiplicative identity is $(1, 0)$*, and* $\mathbb{R}\times\{0\}$ *and* $\mathbb{C}\times\{0\}$ *are subrings isomorphic to* $\mathbb{R}$ *and* $\mathbb{C}$ *respectively.*

Show that $\mathbb{C}\times\mathbb{C}$ *with these operations is ring isomorphic to the quaternions.*

With this identification, the conjugate quaternion for $h = (u, v)$ *is* $\overline{h} = (\overline{u}, -b)$ *and also* $\overline{h} * h = h * \overline{h} = (u\overline{u} + b\overline{b}, 0)$*. If* h *is nonzero,* $h^{-1} = \overline{h}/\left(h * \overline{h}\right)$*.*

There is considerable nomenclature involving ideals in a ring R.

If A and B are nonempty subsets of R define $\mathbf{AB} = \{\, ab \mid a \in A \text{ and } b \in B \,\}$. If $A = \{a\}$ and B is a nonempty set we denote AB by $\mathbf{aB}$ while if $B = \{b\}$ and A is a nonempty set we denote AB by $\mathbf{Ab}$. Define $\mathbf{A} + \mathbf{B} = \{\, a+b \mid a \in A \text{ and } b \in B \,\}$.

We extend these notations in the obvious way to include products $A_1A_2\cdots A_n$ and sums $A_1 + A_2 + \cdots + A_n$ of any finite number of nonempty subsets A_i of R.

21.17. ***Exercise.*** *(i) If both* A *and* B *are ideals, so are* $A\cap B$ *and* $A + B$*. Also* $AB \subset A\cap B \subset A\cup B \subset A + B$*. The sets* AB *and* $A\cup B$ *need not be ideals.*

(ii) The intersection of any nonempty family of ideals in R *is an ideal.*

(iii) The union of any chain of ideals in R *is an ideal.*

The intersection of all ideals containing a set $A \subset R$ is called the **ideal generated by A**. We use $(\mathbf{A})$ to denote this ideal. (A) is the collection of all finite sums of elements of the form a or ar_2 or r_1a or r_1ar_2 where $a \in A$ and r_1 and r_2 are in R.

21.18. ***Exercise.*** *If* B *is an ideal and* $A \subset B$ *then* $(A) \subset B$*. If* A *and* B *are ideals it is easy to see that* $(AB) \subset A\cap B$ *and* $(A\cup B) = A + B$*. If* A *is a subset of* R *and* C *is an ideal in* R *then* $(AC) = ((A)C)$*.*

If an ideal B is generated by a set containing a single element x we say that B is a **principal ideal** and use the notation $\mathbf{B} = (\mathbf{x})$.

So a generic member of a principal ideal (x) has the form

$$nx + rx + \sum_{i=1}^{k} r_i x s_i \quad n \text{ an integer and } r, r_i, s_i \in R.$$

This simplifies somewhat in various special cases. If R is commutative this becomes $nx + \sum_{i=1}^{k} r_i x$ for integer n and $r_i \in R$. If R has identity the generic sum has form $rx + \sum_{i=1}^{k} r_i x s_i$ while if R is both commutative and has identity, $(x) = Rx = xR$.

The ideal $\{0\}$ is called **trivial**, and every ideal in R except R itself is called **proper.**

A proper ideal P is called **prime** if whenever A and B are ideals in R and $AB \subset P$ then $A \subset P$ or $B \subset P$.

21.19. ***Exercise.*** *Let R denote the ring consisting of just the diagonal matrices in $M_2(\mathbb{R})$. The ideal in R containing just the zero matrix is not prime.*

21.20. ***Exercise.*** *Suppose R is a nontrivial ring and P a proper ideal in R.*

(i) If $xy \in P$ implies $x \in P$ or $y \in P$ then P is prime.

(ii) If R is commutative the converse is true.

(iii) If $x, y \in R - P$ implies $xy \in R - P$ then P is prime.

(iv) If R is commutative the converse is true.

Let S denote the set of chains of prime ideals in a ring R and order S by containment. The union of any "chain of chains" is itself a chain so, by invocation of the Axiom of Choice, S contains maximal members. The intersection of all members of one of these maximal chains of prime ideals is itself prime, so the collection of prime ideals in a ring (if there are any) has minimal elements: prime ideals which contain no smaller prime ideal. In fact, every prime ideal contains at least one of these. They are called **minimal prime ideals.**

More generally, if A is a subset of a ring R and if there are any prime ideals containing A at all then the set of all prime ideals containing A has minimal members which, though prime, need not be minimal prime ideals.

Ideals A and B in R are called **coprime** if $A + B = R$.

21.21. ***Exercise.*** *If A, B and P are ideals in R and P is a prime ideal then $AB \subset P$ if and only if $A \cap B \subset P$. Rephrased, in case P is a prime ideal and A, B are ideals then $A \cap B \subset P$ if and only if $A \subset P$ or $B \subset P$.*

A **maximal ideal** is a proper ideal contained in no other proper ideal.

21.22. ***Exercise.*** *Every ring R is ring isomorphic to a maximal ideal in a ring with identity. (hint: Define multiplication on $\widetilde{R} = R \times \mathbb{Z}_2$ by $(r, a) \cdot (s, b) = (rs + br + as, ab)$.)*

21.23. ***Proposition.*** *In a ring with identity, every proper ideal P is contained in a maximal ideal.*

Proof. If we examine a chain of proper ideals containing P ordered by containment and let A be the union of that chain then A is an ideal. The ideal A cannot be R because then 1 would have to be in one of the ideals of the chain, impossible because all ideals in the chain are proper. So chains in the set of all proper ideals containing P have least upper bounds with containment order that are proper ideals containing P, so the set of all proper ideals containing P has a maximal member. This ideal is a maximal ideal. □

21.24. ***Exercise.*** *If M is a maximal ideal in a ring R with identity and A is a proper ideal in R then $A \subset M$ or A and M are coprime.*

22. Commutative Rings

In this section we consider commutative rings. In a commutative ring there is no distinction between left and right ideals.

A commutative ring with identity and no zero divisors is called an **integral domain.**

22.1. ***Exercise.*** *Suppose R is an integral domain and $S = R \times (R - \{0\})$. Define a relation $\sim$ on S by $(a, b) \sim (c, d)$ if and only if $ad = bc$.*

(i) Show that $\sim$ is an equivalence relation on S. The equivalence class of $(a, b) \in S$ is usually denoted $\frac{a}{b}$.

(ii) If $\frac{a}{b}$ and $\frac{c}{d}$ are in $S/\sim$ define $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ and $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$. Show that these members of $S/\sim$ are well defined.

*(iii) Show that with these operations $S/\sim$, which we will denote $\mathbf{Q(R)}$, is a field with additive identity $\frac{0}{1}$ and multiplicative identity $\frac{1}{1}$. We call it the **field of quotients of R.***

(iv) Define $\phi\colon R \to Q(R)$ by $\phi(a) = \frac{a}{1}$. Show that ϕ is one-to-one and a ring homomorphism and note that $\phi(1)$ is the identity in $Q(R)$. We have shown that every integral domain can be embedded in its field of quotients, and this embedding is a ring homomorphism which carries identity to identity.

A **Euclidean valuation on a commutative ring R** is a function
$d\colon R - \{0\} \to \mathbb{N}$ with the following properties:
(i) $d(f) \leq d(fg)$ $\forall f, g \in R$ with $fg \neq 0$ and
(ii) $\forall f, g \in R$ with $g \neq 0$ there exist $r, s \in R$ with $f = sg + r$ and either $r = 0$ or $r \neq 0$ and $d(r) < d(g)$.

A **Euclidean ring** is a commutative ring R together with a Euclidean valuation on R. If a Euclidean ring is also an integral domain it is called a **Euclidean domain**.

22.2. ***Exercise.*** *(i) $\mathbb{Z}$ is a Euclidean domain with valuation $d(n) = |n|$.*

(ii) Note that $|qr| = |q||r|$ $\forall q, r \in \mathbb{C}$. Also $|q| = |\overline{q}| = \sqrt{q\overline{q}}$. Finally, when $q \neq 0$ then $q^{-1} = \overline{q}/|q|$.

(iii) If $y, z \in \mathbb{C}$ and $y \neq 0$ let $u = u_1 + u_2 i = zy^{-1}$. Let s_j be an integer in $[u_j - \frac{1}{2}, u_j + \frac{1}{2}]$ for $j = 1, 2$ and define $s = s_1 + s_2 i$. In that case

$$|u - s|^2 = (u_1 - s_1)^2 + (u_2 - s_2)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}.$$

It follows that

$$|y| > |u - s||y| = |uy - sy| = |z - sy|.$$

Conclusion: There is a Gaussian integer multiple of y less than distance $|y|$ away from any particular $z \in \mathbb{C}$.

(iv) Use part (iii) to show that the Gaussian integers $\mathbb{Z}[i]$ form a Euclidean domain with squared magnitude as Euclidean valuation.

22.3. ***Exercise.*** *(i) Create a Euclidean valuation for any field.*

(ii) Verify the following statements and conclude that $F(x)$ is a Euclidean domain for any field F.

Define for any nonzero polynomial $f \in F(x)$ the number $d(f)$ to be the degree of the highest power of x for which f has a nonzero coefficient. It is clear that $d(fg) = d(f)d(g) \geq d(f)$ whenever $f, g \in F(x)$ and $f \neq 0 \neq g$. We will now show that if $f, g \in F(x)$ with $g \neq 0$ there exist $r, s \in F(x)$ with $f = sg + r$ and either $r = 0$ or $r \neq 0$ and $d(r) < d(g)$.

It is obvious if $d(f) < d(g)$ or if $d(f) = d(g) = 0$. So we will assume that r and s have been shown to exist whenever $g \neq 0$ and $n = d(f) \geq d(g)$ for all integers $0 \leq n < k$. Let us now suppose that $g \neq 0$ and $k = d(f) \geq d(g) = i$. Let f_k denote the coefficient of x^k in f and g_i the coefficient of x^i in g. If we let $\widetilde{f} = f - x^{k-i} f_k g_i^{-1} g$ then $d(\widetilde{f}) < k$ so there are $\widetilde{s}$ and r with $\widetilde{f} = \widetilde{s}g + r$ and where either $r = 0$ or $r \neq 0$ and $d(r) < d(g)$. But then $f = \left(x^{k-i} f_k g_i^{-1} + \widetilde{s}\right) g + r$.

*(iii) When R is a ring and $c \in R$ and $f \in R[x]$ we call $x - c$ a factor of f in $R[x]$ exactly when $f(x) = (x - c)g(x)$ for some $g \in R[x]$. We call c a **root of $\mathbf{f}$ in $\mathbf{R}$** when $f(c) = 0$. Show that when R is a field and $f \in R[x]$, an element $c \in R$ is a root of f in R exactly when $x - c$ is a factor of f in $R[x]$.*

An integral domain is called a **principal ideal domain** if every ideal in the ring is principal.

22.4. ***Exercise.*** *In a principal ideal domain, any prime ideal is maximal.*

22.5. ***Exercise.*** *Suppose that R is a principal ideal domain and S is any ring and $f \in Hom_{ring}(R, S)$ is onto S. Then S itself must be commutative with identity and a principal ideal ring. It need not be an integral domain.*

22.6. ***Exercise.*** *Suppose that R is a principal ideal domain and S is a chain of ideals of R with inclusion order. If S has a least member then S is finite.*

22.7. ***Exercise.*** *Show that if R is a Euclidean ring then R is a principal ideal domain.*

To see this, follow this argument. Let d be the Euclidean valuation and suppose J is a nontrivial ideal in R. There is an element y in J with $d(y) \leq d(z)$ whenever $z \neq 0$ and $y \in J$. Now suppose that $z \in J$. Then there is $s \in R$ with $z - sy = 0$ or $d(z - sy) < d(y)$. Since both z and sy are in the ideal J the second condition is impossible and so $z = sy$. That means $zR = J$.

That R has an identity follows from observing that R is an ideal so $R = zR$ for some z. For each $y \in R$ let c_y denote a member of R with $y = zc_y$. So $y = zc_y = zc_zc_y = zc_yc_z = yc_z$ for every y. The element c_z is, therefore, the identity.

22.8. ***Exercise.*** *$\mathbb{Z}[x]$ is not a principal ideal domain. (hint: $x\mathbb{Z}[x]+2\mathbb{Z}[x]$ is not a principal ideal.)*

22.9. ***Exercise.*** *Consider the polynomial ring $\mathbb{R}[x]$ and its ideal (x^2+1). Show that (x^2+1) is a maximal ideal and that $\mathbb{R}[x]/(x^2+1)$ is ring isomorphic to $\mathbb{C}$.*

22.10. ***Exercise.*** *Suppose F is a field and A is a maximal ideal in $F[x]$. So there is $p(x) \in F[x]$ with $A = p(x)F[x] = (p(x))$. If $p(x)$ could be written as a product of polynomials $h(x)$ and $g(x)$ both of first degree or higher then A would be contained in but not equal to the proper ideal $(h(x))$, contradicting maximality of A. In particular, $p(x)$ can have no roots in the field F.*

$G = F[x]/A$ is a field, and F is isomorphic to a subfield of G. The polynomial $p(y) \in G[y]$ has a root c in G, so $y - c$ is a factor of $p(y)$.

22.11. ***Exercise.*** *Suppose A and B are ideals in $\mathbb{Z}$. So $A = (a)$ and $B = (b)$ for certain integers a and b. Show that A and B are coprime ideals if and only if a and b are relatively prime integers.*

More generally, if $r > 0$ and $(a)+(b) = (r)$ then r is the greatest common factor of a and b.

22.12. ***Exercise.*** *Suppose R is a ring with identity e. Define $f\colon \mathbb{Z} \to R$ by $f(n) = ne$. The function f is a ring homomorphism and has a kernel which is an ideal in the principal ideal domain $\mathbb{Z}$. So $Ker(f) = (k) = k\mathbb{Z}$ for some unique integer $k \geq 0$. R is said to have* ***characteristic*** **k**.

$Image(f)$ is a subring of R. If $k = 0$ this image is ring isomorphic to $\mathbb{Z}$. If k is nonzero the image of f is ring isomorphic to $\mathbb{Z}/(k) = \mathbb{Z}_k$.

If the ring R is a field, its characteristic must be 0 or prime. If its characteristic is 0 it contains a subring isomorphic to $\mathbb{Q}$.

Show that if R is a finite field then it has prime characteristic k and k divides $|R|$. Must a field of prime characteristic be finite? (See Exercise 28.12.)

23. The Hyperreal Numbers

The historic Euclid-derived conception of a line was as an object possessing "the quality of length without breadth" and which satisfies the various axioms of Euclid's geometric structure. Euclidean constructions involved finitely many points identified on the line by application of certain allowable operations. Arithmetical properties followed from their way of doing things, such as the Archimedean order property: "There is an integer multiple of the smaller of two numbers which exceeds the greater."

Our modern point of view identifies a certain algebraic object, a Dedekind complete ordered field called the real numbers, with infinitely many points on a line. These properties are intended to codify some of our intuition about the concept of "line" in a way that builds on the old view. For instance Dedekind completeness implies the Archimedean order property, though the reverse implication does not hold.

Dedekind completeness, which affirms the existence of a supremum for every bounded set, is a key feature: it guarantees that most of the things we would

like to do with real numbers do not cause us to *leave* the real numbers, thereby insulating us from defects of earlier number systems.

Most of us take it for granted that the real numbers can be used to represent *all* the points on the line. However the inventors of calculus had a conception of "vanishingly small quantities" and numbers separated from each other by infinitesimal displacements. They performed arithmetic with their evanescent creations, and added up infinitely many of them or calculated infinite multiples of them, to produce tangible numbers. They could obtain verifiably correct results by proper use of these methods, though "proper use" was never completely codified. They just *knew* when they were doing it correctly, even if they had problems explaining it to their philosopher critics (such as George Berkeley) who disdained their use, with considerable verve, as intellectually hopeless.

The real number system has no room for "infinitesimals," nor is there a direct way to discuss their reciprocals which must exceed any integer. The concept of limit developed by Cauchy and others has successfully replaced both, much to the relief of those who were distressed by the widely acknowledged lack of rigor of infinitesimal arithmetic.

In 1960 Abraham Robinson realized that the elements were in place to create a system which *could* represent "infinitesimals" directly and whose properties could be used to prove theorems in our standard world.

Analysis using this augmented number system is called **nonstandard analysis.** The augmented number system itself is called the set of **hyperreal numbers**. Many practionioners of nonstandard analysis believe that it will *become* standard, that the real number system was a stopgap required by limitations in mathematical and logical technique of its nineteenth century creators. At this time it is not universally accepted that this would be beneficial.

We outline below the construction of this field and discuss a few properties. Those interested can consult the very readable *Lectures on the Hyperreals* by Robert Goldblatt [**?**]. Robinson's book *Non-Standard Analysis*[**?**] is an interesting and somewhat more advanced source.

Let $\mathcal{S}$ denote the ring of real valued sequences with the usual pointwise operations. If x is a real number we let s^x denote the constant sequence, $s^x_n = x$ for all n. The function sending x to s^x is a one-to-one ring homomorphism, providing an embedding of $\mathbb{R}$ into $\mathcal{S}$. In the following, wherever it is not too confusing we will not distinguish between $x \in \mathbb{R}$ and the constant function s^x, leaving the reader to derive intent from context.

The ring $\mathcal{S}$ has additive identity 0 and multiplicative identity 1. $\mathcal{S}$ is not a field because if r is any sequence having 0 in its range it can have no multiplicative inverse. There are lots of zero divisors in $\mathcal{S}$.

Select a free ultrafilter $\mathbb{F}$ on $\mathbb{N}$. These exist on any infinite set, a fact implied by the Axiom of Choice. We list the properties we will use here:

(*i*) $\varnothing \notin \mathbb{F} \subset \mathbb{P}(\mathbb{N})$.

(*ii*) $\mathbb{F}$ contains every cofinite subset of $\mathbb{N}$.

(*iii*) $A, B \in \mathbb{F} \Rightarrow A \cap B \in \mathbb{F}$.

(*iv*) $A \subset \mathbb{N},\ B \in \mathbb{F} \Rightarrow A \cup B \in \mathbb{F}$.

(*v*) If $V_1, \ldots, V_n$ is a finite partition of $\mathbb{N}$ then $\mathbb{F}$ contains exactly one of the V_i.

We create a convenient shorthand for the usual "set builder" notation for subsets of $\mathbb{N}$. If P is a property that can be true or false for natural numbers we let $[\![P]\!]$ denote $\{n \in \mathbb{N} \mid P(n) \text{ is true}\}$.

For example, if s, t is a pair of sequences in $\boldsymbol{\mathcal{S}}$ we define three sets of integers

$$[\![s < t]\!], \qquad [\![s = t]\!], \qquad [\![s > t]\!].$$

Since these three sets partition $\mathbb{N}$, exactly one of them is in $\mathbb{F}$, and we declare $s \equiv t$ when $[\![s = t]\!] \in \mathbb{F}$.

23.1. ***Exercise.*** *$\equiv$ is an equivalence relation on $\boldsymbol{\mathcal{S}}$. We denote the equivalence class of any sequence s under this relation by $[s]$.*

Define for each $r \in \boldsymbol{\mathcal{S}}$ the sequence $\tilde{r}$ by

$$\tilde{r}_n = \begin{cases} 0, & \text{if } r_n = 0; \\ (r_n)^{-1}, & \text{if } r_n \neq 0. \end{cases}$$

23.2. ***Exercise.*** *(i) There is at most one constant sequence in any class $[r]$.*

(ii) $[0]$ is an ideal in $\boldsymbol{\mathcal{S}}$ so $\boldsymbol{\mathcal{S}}/[0]$ is a commutative ring with identity $[1]$.

(iii) Consequently $[r] = r + [0]$ for all $r \in \boldsymbol{\mathcal{S}}$.

(iv) If $[r] \neq [0]$ then $[\tilde{r}][r] = [1]$. So $[r]^{-1} = [\tilde{r}]$.

From this exercise, we conclude that ${}^*\mathbb{R}$, defined to be $\boldsymbol{\mathcal{S}}/[0]$, is a field containing an embedded image of $\mathbb{R}$ as a subfield. This quotient ring is called the field of **hyperreal numbers**.

We declare $[s] < [t]$ provided $[\![s < t]\!] \in \mathbb{F}$.

Recall that any field A with a linear order $<$ is called an ordered field provided

(*i*) $x + y > 0$ whenever $x, y > 0$

(*ii*) $xy > 0$ whenever $x, y > 0$

(*iii*) $x + z > y + z$ whenever $x > y$

23.3. ***Exercise.*** *(i) The relation given above is a linear order on ${}^*\mathbb{R}$, and makes ${}^*\mathbb{R}$ into an ordered field. As with any ordered field, we define $|x|$ for $x \in {}^*\mathbb{R}$ to be x or $-x$, whichever is nonnegative.*

(ii) If x, y are real then $x \leq y$ if and only if $[x] \leq [y]$. So the ring isomorphism of $\mathbb{R}$ into ${}^*\mathbb{R}$ is also an order isomorphism onto its image in ${}^*\mathbb{R}$.

(iii) It is also true that if the sequences s, t satisfy $s_n \leq t_n$ for every n then $[s] \leq [t]$. The converse, of course, need not hold.

Because of this last exercise and the essential uniqueness of the real numbers it is common to identify the embedded image of $\mathbb{R}$ in ${}^*\mathbb{R}$ with $\mathbb{R}$ itself. One does not (unless *absolutely necessary*) make, for instance, the two-step transition

$$2 \to \text{ (constant sequence equal to 2 } \forall n) \to [2] = \{\, t \in \mathcal{S} \mid [\![t = 2]\!] \in \mathbb{F} \,\}.$$

We do not distinguish 2 from [2].

Though obviously circular, we did something similar when we identified $\mathbb{Q}$ with its isomorphic image in $\mathbb{R}$, and $\mathbb{N}$ itself with the corresponding subset of $\mathbb{Q}$. This kind of notational simplification usually does not cause problems.

Now we get to the ideas that prompted the construction. Define the sequence r by $r_n = \frac{1}{n+1}$. For every positive integer k, $[\![r < \frac{1}{k}]\!] \in \mathbb{F}$. So $0 < [r] < \frac{1}{k}$. We have found a positive hyperreal smaller than (the embedded image of) any real number. This is our first nontrivial infinitesimal number. The sequence $\tilde{r}$ is given by $\tilde{r}_n = n + 1$. So $[r]^{-1} = [\tilde{r}] > k$ for every positive integer k. $[r]^{-1}$ is a hyperreal larger than any real number. This is our first "infinite" number.

Note that if s is the sequence given by $s_n = \frac{1}{n+1+\left(\frac{1}{n+1}\right)}$ for $n \in \mathbb{N}$ then $[s] < [r]$. So the order structure on infinitesimals will reflect rather delicate information about the *rate* at which "most" of its terms converge to 0, not merely that they do so.

Define $\mathbb{I}$ to be the set of hyperreals z for which $|z| < x$ for all $x \in \mathbb{R}$. These are the **infinitesimal** hyperreals. Let $\mathbb{L}$ denote the set of hyperreals z for which there are real numbers a and b with $a < z < b$. These are the **limited** hyperreals.

23.4. ***Exercise.*** *(i) Show that $\mathbb{I}$ is an ideal in $\mathbb{L}$. What do you think the quotient $\mathbb{L}/\mathbb{I}$ looks like?*

*(ii) Since ${}^*\mathbb{R}$ is an ordered field and is not isomorphic to $\mathbb{R}$ it **cannot** be Dedekind complete. We can prove this directly. $\mathbb{N}$ is bounded above by the member $[t] \in {}^*\mathbb{R}$, where t is the sequence given by $t_n = n$ for all $n \in \mathbb{N}$. But $\mathbb{N}$ can have no least upper bound: if $n \le c$ for all $n \in \mathbb{N}$ then $n \le c - 1$ for all $n \in \mathbb{N}$. As another example consider $\mathbb{I}$. This set is (very) bounded, but has no least upper bound.*

24. Factorization

For any commutative ring R an element a is said to be a **factor** of an element b if there is an element c with $b = ac$. The phrase "a is a factor of b in R" is used when a, b and c are in R and specificity is required. Elements a and b are said to be **associates** if a is a factor of b and b is a factor of a.

A nonzero nonunit v is called **irreducible** if all factors of v are either associates of v or units. Obviously, if v is irreducible and u a unit then uv is irreducible.

A nonzero nonunit p is called **prime** if, whenever p is a factor of ab then p is a factor of a or p is a factor of b.

24.1. ***Exercise.*** *(i) In an integral domain a and b are associates exactly when $a = cb$ for some unit c. Association is an equivalence relation on the ring.*

(ii) For nonzero nonunit p in a principal ideal domain, p is irreducible, p is prime and (p) is a prime ideal are equivalent properties.

(iii) Show that the definition of prime used here agrees with the definition of prime integer we gave in the ring $\mathbb{Z}$ for positive integers. The exclusion of negative integers from the prime integers is by convention.

An integral domain is called a **unique factorization domain** if every nonzero nonunit g can be written as a product $g = a_1 \cdots a_n$ where each a_i is irreducible and if this factorization is, essentially, unique. By this we mean that if $g = b_1 \cdots b_L$ is another factorization of this kind then $L = n$ and there is a permutation σ of the subscripts so that b_i is an associate of $a_{\sigma(i)}$ for each i.

24.2. ***Exercise.*** *Let R be the ring of real valued functions on $\mathbb{R}$. If s is the sine function and c the cosine function then $\mathbb{R}(s, c)$ is a subring of R and an integral domain, though it takes techniques from calculus to show this. But $s^2 = (1-c)(1+c)$ so $\mathbb{R}(s, c)$ is not a unique factorization domain.*

24.3. ***Proposition.*** *Principal ideal domains are unique factorization domains.*

Proof. We first show essential uniqueness of these factorizations, should they exist. Suppose, for nonzero nonunit g and certain irreducible a_i and b_j and $1 < n \leq L$ that $g = a_1 \cdots a_n = b_1 \cdots b_L$. If a_1 is not an associate of any of the b_i then $(a_1) + (b_j) = (1)$ for each j so there are elements c_j and f_j with $c_j b_j = 1 - f_j a_1$ for each j. But then there is a k with

$$c_1 \cdots c_L a_1 \cdots a_n = c_1 \cdots c_L p = (1 - f_1 a_1) \cdots (1 - f_L a_1) = 1 - k a_1$$

and so $1 = a_1(k + c_1 \cdots c_L a_2 \cdots a_n)$ which is impossible because a_1 is a nonunit.

So a_1 is an associate of at least one of the b_j. Any failure of essential uniqueness therefore could be used to produce a failure when one of the two factorizations consists of a single irreducible, which obviously cannot happen.

It remains to show that factorizations consisting of irreducibles always exist for nonzero nonunit g. The ideal (g) is contained in maximal ideal (f_1) and f_1 is irreducible so $g = h_1 f_1$ for some h_1. If h_1 is a unit or itself irreducible we are done. Otherwise (h_1) is contained in maximal ideal (f_2) for irreducible f_2 and then $g = h_2 f_2 f_1$ for some h_2.

Note that in this event $(g) \subset (h_1)$ but $h_1 \notin (g)$ else $h_1 = gk = h_1 f_1 k$ which would imply that f_1 is a unit in this integral domain, contrary to the assumption that (f_1) is a maximal ideal.

Back to the construction, if h_2 is irreducible or a unit we are done. Otherwise we can continue this process. But sooner or later this procedure must terminate with the desired factorization, or it could be used to produce an infinite chain of unequal proper ideals

$$(p) \subset (h_1) \subset (h_2) \subset \cdots$$

which is impossible in a principal ideal domain. □

An element a in a commutative ring R is called a **least common multiple** of a nonempty set A of nonzero members of R if every member of A is a factor of a, and if every member of A is a factor of b then a is a factor of b too.

An element a is called a **greatest common factor** of a nonempty set A of nonzero members of R if a is a factor of every member of A, and if b is a factor of every member of A then b is a factor of a too.

24.4. ***Exercise.*** *(i) In a unique factorization domain R, greatest common factors exist for any nonempty set A of nonzero members of R. The set of all these forms an associate class which we denote* $\mathbf{GCF(A)}$.

(ii) In a unique factorization domain R, least common multiples exist for any nonempty ***finite*** *set A of nonzero members of R. The set of all these forms an associate class which we denote* $\mathbf{LCM(A)}$.

(hint: If $A = \{a_1, \ldots a_n\}$ show that each a_i can be written as $a_i = c_i d_1^{n_{i,1}} \cdots d_L^{n_{i,L}}$ where each c_i is a unit and the d_k are ***distinct*** *irreducibles and each $n_{i,L} \geq 0$, where we interpret any factor d_k^0 to be the identity. Produce $LCM(A)$ and $GCF(A)$ and then show that it suffices to consider finite sets for part (i).*

Suppose R is a unique factorization domain. The **content of $\mathbf{f} \in \mathbf{R}[\mathbf{x}]$** is the associate class of any greatest common factor of the nonzero coefficients of f. It is denoted $\mathbf{content(f)}$. The polynomial f is called **primitive** if the content of f is the class of units. If $a \in content(f)$ then $f = ag$ where g is primitive. It is obvious that if $c \neq 0$ in R then $ca \in content(cf)$ exactly when $a \in content(f)$.

24.5. ***Proposition.*** *Suppose R is a unique factorization domain and f and g are nonzero members of $R[x]$. If $a \in content(f)$ and $b \in content(g)$ then $ab \in content(fg)$.*

Proof. It is obvious that ab is a factor of any member of $content(fg)$ so the result will follow if we can show that fg is primitive whenever both f and g are primitive.

Let f_i denote the degree i coefficient for f whenever that coefficient is nonzero and define f_i for all other i in $\mathbb{Z}$ to be 0, with a similar definition for g_i for $i \in \mathbb{Z}$.

So $fg = \sum_p \left(\sum_i f_i g_{p-i}\right) x^p$ where each sum is over $\mathbb{Z}$, though only finitely many terms in each sum are nonzero.

Suppose both f and g are primitive but d is an irreducible factor of an element (any element) of $content(fg)$.

Since f is primitive there is an i_1 so that $f_i = 0$ or d is a factor of f_i for $i < i_i$ but d is not a factor of nonzero f_{i_1}.

Since g is primitive there is a j_1 so that $g_j = 0$ or d is a factor of g_j for $j > j_i$ but d is not a factor of nonzero g_{j_1}.

If $p = i_1 + j_1$ the coefficient of x^p in fg is $\sum_i f_i g_{p-i}$. Letting $k = i_1 - i$ this is $\sum_k f_{i_1-k} g_{j_1+k}$. d is a factor of every nonzero term in this sum except nonzero $f_{i_1} g_{j_1}$ so d does not divide the coefficient of this term, contradicting the fact that d is an irreducible factor of a member of $content(fg)$.

So there are no irreducible factors of any member of $content(fg)$ when both f and g are primitive. The result follows. □

24.6. ***Exercise.*** *Suppose R is a unique factorization domain and F the field of quotients of R.*

A member $\frac{a}{b}$ of F is said to be in ***lowest terms*** *if a and b have no irreducible factor in common.*

If f is a generic member of $F[x]$ you may presume that f is given initially with nonzero coefficients in lowest terms. We let d_f be a selection of a least common

multiple of the denominators of the nonzero coefficients in f and n_f a selection of a greatest common factor of the nonzero numerators from f.

In this case $d_f f$ is in $R[x]$ and the content of $d_f f$ is the class of n_f.

24.7. ***Proposition.*** *Suppose $f \in R[x]$. Then f can be factored as a product of two members of $R[x]$ of first degree or higher if and only if f can be factored as a product of two members of $F[x]$ of first degree or higher.*

We conclude that f is irreducible in $R[x]$ precisely when it is primitive in $R[x]$ and irreducible in $F[x]$.

Proof. The implication in one direction is obvious, so we concentrate on the case of a factorization in $F[x]$ and show that it generates a factorization in $R[x]$. We use the last exercise and assume, first, that f is primitive. Suppose $f = pq$ where p and q are in $F[x]$ of degree 1 or higher. So $d_p d_q f = (d_p p)(d_q q)$ and the two factors on the right are in $R[x]$ with $n_p \in \mathit{content}(d_p p)$ and $n_q \in \mathit{content}(d_q q)$. So the contents of the left and right sides are the same. So there is a unit u with

$$d_p d_q u = n_p n_q.$$

But d_p has no factor in common with n_p, and d_q has no factor in common with d_q. So there are members w_p and w_q in R with $n_p = w_p d_q$ and $n_q = w_q d_p$.

Since $n_p \in \mathit{content}(d_p p)$ there is primitive $\widetilde{p} \in R[x]$ with $d_p p = n_p \widetilde{p}$. Since $n_q \in \mathit{content}(d_q q)$ there is primitive $\widetilde{q} \in R[x]$ with $d_q q = n_q \widetilde{q}$. Then

$$d_p d_q f = n_p \widetilde{p} n_q \widetilde{q} = w_p d_q w_q d_p \widetilde{p}\widetilde{q}.$$

It follows that $f = (w_p w_q \widetilde{p})\widetilde{q}$ is a factorization of the required type in $R[x]$.

The extension to the case where f is not primitive is trivial. □

24.8. ***Exercise.*** *If F is any field then $F[x]$ is a principal ideal domain and, therefore, a unique factorization domain. Use this fact and the last few results to conclude that $R[x]$ is a unique factorization domain whenever R is a unique factorization domain. So is $R[x, y]$, the polynomial ring in two variables. (hint: $R[x, y] = R[x][y]$.)*

A polynomial $p \in R[x]$ is said to **split in R[x]** if it can be written as a product consisting entirely of first degree factors from $R[x]$.

24.9. ***Exercise.*** *When R is isomorphic to a subring of some field F, we let (for the purposes of this exercise) $\widetilde{p} \in F[y]$ denote the polynomial associated with $p \in R[x]$ by a specific isomorphism.*

*If R is any unique factorization domain and $p \in R[x]$ there is a field F, which may depend on p, for which $\widetilde{p}$ splits in $F[y]$. The reader is invited to ponder the existence of a single field F for which **any** $\widetilde{p}$ splits. In this regard it is interesting to note that any polynomial in $\mathbb{C}[x]$ splits. It is also interesting that all the proofs I have seen of this fact are essentially analytical, relying on order, connectedness and other properties of $\mathbb{R}$, and in that sense are not purely algebraic.*

25. Coprime, Primary, Prime and Maximal Ideals

We define $\boldsymbol{\mathcal{J}ac(R)}$ to be the intersection of all the maximal ideals of R. In a nontrivial commutative ring with identity there are always maximal ideals. In particular, each nonunit is contained in a maximal ideal. So for nontrivial R, $\mathcal{J}ac(R)$ is nonempty and therefore an ideal, called the **Jacobson radical of R**.

25.1. ***Proposition.*** *We suppose that R is a nontrivial commutative ring with identity. $a \in \mathcal{J}ac(R)$ if and only if $1 + ab$ is a unit for every $b \in R$.*

Proof. If $1 + ab$ is not a unit then $(1 + ab)$ is contained in a maximal ideal M. If $a \in \mathcal{J}ac(R)$ then $a \in M$ so $ab \in M$ so $1 \in M$, which is impossible. So $1 + ab$ must be a unit whenever $a \in \mathcal{J}ac(R)$.

Now suppose a is not in some maximal ideal M. So $(a) + M = R$. So there are members $m \in M$ and $r \in R$ with $m + ar = 1$. So $1 + a(-r) \in M$ and we have found a member $b = -r$ of R for which $1 + ab$ is not a unit. □

We define $\boldsymbol{\mathcal{N}il(R)} = \{x \in R \mid \ x^n = 0 \ \text{ for some positive integer } n\ \}$. The set $\mathcal{N}il(R)$ is called the **nilradical of R**. Elements of $\mathcal{N}il(R)$ are called **nilpotent.**

We generalize this to define the **radical of an ideal J** to be $\boldsymbol{\mathcal{R}ad(J)} = \{x \in R \mid \ x^n \in J \ \text{ for some positive integer } n\ \}$.

25.2. ***Exercise.*** *Suppose R is a nontrivial commutative ring and P is a prime ideal in R. Because P is an ideal, a nonempty set $A \subset P$ exactly when $(A) \subset P$. Because P is prime, this happens exactly when $\mathcal{R}ad((A)) \subset P$.*

25.3. ***Exercise.*** *If R is a nontrivial commutative ring $\mathcal{N}il(R)$ is an ideal. More generally, if J is an ideal in nontrivial commutative R, $\mathcal{R}ad(J)$ is an ideal.*

25.4. ***Exercise.*** *Suppose that R is a nontrivial commutative ring with identity.*

(i) Show that $\mathcal{N}il(R)$ is the intersection of all prime ideals in R.

Since 0 is in every ideal, it is obvious that every nilpotent element must be in every prime ideal. So we need only show that if a is not a member of $\mathcal{N}il(R)$ then there is a prime ideal which does not contain a.

(hint: Suppose a is not in $\mathcal{N}il(R)$. Let S denote the set of ideals which do not contain any positive power of a. S is not empty because the trivial ideal is in S. Show that if M is maximal in S then $x, y \notin M$ implies $xy \notin M$ so M is prime.)

(ii) If a subset A of R is contained in any ideal then so too must be all of (A). This implies that $\mathcal{R}ad((A))$ is in every prime ideal containing A.

(iii) If A is a proper ideal show that $\mathcal{R}ad(A)$ is the intersection of all prime ideals containing A.

A proper ideal P in a commutative ring R is called **primary** if whenever $x, y \in R$ and $xy \in P$ and $x \notin P$ then $y^n \in P$ for some positive integer n. In particular, in a commutative ring any prime ideal is primary.

25.5. ***Exercise.*** *Show that if P is primary in a commutative ring with identity then $\mathcal{R}ad(P)$ is a prime ideal.*

25.6. ***Exercise.*** *We suppose that R is a nontrivial commutative rings with identity and A is a proper ideal in R.*

(i) A is a primary ideal if and only if each zero divisor in R/A is in $\mathcal{N}il(R/A)$.

(ii) A is a prime ideal if and only if R/A is an integral domain.

(iii) A is a maximal ideal if and only if R/A is a field.

Among other things, we conclude from this exercise (as also implied by Exercise 25.4) that maximal ideals are prime in a commutative ring with identity.

25.7. ***Exercise.*** *Suppose P is a proper ideal in a nontrivial commutative ring R with identity. Show that if $\mathcal{R}ad(P)$ is maximal then P is primary. (hint: R/P has only one prime ideal, namely $\mathcal{R}ad(P)/P$. So $\mathcal{R}ad(P)/P = \mathcal{N}il(R/P)$.)*

25.8. ***Exercise.*** *Suppose R is a nontrivial commutative ring with identity. Show that if for each member x of R there is an integer $n \geq 2$ with $x^n = x$ then every prime ideal is maximal. (hint: If J is prime show that R/J is a field.)*

25.9. ***Exercise.*** *We suppose that R and S are nontrivial commutative rings with identity and $w \in Hom_{ring}(R, S)$.*

(i) If P is a primary ideal in S then $w^{-1}(P)$ is a primary ideal in R.

(ii) If Q is a primary ideal in R containing $Ker(w)$ and $Image(w) = S$ then $w(Q)$ is a primary ideal in S.

(iii) If P is a prime ideal in S then $w^{-1}(P)$ is a prime ideal in R.

(iv) If Q is a prime ideal in R containing $Ker(w)$ and $Image(w) = S$ then $w(Q)$ is a prime ideal in S.

(v) If P is a maximal ideal in S then $w^{-1}(P)$ need not be a maximal ideal in R. (hint: let w be the natural embedding of $\mathbb{Z}$ into $\mathbb{Q}$.) If $Image(w) = S$, however, $w^{-1}(P)$ will be maximal.

(vi) If Q is a maximal ideal in R containing $Ker(w)$ and $Image(w) = S$ then $w(Q)$ is a maximal ideal in S.

25.10. ***Exercise.*** *Suppose R is a nontrivial commutative ring with identity. Let S be the set of all prime ideals containing a given proper ideal J. S is nonempty and S contains both maximal and minimal members with respect to containment ordering. The maximal members are maximal ideals in R.*

25.11. ***Lemma.*** *Suppose $P_1, \ldots P_n$, with $n > 1$, is a list of pairwise coprime ideals in a nontrivial commutative ring R with identity. Let $Q_1 = (P_2 \cdots P_n)$. Then P_1 and Q_1 are coprime.*

Proof. For each i with $1 < i \leq n$ let $f_i \in P_1$ and $g_i \in P_i$ and $1 = f_i + g_i$. So $1 = (f_2 + g_2)(f_3 + g_3) \cdots (f_n + g_n)$. Expanded completely, this product is a sum of multiples of the various f_i, each of which is in P_1, plus one term $g_2 g_3 \cdots g_n$ in Q_1. So P_1 and Q_1 are coprime. □

25.12. ***Proposition.*** *(The **Chinese Remainder Theorem**) Suppose $P_1, \ldots P_n$, for $n > 1$, is a list of pairwise coprime proper ideals in a nontrivial commutative ring R with identity, and $a_i \in R$ for $i = 1, \ldots, n$. Then there is an element $b \in R$ for which $b \equiv a_i \ mod \ P_i$ for $i = 1, \ldots, n$. Also, if c is any other element of this kind then $b \equiv c \ mod \ \cap_{i=1}^{n} P_i$.*

Proof. Suppose $n = 2$. Find $c_1 \in P_1$ and $c_2 \in P_2$ with $1 = c_1 + c_2$ and let $b = c_1a_2 + c_2a_1$. Then $b + P_1 = c_1a_2 + (1 - c_1)a_1 + P_1 = a_1 + P_1$ and similarly $b + P_2 = a_2 + P_2$. So we have an element b of the kind we want in the case of a pair of coprime ideals. We now consider the general case of n ideals for $n > 2$.

For each k with $1 \leq k \leq n$ we define the ideal Q_k to be the ideal generated by all products of $n-1$ elements of R of the form $c_1 \cdots c_{k-1} \cdot c_{k+1} \cdots c_n$ where $c_i \in P_i$ for $i \neq k$. Note: the products used to create Q_k do not contain factors from P_k, but all these products do contain factors from P_i for $i \neq k$.

Appealing to Lemma 25.11, P_i and Q_i are coprime for each $i = 1, \ldots, n$. So we can find for each i an element r_i in R with $r_i + P_i = 1 + P_i$ and $r_i + Q_i = Q_i$. Now let $b = \sum_{i=1}^{n} a_i r_i$.

Since $r_i \in P_k$ whenever $k \neq i$ we have $b \equiv a_i \ mod\ P_i$ for each i.

If c is another member of R and $c \equiv a_i \ mod\ P_i$ for each i then $b - c \equiv 0 \ mod\ P_i$ for each i: that is, $b \equiv c \ mod \cap_{i=1}^{n} P_i$. □

25.13. ***Exercise.*** *Use the Chinese Remainder Theorem to prove the following statement. Suppose $P_1, \ldots, P_n$ is a finite list of pairwise coprime proper ideals in a nontrivial commutative ring R with identity. Let Q stand for the ideal $\cap_{i=1}^{n} P_i$. Then R/Q is ring isomorphic to $R/P_1 \times \cdots \times R/P_n$.*

25.14. ***Exercise.*** *Suppose $P_1, \ldots, P_n$ is a finite list of pairwise coprime proper ideals in a nontrivial commutative ring R with identity. Fill in the details in the following argument to show that $(P_1 \cdots P_n) = \cap_{i=1}^{n} P_i$.*

If $n = 2$ and $c \in P_1 \cap P_2$ find $c_1 \in P_1$ and $c_2 \in P_2$ with $c_1 + c_2 = 1$. So $c = c(c_1 + c_2) = cc_1 + cc_2$ represents c explicitly as a member of (P_1P_2) so $P_1 \cap P_2 \subset (P_1P_2)$. The reverse containment is obvious so we have the result in case $n = 2$.

Now observe that $(P_1 \cdots P_n) = ((P_1 \cdots P_{n-1})P_n)$ and recall (Lemma 25.11) that $(P_1 \cdots P_{n-1})$ and P_n are coprime. The result follows by induction.

25.15. ***Exercise.*** *Suppose $M_1, \ldots, M_n$ is a finite list of maximal ideals in a nontrivial commutative ring R with identity. Then $(M_1 \cdots M_n) = \cap_{i=1}^{n} M_i$.*

25.16. ***Exercise.*** *Suppose that there are n holidays and the ith holiday occurs periodically with period p_i days for $i = 1, \ldots, n$. Suppose that each of these periods is relatively prime to every other period. Then there is a day upon which all of these holidays occur simultaneously. These "common holiday" days occur periodically, with period $p_1 \cdots p_n$.*

25.17. ***Exercise.*** *Suppose $P_1, \ldots, P_n$ is a finite list of prime ideals in a nontrivial commutative ring with identity. Suppose J is an ideal and $J \subset \cup_{i=1}^{n} P_i$. Follow the argument below to conclude that $J \subset P_i$ for at least one i.*

First suppose (renumbering if necessary) that all superfluous P_i have been deleted at the outset: that is, if any of the P_i are removed the union no longer contains J. We would like to conclude that $n = 1$. If $n > 1$ then for each i there is a member $a_i \in J \cap P_i$ but $a_i \notin P_j$ for $j \neq i$. Let b_i be the product of these a_j for all $j \neq i$. There are $n - 1$ terms in each product. Because each P_i is a prime ideal $b_i \in P_j$ precisely when $i \neq j$. Also $b_i \in J$ for each i.

So $b_1 + \cdots + b_n \in J$ but this sum is not in any of the P_i. This contradiction implies that $n = 1$.

25.18. ***Exercise.*** *Suppose $J_1, \ldots, J_n$ is a finite list of ideals in a commutative ring with identity. Suppose P is a prime ideal and $\cap_{i=1}^n J_i \subset P$. Then $J_i \subset P$ for at least one i. (hint: if not pick $a_i \in J_i - P$ for each i. So $a_1 \cdots a_n$ is in $\cap_{i=1}^n J_i$.)*

25.19. ***Exercise.*** *In $\mathbb{Z}$ the prime ideals are of the form (p) and the primary ideals of the form (p^n) where p or $-p$ is a prime integer and n is some positive integer.*

26. The Prime Spectrum

Suppose R is a nontrivial commutative ring with identity. Let $\mathbf{Spec(R)}$ denote the set of prime ideals in R. If $A \subset R$ define the subset $In(A) \subset Spec(R)$ to be the set of all prime ideals containing A. For $a \in R$ define $Out(a) \subset Spec(R)$ to be those prime ideals not containing a. For $A \subset R$ define $\widetilde{Out}(A) \subset Spec(R)$ to be $\cup_{a \in A} Out(a)$. The prime ideals in $\widetilde{Out}(A)$ are missing at least one member of A.

Let $\mathbb{K}$ denote the family $\{\ In(A) \mid A \subset R\ \} \subset \mathbb{P}(Spec(R))$.

26.1. ***Exercise.*** *(i) Suppose W is any subset of $Spec(R)$ with the property that $Q \in Spec(R)$ and $P \in W$ and $P \subset Q$ implies $Q \in W$. Then W consists exactly of those prime ideals containing the ideal P_W defined to be $\cap_{P \in W} P$. P_W won't generally be prime but $\mathcal{R}ad(P_W) = P_W$. Also, $W = In(P_W)$. Moreover, if $W = In(A)$ then $P_W = \mathcal{R}ad((A))$.*

(ii)
$$\begin{aligned} \mathbb{K} &= \{\ In(A) \mid A \subset R\ \} \\ &= \{\ In(A) \mid A \text{ is an ideal in } R\ \} \\ &= \{\ In(A) \mid A \text{ is an ideal in } R \text{ and } \mathcal{R}ad(A) = A\ \}. \end{aligned}$$

26.2. ***Exercise.*** *$In(A) \cup \widetilde{Out}(A) = Spec(R)$ and $In(A) \cap \widetilde{Out}(A) = \varnothing$.*

26.3. ***Exercise.*** *Verify: (i) $Spec(R) = In(\{0\})$ and $\varnothing = In(\{1\})$.*

(ii) $In(A) = \bigcap_{a \in A} In(\{a\})$. It follows immediately that $\mathbb{K}$ is closed under arbitrary intersections.

(iii) $In(A) \cup In(B) = In((A)) \cup In((B)) = In((A) \cap (B))$. So $\mathbb{K}$ is closed under finite unions.

This exercise shows that sets of the form $In(A)$ satisfy the conditions on closed sets for a topology.

The topology consisting of complements of these closed sets is called the **Zariski topology** and $Spec(R)$ with this topology is called the **prime spectrum of R.** The set of maximal ideals is denoted $\mathbf{Max(R)}$ and when endowed with the subspace topology is called the **maximal spectrum of R.**

Any open set is of the form $Spec(R) - In(A) = \widetilde{Out}(A) = \bigcup_{a \in A} Out(a)$. Each $Out(a) = Spec(R) - In(\{a\})$ is open. So sets of the form $Out(a)$ constitute a base for the Zariski topology.

26.4. ***Exercise.*** *Verify: (i) $Out(a) \cap Out(b) = Out(ab)$ $\forall a, b \in R$*

(ii) $\mathcal{N}il(R)$ is the intersection of all prime ideals of R so $a \in \mathcal{N}il(R)$ if and only if $Out(a) = \varnothing$.

(iii) No unit is in any prime ideal but every nonunit is in at least one. So a is a unit if and only if $Out(a) = Spec(R)$.

26.5. ***Exercise.*** *Verify the following argument to show that every basic open set $Out(x)$ (including $Out(1) = Spec(R)$ itself) is compact.*

To prove this we will assume that the open cover is of the form $\{\ Out(a) \mid a \in A\ \}$, a collection of basic open sets. This means that $Out(x) \subset \cup_{a\in A} Out(a) = \widetilde{Out}(A) = Spec(R) - In(A)$. Any prime ideal not containing x cannot contain all of A either. So x is in every prime ideal containing A: that is, $x \in \mathcal{R}ad((A))$. So $x^n \in (A)$ for some integer n. So there is a finite listing $a_1, \ldots, a_n$ of members of A and a listing $r_1, \ldots, r_n$ of members of R with $\sum_{i=1}^n r_i a_i = x^n$. If a prime ideal does not contain x then it must be missing at least one of these a_i. So $Out(x) \subset \cup_{i=1}^n Out(a_i)$.

26.6. ***Exercise.*** *Suppose A is an open subset of $Spec(R)$. A is compact precisely when A is a finite union of basic open sets.*

26.7. ***Exercise.*** *The closure of a set $S \subset Spec(R)$ with this topology is denoted $\overline{S}$. If P is prime, $\overline{\{P\}} = In(P)$. So the only closed points in $Spec(R)$ are maximal ideals. In case all prime ideals are maximal, points in $Spec(R)$ are closed: that is, $Spec(R)$ is a T_1 space.*

In any case, given any pair of distinct prime ideals P, Q, it cannot happen that $Q \in In(P) = \overline{\{P\}}$ and also $P \in In(Q) = \overline{\{Q\}}$. So $Spec(R)$ is always a T_0 space: given any pair of prime ideals there is a basic open set containing one of the two but not the other.

26.8. ***Exercise.*** *(i) Suppose $w\colon R \to S$ is a ring homomorphism. Because $w^{-1}(P)$ is prime in R whenever P is prime in S, the function w induces a function $w^*\colon Spec(S) \to Spec(R)$ defined by $w^*(P) = w^{-1}(P)$.*

*(ii) This map does not necessarily take maximal ideals to maximal ideals, however. But if w is onto S it **does** and induces a one-to-one function from the subspace $Max(S)$ of $Spec(S)$ to $Max(R)$. If, further, $Ker(w) \subset \mathcal{J}ac(R)$ then this induced map is onto $Max(R)$.*

(iii) If $v\colon S \to T$ is another ring homomorphism then $(v \circ w)^*\colon Spec(T) \to Spec(R)$ and $(v \circ w)^* = w^* \circ v^*$.

(iv) Suppose $Out(r)$ is a basic open set in $Spec(R)$. Then ${w^*}^{-1}(Out(r)) = \{\ P \in Spec(S) \mid w(r) \notin P\ \} = Out(w(r))$. So w^* is a continuous function.

(v) $Ker(w) \subset \mathcal{N}il(S)$ if and only if $Image(w^*)$ is dense in $Spec(R)$.

(vi) If $Image(w) = S$ then w^* is a homeomorphism of $Spec(S)$ onto $In(Ker(w))$.

(vii) If $A \subset R$ then ${w^*}^{-1}(In(A)) = In(w(A))$.

(viii) If $B \subset S$ then $\overline{w^*(In(B))} = In(w^{-1}(B))$.

27. Modules

If R is a ring, a **left R-module** is an additive abelian group V together with a function $\odot\colon R \times V \to V$ called **scalar multiplication** with certain properties to be listed below. The notation rv will be used to mean $\odot(r, v)$ for $r \in R$ and $v \in V$. The properties are:

$$r(v + w) = rv + rw \quad (r + s)v = rv + sv \quad r(sv) = (rs)v \quad \forall r, s \in R \text{ and } v, w \in V.$$

Note that scalar multiplication is not an action of $(R, +)$ on the set V unless $rv = 0\ \forall r \in R, v \in V$. But scalar multiplication will generate an action of the nonzero members of R on V provided R is a division ring and $1v = v\ \forall v \in V$.

Scalar multiplication always has the member of R on the left: that is the significance of the word "left" in the name "left R-module." We will have no occasion to discuss any other kind of scalar multiplication, so we drop the word "left" in our discussion below.

If R has a multiplicative identity and $1v = v\ \forall v \in V$ the R-module is called **unitary.** If R is a field, a unitary R-module is called a **vector space over R**.

A **subR-module** of an R-module V is a subgroup of V which is also an R-module with scalar multiplication that agrees with that on V. If R is a field, a sub**R**-module is called a **vector subspace** (or simply a subspace) of V.

Most of the R-modules in this work will be vector spaces over $\mathbb{R}$, but other types are found in many branches of mathematics.

A ring R is, itself, an R-module with the obvious scalar multiplication as is any ideal of R. Also, if G is an abelian group we saw in Section 11 that G is a unitary $\mathbb{Z}$-module in a natural way, though we did not use this vocabulary in that section, regarding the scalar multiplication as a notational convenience to indicate iterated addition or subtraction.

The quaternions $\mathbb{H}$ and the complex numbers $\mathbb{C}$ are both vector spaces over $\mathbb{R}$. These two, and $\mathbb{R}$ itself, are also vector spaces over $\mathbb{Q}$.

If $R[x]$ is the set of all polynomials of finite degree in the variable x with coefficients in the ring R then $R[x]$ is an R-module with the obvious scalar multiplication.

We can generalize this last example in two ways at once. If A is a nonempty set and J an ideal in the ring R let J^A denote the set of all functions from A to J. If $f \in J^A$ and $r \in R$ define rf to be the function given by $(rf)(a) = r(f(a))$. This operation makes J^A into an R-module.

$M_n(R)$ is an R-module with the obvious scalar multiplication.

If M and N are two R-modules we make $M \times N$ into an R-module by $(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2)$ and $r(m, n) = (rm, rn)$. This is called the **product module of M and N**.

More generally, if A is a nonempty set and M_a is an R-module for each $a \in A$ let $H = \cup_{a \in A} M_a$ and define $\prod_{\mathbf{a} \in \mathbf{A}} \mathbf{M_a}$ to be the set of all functions $f\colon A \to H$ with $f(a) \in M_a\ \forall a \in A$. This set of functions is an additive group with operation $(f + g)(a) = f(a) + g(a)\ \forall a \in A$. The abelian group $\prod_{a \in A} M_a$ is an R-module with scalar multiplication $(rf)(a) = rf(a)\ \forall a \in A$ and $r \in R$. This R-module is called the **direct product of the $\mathbf{M_a}$**.

There is an interesting sub$R$-module of $\prod_{a \in A} M_a$. It consists of those members of $\prod_{a \in A} M_a$ which are 0 except at finitely many $a \in A$. It is denoted $\sum_{\mathbf{a} \in \mathbf{A}} \mathbf{M_a}$, and called the **direct sum of the $\mathbf{M_a}$**. Obviously, if A is finite, the direct product and direct sum coincide.

If $w\colon V \to W$ is a member of $Hom(V, W)$ where V and W are both R-modules we call w an **R-module homomorphism** provided $w(rv) = rw(v)\ \forall r \in R$ and

$v \in V$. The set of all members of $Hom(V, W)$ which are R-module homomorphisms is denoted $\mathbf{Hom_{R-mod}(V, W)}$.

Members of $Hom_{R-mod}(V, W)$ are customarily called **linear transformations** when R is a field and V and W are vector spaces over R.

In case an R-module homomorphism w as above has an inverse then the inverse is also an R-module homomorphism and w is called an **R-module isomorphism**. V and W are called **isomorphic R-modules** by virtue of the existence of an R-module isomorphism between them.

If $M_a,\ a \in A$ are all sub$R$-modules of an R-module M define $\Phi\colon \sum_{a\in A} M_a \to M$ by $\Phi(f) = \sum_{a\in A} f(a)$. Then Φ is an R-module homomorphism and $Image(\Phi)$ is a sub$R$-module of M. In case $\Phi(f) = \Phi(g)$ implies $f = g$ we say that $Image(\Phi)$ is the **internal direct sum of the $\mathbf{M_a}$**. The notation $\bigoplus_{a\in A} M_a$ is used to indicate $Image(\Phi)$ in this case. Often Φ is onto M. Note that if $M = \bigoplus_{a\in A} M_a$ then M is R-module isomorphic to $\sum_{a\in A} M_a$.

If V and W are R-modules then $Hom_{R-mod}(V, W)$ is a subgroup of $Hom(V, W)$ with addition of homomorphisms. $Hom_{R-mod}(V, W)$ is itself an R-module with scalar multiplication defined for $r \in R$ and $f \in Hom_{R-mod}(V, W)$ by $(rf)(v) = r(f(v))\ \forall v \in V$.

27.1. ***Exercise.*** *The set of matrices of a given size with entries in a ring R is an R-module in a natural way, unitary if R has an identity.*

$Hom_{R-mod}(V, V)$ also forms a semigroup with composition.

We define $\mathbf{Aut_{R-mod}(V)}$ to be $Perm(V) \cap Hom_{R-mod}(V, V)$. These homomorphisms are called the **R-module automorphisms of V**. They form a group with composition, and a subgroups of $Aut(V)$.

If N is any sub$R$-module of V define scalar multiplication on V/N by $r(v+N) = (rv) + N$. This makes V/N into a R-module, the **quotient module of V by N**. The function $w\colon V \to V/N$ defined by $w(v) = v+N$ is an R-module homomorphism and $Ker(w) = N$.

27.2. ***Exercise.*** *In Exercise 21.22 we showed that any ring R is ring isomorphic to a maximal ideal in a ring with identity. This larger ring was $\widetilde{R} = R \times \mathbb{Z}_2$ with multiplication $(r, a) \cdot (s, b) = (rs + as + br,\ ab)$. If V is an R-module we can make V into a unitary $\widetilde{R}$-module with scalar multiplication $(r, a)v = rv + av$. This gives a correspondence between members of $Hom_{R-mod}(V, W)$ and members of $Hom_{\widetilde{R}-mod}(V, W)$.*

If w is any member of $Hom_{R-mod}(V, W)$ then $Image(w)$ is a sub$R$-module of W and $Ker(w)$ is a sub$R$-module of V. So $V/Ker(w)$ is R-module isomorphic to $Image(w)$. Thus, sub$R$-module of V are precisely the kernels of R-module homomorphisms with domain V.

We can also conclude that any $w \in Hom_{R-mod}(V, W)$ provides a correspondence between sub$R$-modules of $Image(w)$ and sub$R$-modules of V which contain $Ker(w)$.

27.3. ***Exercise.*** *(i) If $X \in Hom_{R-mod}(V, W)$ and $Y \in Hom_{R-mod}(W, V)$ and if $Y \circ X(v) = v\ \forall v \in V$ then $Image(X) \cap Ker(Y) = \{0\}$ and W is R-module isomorphic to $Image(X) \times Ker(Y)$.*

(ii) If $w \in Hom_{R-mod}(V,V)$ and $w \circ w = w$ then V is R-module isomorphic to $Image(w) \times Ker(w)$.

(iii) If H and W are submodules of V and $H + W = V$ then V is R-module isomorphic to $(H/H \cap W) \times W$. So if $H \cap W = \{0\}$ then V is R-module isomorphic to $H \times W$.

27.4. ***Exercise.*** *According to our definitions, $R[x]$ and $\sum_{k\in\mathbb{N}} R$ are virtually identical. $R[x]$ **is actually identical**, as a set, to the subR-module V of $\sum_{k\in\mathbb{Z}} R$ consisting of all members f for which $f_k = 0$ whenever $k < 0$. And V is R-module isomorphic to $\sum_{k\in\mathbb{N}} R$. These three, $R[x]$, V and $\sum_{k\in\mathbb{N}} R$, are distinguished chiefly by context and the operations you intend to perform with these sets of functions. You are free to change your mind about that whenever it is convenient.*

27.5. ***Exercise.*** *Suppose V is an R-module for commutative R.*

*(i) If $v \in V$ define $\mathbf{Ann(R, v)}$ to be the set $\{r \in R \mid rv = 0\}$. $Ann(R, v)$ is an ideal of R called the **$\mathbf{R}$-annihilator of $\mathbf{v}$**. If $Ann(R, v) \neq \{0\}$ we call v a **torsion element of the $\mathbf{R}$-module $\mathbf{V}$**. The set of torsion elements of the R-module V is denoted $\mathbf{V_{tor}}$ and is an R-submodule of V when R is an integral domain.*

(ii) R itself can be regarded as an R-module. When R is commutative, the set of nonzero torsion elements is exactly the set of zero divisors in R.

*(iii) If $V_{tor} = \{0\}$ we call V **torsion-free**. If $V_{tor} = V$ we say V is a **torsion module**. When $\mathbf{V_{tor}}$ is an R-submodule of V then V/V_{tor} is torsion free and V is R-module isomorphic to $(V/V_{tor}) \times V_{tor}$.*

27.6. ***Exercise.*** *Suppose F is a field and n is a positive integer. Let G be a multiplicative subgroup of $M_n(F)$, the set of n by n matrices with entries in F.*

(i) There is an action of G on the additive group F^n given by left matrix multiplication: i.e. the action of $g \in G$ on $x \in F^n$ is given by gx. Each $g \in G$ induces a linear transformation on F^n, an F-module isomorphism.

What is the orbit of $y \in F^n$ under this action? When is the action transitive? Is representation corresponding to this action faithful? What is the stabilizer of $y \in F^n$?

(ii) $\mathbf{Aff(F^n, G)}$ is defined as the set $F^n \times G$ together with the semidirect product operation

$$(x, g)\,(y, h) = (x + gy,\ gh).$$

*$Aff(F^n, G)$ is then a nonabelian group (unless, of course, G consists solely of the identity matrix) as we saw in Section 19, and called the **affine group on $\mathbf{F^n}$ generated by $\mathbf{G}$**.*

$Aff(F^n, G)$ itself acts on the additive group F^n by $(x, g)\, y = x + gy$.

What is the orbit of $y \in F^n$ under this action? When is the action transitive? Must the representation corresponding to this action be faithful? Show that the stabilizer of $y \in F^n$ is $\{(y - gy, g) \mid g \in G\}$.

28. Basis and Dimension for Modules

Suppose S is a nonempty set in an R-module V. An **R-linear combination of the members of S** is a representation of a member of V as a specific finite sum of scalar multiples $r_1s_1 + r_2s_2 + \cdots + r_ns_n$ where each r_i is from R and each s_i is from S. The member $r_i \in R$ is called the **coefficient of the ith term in the sum.** If all the r_i are 0 or if some $s_i = s_j$ with $i \neq j$ we call the R-linear combination **trivial**, and **nontrivial** otherwise. In a nontrivial linear combination each coefficient is associated with a distinct member of S. The set S is called **R-linearly independent** if there are no nontrivial R-linear combinations of the members of S whose sum is 0.

If A is a nonempty subset of R and S a nonempty subset of the R-module V we define $\mathbf{AS} = \{as \mid a \in A \text{ and } s \in S\}$. If T is a nonempty subset of V let $\langle \mathbf{T} \rangle$ denote all finite sums of members of T. It is the additive subgroup generated by the members of T. The **R-span of S**, denoted $\mathbf{Span_R(S)}$ or $\langle \mathbf{RS} \rangle$, is the set of members of V which have a representation as an R-linear combination of members of S. Note that $\langle RS \rangle$ is, itself, an R-module, a sub$R$-module of V. Unless R has an identity, there is no reason to think that S will be contained in $\langle RS \rangle$.

28.1. ***Exercise.*** *(i) If R is a commutative ring with identity and A a nonempty subset of R then the ideal (A) generated by A is $\langle RA \rangle$.*

(ii) If G is an abelian group and B a nonempty subset of G then the subgroup of G generated by B is $\langle \mathbb{Z}B \rangle$.

(iii) Suppose R is a commutative ring with identity and A is the principle ideal pR. Suppose that V is an R-module. Then $\langle AV \rangle = AV = pV$.

If W is a sub$R$-module of V the subset S of V is said to **span the R-module W** provided $\langle RS \rangle = W$. If S is R-linearly independent and spans the R-module W and if $S \subset W$ we say that S is a **basis for the R-module W**. When R is a division ring the descriptor **Hamel basis** is used, to distinguish a basis in our sense from a somewhat different concept found in analysis.

Note that an R-linearly independent set S will not in general be a basis for the R-module $\langle RS \rangle$, because S will not necessarily be a subset of $\langle RS \rangle$. This is not an issue if the module is unitary.

When there is only one ring around, the repetitive reference to R is sometimes dropped and, for example, the phrase "linear combination" or "a basis for V" or "the span of S" is used for convenience.

28.2. ***Exercise.*** *(i) If the ring R has no zero divisors and S is a linearly independent subset of the R-module V then $\langle RS \rangle \cap V_{tor} = \{0\}$.*

(ii) If R is a division ring and V a unitary R-module then $V_{tor} = \{0\}$.

28.3. ***Exercise.*** *(i) Show that if S is a linearly independent set then each member of $\langle RS \rangle$ can be written as a linear combination of members of S in exactly one way. That means that there is one and only one function $r\colon \langle RS \rangle \times S \to R$ so that for each $v \in \langle RS \rangle$ there are only finitely many $b \in S$ for which $r(v, b) \neq 0$ and*

$$v = \sum_{b \in S} r(v, b)b \quad \forall v \in \langle RS \rangle.$$

(ii) If S is nonempty and linearly independent show that $\langle RS\rangle$ is R-module isomorphic to $\sum_{b\in S} Rb$, to $\bigoplus_{b\in S} Rb$ and also to $\sum_{b\in S} R$ where R is thought of as an R-module.

(iii) Suppose S is a basis for V and B is a nonempty subset of S and $A = S - B$ is nonempty. Show that $\langle RA\rangle \cap \langle RB\rangle = \{0\}$.

(iv) Define $Proj_B\colon \langle RS\rangle \to \langle RB\rangle$ by $Proj_B(v) = \sum_{b\in B} r_S(v,b)b$. Define $Proj_A$ in an analogous way. So for each $v \in V = \langle RS\rangle$ we have $v = Proj_A(v) + Proj_B(v)$. Observe that $Proj_B \in Hom_{R-mod}(\langle RS\rangle, \langle RB\rangle)$ and that $Proj_B(v) = v\ \forall v \in \langle RB\rangle$. Show that $Ker(Proj_B) = \langle RA\rangle$. Conclude that V is isomorphic to $\langle RB\rangle \times \langle RA\rangle$.

28.4. ***Exercise.*** *Suppose A is a proper ideal of R and V is an R-module. Suppose S is a subset of the R-module V.*

(i) $Span_A(S) = \langle AS\rangle$ is both an A-module and a subR-module of V and $V/\langle AS\rangle$ is an R-module with scalar multiplication $r(v + \langle AS\rangle) = rv + \langle AS\rangle$.

(ii) Even if S is R-linearly independent, S will not necessarily be a basis of the R-module $\langle AS\rangle$, because in general S will not be contained in $\langle AS\rangle$. Still, it will be possible to write every nonzero member of $\langle AS\rangle$ in a unique way as a nontrivial A-linear combination of members of S. In general $\langle AS\rangle = \langle A\langle AS\rangle\rangle = \langle AV\rangle$ but if S is a basis of the R-module V then $\langle AS\rangle = \langle AV\rangle$.

(iii) The function $Q\colon V \to V/\langle AS\rangle$ defined by $Q(v) = v + \langle AS\rangle$ is a member of $Hom_{R-mod}(V, V/\langle AS\rangle)$. Q is onto $V/\langle AS\rangle$.

(iv) $V/\langle AS\rangle$ can also can be made into an R/A-module using scalar multiplication $(r + A)(v + \langle AS\rangle) = rv + \langle AS\rangle$.

In the following proposition, if A is an ideal of R and $S \subset V$ for R-module V. We consider the function $Q\colon S \to V/\langle AV\rangle$ defined by $Q(v) = v + \langle AV\rangle$ and define $\widetilde{S} = Q(S)$.

28.5. ***Proposition.*** *Suppose A is an ideal in a ring R and V is an R-module.*

If S is a basis for the R-module V then $\widetilde{S}$ is a basis for the R/A-module $V/\langle AV\rangle$.

If R is a ring with identity and V is a unitary R-module and S is a basis for the R-module V then Q is one-to-one on S so $|S| = |\widetilde{S}|$.

Proof. Suppose S is a basis for the R-module V. So $Span_{R/A}(\widetilde{S}) = V/\langle AV\rangle$. Suppose that $0 + \langle AV\rangle = \langle AV\rangle = \sum_{i=1}^{n}(r_i + A)(s_i + \langle AV\rangle)$ for nonzero members $r_i + A \in R/A$ and distinct nonzero $s_i + \langle AV\rangle \in \widetilde{S}$. So $w = \sum_{i=1}^{n} r_i s_i \in \langle AV\rangle$ and none of the r_i are in A.

Since $w \in \langle AV\rangle$, w can be written as $w = \sum_{i=1}^{k} a_i v_i$ where each $a_i \in A$ and each $v_i \in V$. Each $v_i = \sum_{s\in S} t_{i,s}s$ for $t_{i,s} \in R$ where for each i only finitely many of the $t_{i,s}$ are nonzero. So $w = \sum_{i=1}^{k} a_i v_i = \sum_{i=1}^{k} a_i \sum_{s\in S} t_{i,s}s = \sum_{s\in S}\left(\sum_{i=1}^{k} a_i t_{i,s}\right)s$. Each coefficient on each $s \in S$ is explicitly a member of A (since A is an ideal) and these coefficients are unique in any nontrivial linear combination of members of S because S is a basis. But we already have a representation with coefficients *not* in A. This contradiction establishes the R/A-linear independence of $\widetilde{S}$ and so that set is a basis for the R/A-module $V/\langle AV\rangle$.

It remains to show the final assertion: that Q is one-to-one.

If $Q(s_1) = Q(s_2)$ for $s_1, s_2 \in S$ then $(s_1 + \langle AV\rangle) - (s_2 + \langle AV\rangle) = 0 + \langle AV\rangle$ as above. So $s_1 - s_2 = w \in \langle AV\rangle$. But then, as in the last paragraph, we can write w as a linear combination of members of S using coefficients from A. Since such coefficients are unique and 1 cannot be in A, we have a contradiction and conclude that Q is one-to-one. □

28.6. ***Proposition.*** *Suppose R is a division ring and V a unitary R-module and C a nonempty subset of V. Suppose A is empty or A is linearly independent and $A \subset C$. If C spans V then there is a basis B for V with $A \subset B \subset C$.*

Proof. Let S denote the set of all linearly independent subsets of C which contain A. S is nonempty, since $A \in S$ or any single element subset of C is in S. Let $W \subset S$ be a chain in S ordered by containment. The union Y of the chain is in C and contains A. Any linear combination of members of Y involves only a finite number of members of Y and so there is a member of the chain containing all these members. A nontrivial linear combination of members of Y cannot sum to 0 because each member of the chain is linearly independent.

So S contains a maximal member B.

If $v \in V - \langle RB\rangle$ then, since $(RC) = V$, there are elements $c_1, \ldots, c_n$ in C with $v = r_1c_1 + \cdots + r_nc_n$ for certain members $r_1, \ldots, r_n$ in R. If each of these members of C is in $\langle RB\rangle$ then so too is v, contrary to choice of v. Therefore at least one of the c_i is not in $\langle RB\rangle$. Let c be such a member of C. If $ac + r_1b_1 + \cdots + r_kb_k$ is any linear combination involving c whose sum is 0 then $ac = -r_1b_1 - \cdots - r_kb_k$. If a is nonzero then, since R is a division ring, we could multiply both sides by a^{-1} and have $c \in \langle RB\rangle$, contrary to choice of c. So $a = 0$. Now the linear independence of the members of B requires that each r_i be 0. But then we have shown that $\{c\} \cup B$ is linearly independent, contradicting the maximality of B.

So $V - \langle RB\rangle$ is empty: that is, $V = \langle RB\rangle$. □

28.7. ***Proposition.*** *Suppose R is a division ring and V a unitary R-module and A and B are both bases of V. Then $|A| = |B|$.*

Proof. Since A and B are both bases there are unique functions $r\colon V \times A \to R$ and $s\colon V \times B \to R$ so that

$$v = \sum_{a\in A} r(v,a)a \;=\; \sum_{b\in B} s(v,b)b \quad \forall v \in V$$

where for each v the sum is finite: r and s are nonzero for only finitely many members of A and B, respectively.

Suppose A is infinite. If $v \in V$ then

$$v = \sum_{b\in B} r(v,b)b = \sum_{b\in B} r(v,b)\left(\sum_{a\in A} s(b,a)a\right) \;=\; \sum_{a\in A}\left(\sum_{b\in B} r(v,b)s(b,a)\right)a.$$

If B is finite, the collection $\widetilde{A}$ of all members a of A for which $s(b,a)$ is nonzero for any b in B would be finite too. This finite collection of members of A are the only ones that could possibly have nonzero coefficients in the representation of generic $v \in V$ above. So a finite subset of infinite A spans V. In particular, there exists $t \in A - \widetilde{A}$. But then the equation $t = \sum_{a\in\widetilde{A}}\left(\sum_{b\in B} r(t,b)s(b,a)\right)a$ can be used to

form a nontrivial linear combination of members of A whose sum is zero, violating the assumption that A is linearly independent.

We conclude that A and B are both finite or both infinite.

Suppose both are infinite.

First note that if C is the set of all finite subsets of A then (see Exercise **??**) $|A| = |C| = |C \times \mathbb{N}|$.

For each $b \in B$ let S_b denote those members of A with $s(b, a) \neq 0$. So $b \in \langle RS_b \rangle$ and b is not in the span of any proper subset of S_b. For each S_b, the set $B \cap S_b$ must be finite. That is because if it were infinite it could be extended to an infinite basis of $\langle RS_b \rangle$. But $\langle RS_b \rangle$ has a finite basis, namely S_b, which would contradict our conclusion from the paragraph above.

Let K denote the subset of C consisting of all S_b for $b \in B$. For each $E \in K$ let E_B denote those members b of B with $E = S_b$. E_B is finite. Each member of B is in one and only one of the nonempty finite sets E_B. Well order B. Each E_B inherits the order from B.

Define a one-to-one function $f\colon B \to K \times \mathbb{N}$ by $f(b) = (E, n)$ where $E = S_b$ and b is the nth member of E_B.

So $|B| \leq |K \times \mathbb{N}| \leq |C \times \mathbb{N}| = |A|$. Switching the positions of A and B we have $|A| = |B|$ when both are infinite.

We now suppose both $|A|$ and B are finite. Let $b_1, \ldots, b_j$ be a listing of the elements of B and $a_1, \ldots, a_k$ a listing of the elements of A. We will assume that $j \leq k$ and that B is not a subset of A.

In that case there is at least one $a_p \in A - B$ and $a_p = s(a_p, b_1)b_1 + \cdots + s(a_p, b_j)b_j$. At least one of the coefficients must be nonzero. By relabeling if necessary suppose that $s(a_p, b_1) \neq 0$. Then

$$b_1 = -s(a_p, b_1)^{-1}a_p - s(a_p, b_1)^{-1}s(a_p, b_2)b_2 - \cdots - s(a_p, b_1)^{-1}s(a_p, b_j)b_j.$$

That means that b_1 can be replaced in B by a_p and the result is a new basis $\widetilde{B}$ for V with the same number of members as before and that has one more member in common with A than did B. This process can be continued until every member of B not already in A has been replaced: we will have a new basis $\widetilde{B}$ that has the same number of members as has B and which is a subset of A.

If k were actually greater than j then $A - \widetilde{B}$ would contain a member of A which could be written as a linear combination of the members of $\widetilde{B}$ which are all different members of A. This could be used to create a nontrivial linear combination whose sum is 0, violating our assumption that A is a basis.

So $|A| = |B|$ in the finite case too. □

Whenever an R-module V has a basis and if any two such have the same cardinal number we define the **dimension of V** to be the cardinal number of any basis of V. We have just shown that if R is a division ring V has a dimension.

28.8. ***Exercise.*** *Suppose F is a field and $(p) = pF[x]$ is a maximal ideal in $F[x]$. Then $F[x]/(p)$ is a vector space over F and its dimension is the degree of p.*

28.9. ***Exercise.*** *Suppose R is any ring with identity which has an ideal J for which R/J is a division ring. Commutative rings with identity have a maximal ideal and the quotient ring is then a field, so commutative rings with identity provide an example. Suppose V is a unitary R-module. If V has bases A and B then $|A| = |B|$.*

Note that we do not imply that V actually has a basis: only that if it has bases, they all have the same cardinality. (Hint: Use Propositions 28.5 and 28.7.)

28.10. ***Exercise.*** *Let H be a basis for $\mathbb{R}$ as a $\mathbb{Q}$-module. H is uncountable. Each $x \in \mathbb{R}$ has a representation as $x = \sum_{b\in H} r(x,b)b$ where the $\mathbb{Q}$-valued function r is uniquely defined and for each x is nonzero for only finitely many $b \in H$.*

Select $h \in H$ and define $f\colon \mathbb{R} \to \mathbb{R}$ by $f(x) = r(x,h)$. Then $f(x+y) = f(x)+f(y)$ for all $x, y \in \mathbb{R}$ but $f(\mathbb{R}) = \mathbb{Q}$ so f is not continuous.

28.11. ***Exercise.*** *(i) Suppose V is a vector space over a field F and that $|V|$ is finite. Then there is a prime integer k so that F has characteristic k and $|V| = mk$ where m is the cardinality of any basis for V.*

(ii) Suppose V is a finite field of order $|V|$ and characteristic k. Let W denote the subfield of V containing e, the identity. W is isomorphic to the field $\mathbb{Z}_k$. V can be regarded as a vector space over W. What is the dimension of V in terms of $|V|$ and k?

28.12. ***Exercise.*** *Suppose F is a field. Let R be the set of rational expressions with numerator and denominator from the unique factorization domain $F[x]$. Show that R is a field, and the characteristic of R is the same as that of F. R can be regarded as a vector space over F. What is its dimension?*

29. Algebras

If R is a commutative ring with identity and V is a unitary R-module and V is, itself, a ring we call V an **R-algebra** provided $r(ab) = (ra)b = a(rb)\ \forall r \in R$ and $a, b \in V$. If V is a division ring and an R-algebra it is called an **R-division algebra.** An R-algebra is called **commutative** if, as a ring, it is commutative. A **subR-algebra** is defined in the obvious way.

Many of the entities we have discussed have this structure. Among others, both the complex numbers and the quaternions are $\mathbb{R}$-division algebras. If J is an ideal in a commutative ring with identity R then J is an R-algebra. In this case if n is a positive integer the set of matrices $M_n(J)$ is an R-algebra too, with the usual matrix operations. $J[x]$ is an R-algebra, a sub$R$-algebra of $R[x]$. $\mathbb{Q}(\sqrt{2})$ is a $\mathbb{Q}$-division algebra.

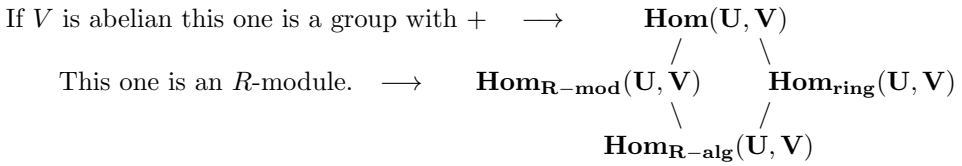
We saw that any abelian group S is a $\mathbb{Z}$-module. If S is in fact a ring, it is actually a $\mathbb{Z}$-algebra in the obvious way.

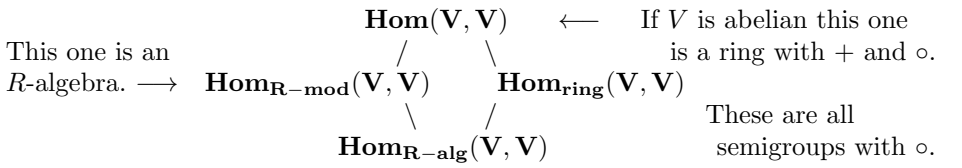
Another very important example is the following. We saw that if V is an R-module that $Hom_{R-mod}(V,V)$ is itself an R-module and forms a semigroup with composition. Then $Hom_{R-mod}(V,V)$ is a unitary R-module if V is a unitary R-module and R is commutative. Composition makes $Hom_{R-mod}(V,V)$ a ring with unit and finally an R-algebra.

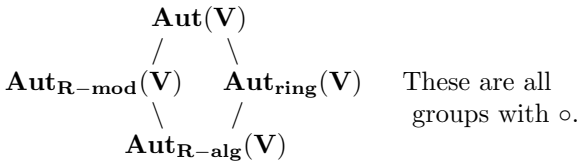
An **R-algebra homomorphism** between two R-algebras V and W is a member of $\mathbf{Hom_{R-alg}}(\mathbf{V},\mathbf{W}) = Hom_{R-mod}(V,W) \cap Hom_{ring}(V,W)$. If a member w of

$Hom_{R-alg}(V,W)$ has an inverse that inverse is also an R-algebra homomorphism and w is called an **R-algebra isomorphism**. V and W are called **isomorphic R-algebras** by virtue of the existence of an R-algebra isomorphism between them. An **R-algebra automorphism** of the R-algebra V is a member of $\mathbf{Aut_{R-alg}(V)} = Hom_{R-alg}(V,V) \cap Perm(V)$.

We have worked with families of homomorphisms of various types in this section and these families themselves have structures which are extremely important in analysis and which we have pointed out here and there. Gathering some of them together in one place might be useful. Within each grouping, as you move down the diagram U, V and R acquire whatever additional structure is required.







A significant fraction of the vocabulary and setting of modern analysis derives from properties of groups, rings, modules and algebras of families of functions and operators on these families. The structure and classification theorems for these objects are central issues in analysis.

30. An Example from an Algebra of Linear Transformations

30.1. ***Exercise.*** *Suppose F is a field. The set of n by n matrices $M_n(F)$ with entries in F is a vector space over F and also a ring with identity with matrix multiplication. It is an F-algebra and is not (usually) commutative. The set of these matrices has dimension n^2 as a vector space over F.*

*If V is a vector space over F, an **ordered basis** is a one-to-one function $b\colon G \to V$ where G is a well ordered set and $b(G)$ is a basis for V. In case $G = \{1, \ldots, n\}$ the function values (that is, the basis vectors) are denoted $b_1, \ldots, b_n$.*

A particular example is the set E of n by 1 matrices with entries in F. This set has standard ordered basis $e_1, \ldots, e_n$ where e_i is the matrix with 1 in row i and 0 elsewhere.

Suppose $G = \{1, \dots, n\}$. For each ordered basis b of generic n dimensional V there is a unique function $k_b \colon \{1, \dots, n\} \times V \to R$ with $v = \sum_{i=1}^{n} k_b^i(v) b_i$ for all $v \in V$. Each of the individual functions k_b^i are called ***coordinate functions for the ordered basis*** **b** *and are vector space homomorphisms onto F.*

k_b can be used to create a vector space isomorphism $\phi_b \colon V \to E$ by $\phi_b(v) = \sum_{i=1}^{n} k_b^i(v) e_i$ for each $v \in V$. Every isomorphism from V to E is of this type for one ordered basis or another.

k_b can also be used to create an F-algebra isomorphism $\Phi_b \colon Hom_{F-mod}(V, V) \to M_n(F)$ as follows: if $f \in Hom_{F-mod}(V, V)$ let $\Phi_b(f)$ denote the n by n matrix with entry $k_b^i(f(b_j))$ in row i and column j for each i and j between 1 and n. Every F-algebra isomorphism from $Hom_{F-mod}(V, V)$ to $M_n(F)$ is of this type for one ordered basis or another.

Even more, the isomorphisms ϕ_b and Φ_b are coordinated in the sense that $\Phi_b(f)\phi_b(v) = \phi_b(fv)$. So if you are interested in the effect of f on members of V you can, instead, study matrices in $M_n(F)$ and how they affect members of E.

Note: for two ordered bases a and b of V, $\Phi_a \circ \Phi_b^{-1} \in Aut_{F-alg}(M_n(F))$.

Suppose f is in $Aut_{F-mod}(V)$ where V has finite dimension n. Let A denote the vector subspace of $Hom_{F-mod}(V, V)$ generated by all the positive powers of f. A is a sub$F$-algebra of $Hom_{F-mod}(V, V)$. Since $Hom_{F-mod}(V, V)$ has dimension n^2, A is finite dimensional. There must be members $a_1, \dots, a_k$ of F which are not all zero for which $k \leq n^2 + 1$ and $a_k \neq 0$ and $\sum_{i=1}^{k} a_i f^i = 0$. Among all possible combinations of this type there is one with least degree: that is, the list $a_1, \dots, a_k$ satisfies the conditions and if members $b_1, \dots, b_j$ of F also satisfy the conditions then $j \geq k$.

Because of this minimality condition, the $a_1, \dots, a_k$ are essentially unique: if $b_1, \dots, b_k$ is another list satisfying the condition then $a_i = b_i \frac{a_k}{b_k}$ for each i. The two lists are a fixed multiple of each other. Also, since f is invertible there must be more than one nonzero a_i. The first coefficient a_1 cannot be 0, else we could cancel invertible f from each term in the sum to produce a shorter list of constants, contrary to the minimality assumption. If we let e denote the identity automorphism and defining $f^0 = e$ we now have

$$a_1 f = -\sum_{i=2}^{k} a_i f^i \text{ and so } e = -\sum_{i=2}^{k} \frac{a_i}{a_1} f^{i-1} = f\left(-\sum_{i=2}^{k} \frac{a_i}{a_1} f^{i-2}\right).$$

This tells us two things. First, e is in A. Second, and with this in hand, we also have f^{-1} in A. Both e and then f^{-1} are given explicitly as polynomials in the ideal $xF[x]$ evaluated at f. We conclude that $A = F(f)$ and that A has dimension $k - 1 \leq n^2$ as a vector space over F.

Let $m(x) = \sum_{i=0}^{j} b_i x^i$ where $j = k-1$ and for each i, $b_i = \frac{a_{i+1}}{a_k}$. Then $m(f) = 0$. In fact, $m(a) = 0$ for all $a \in A$. The polynomial $m(x)$ has lowest degree among all polynomials p in $F[x]$ with $p(f) = 0$. It is the unique polynomial of this type with leading coefficient 1. It is called the **minimal polynomial for f (or for A) in F[x]**.

30.2. ***Exercise.*** *Suppose given $f \in Aut_{F-mod}(V)$ as above for n dimensional V. $F[x]$ is a principal ideal domain and so a unique factorization domain. The function*

Ψ taking any $p(x) \in F[x]$ to $p(f)$ is a ring homomorphism, so its image, namely $F(f) = A$, is also a principal ideal ring. It is commutative and contains the identity automorphism, but if $m(x)$ has a nontrivial factorization it will not be an integral domain. The kernel of Ψ is an ideal. $Ker(\Psi) = m(x)F[x] = (m(x))$.

More generally, if J is any ideal in A then $\Psi^{-1}(J)$ is an ideal in the principal ideal domain $F[x]$ containing $Ker(\Psi) = m(x)F[x]$. So $\Psi^{-1}(J) = p(x)F[x] \supset m(x)F[x]$ and we must have $p(x)$ a factor of $m(x)$. So the ideals in A are exactly all principal ideals of the form $p(f)A$ where $p(x)$ is a factor of $m(x)$. If $p(x)$ is a factor of $m(x)$ which cannot, itself, be factored then $p(f)A$ is a prime ideal, and all prime ideals in A are of this type. Prime ideals are maximal in A.

V is an A-module (in addition to being a vector space over F) and as such every element v of V is a torsion element. The annihilator $Ann(A, v)$ is a nontrivial proper ideal of A unless $v = 0$. So there is a unique polynomial $\mathbf{m_v(x)}$, called the **minimal polynomial for v in F[x]**, with leading coefficient 1 with $Ann(A, v) = m_v(f)A$ where $m_v(x)$ is a factor of $m(x)$.

So the factors of $m(x)$ are important in understanding A. Suppose $m(x) = S_1(x)^{n_1} \cdots S_L(x)^{n_L}$ where each $S_i(x)$ is an irreducible and distinct polynomial of first degree or higher. This can be done in one and only one way (up to order) because $F[x]$ is a unique factorization domain.

30.3. ***Exercise.*** *Suppose $f \in Hom_{R-mod}(V, V)$. Any subR-module W of V with $fW \subset W$ is said to be **invariant under f**.*

(i) If f is one-to-one and W is finite dimensional then $f(W) \subset W$ implies that $f(W) = W$.

(ii) If R is commutative with identity and W is invariant under f then it is actually invariant under $q(f)$ for any polynomial $q(x) \in R[x]$. Any subspace of V created as $p(f)V$ for some polynomial $p(x) \in R[x]$ is invariant under f since $fp(f)V = p(f)fV \subset p(f)V$.

Carrying on with our discussion from above, define the polynomial

$$p_i(x) = (S_1(x))^{n_1} \cdots (S_{i-1}(x))^{n_{i-1}} (S_{i+1}(x))^{n_{i+1}} \cdots (S_L(x))^{n_L} \text{ for } i = 1, \ldots, L.$$

The polynomial $p_i(x)$ differs from $m(x)$ only by the missing factors $(S_i(x))^{n_i}$ for each i. Now define the vector subspaces

$$V_i = p_i(f)V \text{ for } i = 1, \ldots, L.$$

By minimality of $m(x)$, none of these vector subspaces can be $\{0\}$. They are all invariant subspaces for any member of A.

If $v \in V_i \cap V_j$ for $i \neq j$ the annihilator of v must be generated by a polynomial which is a factor of both $(S_i(x))^{n_i}$ and $(S_j(x))^{n_j}$. This polynomial must therefore be 1 and so $Ann(A, v) = A$ so $v = 0$.

This implies we can create the internal direct sum $V_1 \bigoplus \cdots \bigoplus V_L$ of these vector subspaces. Consider the function $H \colon V \to V_1 \bigoplus \cdots \bigoplus V_L$ defined by $H(v) = p_1(f)v + \cdots + p_L(f)v$. If $H(v) = 0$ then $p_1(f) + \cdots + p_L(f)$ is in the annihilator of v. So the generator of the annihilator is of the form $h(f)$ where $h(x)$ has a factor which is a factor of both $p_1(x) + \cdots + p_L(x)$ and a factor of $m(x)$. But $m(x)$ and $p_1(x) + \cdots + p_L(x)$ share no nontrivial factors. So $h(f) = 1$ and $v = 0$.

This means H is one-to-one so the dimension of $image(H)$ is the same as V. Since $image(H) \subset V$ we conclude that H is onto and that $V = V_1 \bigoplus \cdots \bigoplus V_L$. Every $v \in V$ can be written in a unique way as $v = v_1 + \cdots + v_L$ where each $v_i \in V_i$.

By definition of H and the v_i,

$$H(v) = H(v_1 + \cdots + v_L) = H(v_1) + \cdots + H(v_L) = P_1(f)v_1 + \cdots + P_L(f)v_L.$$

So H restricted to each V_i is $P_i(f)$ and an isomorphism on V_i. Also $P_i(V_j) = \{0\}$ when $i \neq j$.

30.4. ***Exercise.*** *(i) Except for the last equality, all of the subspaces on the chain*

$$V_i \supset S_i(x)V_i \supset (S_i(x))^2V_i \supset \cdots (S_i(x))^{n_i}V_i = \{0\}$$

are distinct. From this we conclude that $n_1 + \cdots + n_L \leq n$, the dimension of V.

(ii) By minimality of $m(x)$ there must be a member $v \in V_i$ with $m_v(x) = (S_i(x))^{n_i}$. Since V_i is invariant under f, if d_i is the degree of $S_i(x)$ then the set $\{v, fv, f^2v, \ldots, f^{n_i d_i - 1}v\}$ constitutes a linearly independent set of $n_i d_i$ distinct members of V_i. We conclude that the degree of $m(x)$, which is $n_1 d_1 + \cdots + n_L d_L$, cannot exceed n. Formerly our best estimate on the degree was n^2.

Now let's focus attention on V_i. $Aut_{F-mod}(V_i)$ is precisely the restriction to V_i of those members of $Hom_{F-mod}(V, V)$ for which V_i is invariant and which are one-to-one when restricted to V_i. Let A_i denote the restriction of the functions in A to V_i.

$p_i(f)$ is an isomorphism when restricted to V_i so by an argument identical to the one for f we can write the inverse of this isomorphism as a polynomial evaluated at $p_i(f)$ which is then by composition a polynomial $q_i(x)$ evaluated at f.

Going back to V now, the member $e_i = q_i(f)p_i(f)$ is the identity isomorphism when restricted to V_i and $e_iV_j = \{0\}$ when $i \neq j$. e_i is called the **projection onto the ith factor of the internal direct sum**.

So $e = e_1 + \cdots + e_L$ is a decomposition of e into the sum of projections. This decomposition is called the **resolution of the identity for A or for f**. Any vector $v \in V$ can be written explicitly as

$$v = ev = e_1v + \cdots e_Lv = v_1 + \cdots + v_L$$

where the v_i are those unique members of V_i whose sum is v.

30.5. ***Exercise.*** *(i) Suppose both f and g are in $Aut_{F-mod}(V)$ for field F and $fg = gf$. Then $v \in V_i$ implies*

$$(S_i(f))^{n_i}gv = g(S_i(f))^{n_i}v = g(\{0\}) = \{0\}.$$

This means $gV_i = V_i$. So the V_i are invariant subspaces for g as well as f.

(ii) Changing notation, let $V_1^f \oplus \cdots \oplus V_L^f$ be the direct sum decomposition of V corresponding to the resolution of the identity $e = e_1^f + \cdots + e_L^f$ for f and similarly let $V_1^g \oplus \cdots \oplus V_M^g$ be the direct sum decomposition of V corresponding to the resolution of the identity $e = e_1^g + \cdots + e_M^g$ for g.

Let $V_{i,j} = V_i^f \cap V_j^g$ and $e_{i,j} = e_i^f e_j^g$ for $i = 1, \ldots, L$ and $j = 1, \ldots, M$.

Then V is the direct sum $\bigoplus_{i,j} V_{i,j}$ where the subscript runs over i and j for which $V_{i,j} \neq \{0\}$.

Also $e = \left(\sum_{i=1}^{L} e_i^f\right)\left(\sum_{j=1}^{M} e_j^g\right) = \sum_{i,j} e_{i,j}$. *The sum over the nonzero* $e_{i,j}$ *is called a* ***resolution of the identity for the commutative algebra*** $\mathbf{F}(\mathbf{f},\mathbf{g})$ *generated by* f *and* g.

$e_{i,j}$ *is a projection onto* $V_{i,j}$ *for each* i *and* j *and* $e_{i,j}e_{l,k} = 0$ *unless* $i = l$ *and* $j = k$.

Each $e_{i,j}$ *can be formed as a linear combination of positive powers of* g *multiplied by a linear combination of positive powers of* f.

Knowing that a minimal polynomial exists and actually finding it are two different things, not to mention factoring it after it has been found. In linear algebra classes the usual routine is to use Φ to identify f with a matrix and use facts about determinants to produce a polynomial whose only factors are all the irreducible factors of $m(x)$, though possibly to higher powers, and still not in factored form.

A practical alternative is to select an ordered basis b as convenient and pick a vector $a_1 \in V$ at random. The list $\phi_b(a_1), \phi_b(fa_1), \phi_b(f^2a_1), \ldots, \phi_b(f^na_1)$ consists of $n+1$ column vectors in an n dimensional space so there is bound to be a nontrivial linear combination adding to 0. One might proceed by adding these vectors one at a time to the empty set until a dependent set is created. This will allow us to find $m_{a_1}(x)$, which divides $m(x)$.

The point of this is that barring extreme coincidence $m_{a_1}(x)$ will actually *be* $m(x)$. Picking a_1 at random and discovering anything else would correspond to landing, by chance, in a finite union of lower dimensional subspaces of V, an unlikely eventuality. And if by chance you do not get $m(x)$ on the first try, m_{a_1} still must be a factor of $m(x)$ and the information this provides could be very useful.

With candidate $m(x)$ in hand you can proceed to factorize it—if you can—and then create the subspaces V_i.

In some cases $m(x)$ can be factored into linear factors in $F[x]$ and we suppose this to be true in our case. This can be regarded as either a condition on F or a condition on f. For example, if $F = \mathbb{C}$ every polynomial factors into linear factors. On the other hand, if b is an ordered basis of V and $fv = \sum_{i=1}^{n} \lambda_i k_b^i(v) b_i$ for certain $\lambda_i \in F$ and all $v \in V$ then $m(x)$ can be factored no matter what F is.

For any linear factor $x - \lambda_i$ of $m(x)$ the number λ_i is called an **eigenvalue** for f.

Putting this sticky issue aside, we will suppose not only that $m(x)$ can be factored into linear factors but that each factor occurs just once: $m(x) = (x-\lambda_1)\cdots(x-\lambda_L)$ where all the λ_i are distinct members of F.

The prime ideals in A consist of the principal ideals $(f - \lambda_i)A$. The **spectrum of A or, equivalently, of f** consists of these L distinct "points" with the discrete topology, which can be identified with the set of eigenvalues $\{\lambda_1, \ldots, \lambda_L\}$ with discrete topology.

30.6. ***Exercise.*** *(i) Show that in the situation described in the preceding paragraph there is a basis* b *for which* $\Phi_b(f)$ *is a diagonal matrix with only the* λ_i *on the diagonal. The number of occurrences of* λ_i *is the dimension of* V_i *for each* i.

(ii) $f = \lambda_1 e_1 + \cdots + \lambda_L e_L$.

(iii) More generally, if $p(x) \in F[x]$ *then* $p(f) = \sum_{i=1}^{L} p(\lambda_i)e_i$.

30.7. ***Exercise.*** *Suppose* f *and* g *commute in* $Aut_{F-mod}(V)$ *and the minimal polynomial for* f *splits into distinct unrepeated factors* $(x-\lambda_1)\cdots(x-\lambda_L)$ *and the minimal polynomial for* g *splits into distinct unrepeated factors* $(x-\mu_1)\cdots(x-\mu_K)$.

(i) There is a basis b *of* V *for which both* $\Phi_b(f)$ *and* $\Phi_b(g)$ *are diagonal.*

(ii) If $p(x,y) \in F[x,y]$ *then* $p(f,g) = \sum_{i,j} p(\lambda_i, \mu_j)e_{i,j}$ *where the* $e_{i,j}$ *are the projections from Exercise 30.5.*

(iii) Consider matrix $M = \Phi_b(h)$ *for* $h = p(f,g) \in A$ *in light of Exercise 11.17. If* $f(x) = \sum_{k=0}^{\infty} a_k x^k$ *is a power series how would you define* $f(h)$*, and under what conditions on the* a_k *does your definition make sense?*

30.8. ***Exercise.*** *In the analysis involving the resolution of the identity for* f *we insisted that* f *be an automorphism which implies that* x *cannot be a factor of the minimal polynomial as we have defined it. Alternatively expressed,* 0 *cannot be an eigenvalue in our formulation.*

Still, there are things that can be done when $f \in Hom_{F-mod}(U,U)$ *is not one-to-one. The positive powers of* f *still generate a subF-algebra* A *of* $Hom_{F-mod}(U,U)$. *We will here, essentially, discard the torsion elements of* W *as an* A*-module. One can proceed further, but we will not in these notes.*

Let W_i *denote the kernel of* f^i *for positive* i. *The* W_i *form an increasing chain of subspaces in finite dimensional* U. *So if* n *is the dimension of* U, $W = W_n$ *is invariant with respect to* f.

If $f(v)+W = f(z)+W$ *then* $f(v-w) \in W$ *so* $v-w \in W$. *So if we let* $V = U/W$, *the function* $\tilde{f}$ *defined by* $\tilde{f}(v+W) = f(v)+W$ *is well defined. It is a member of* $Aut_{F-mod}(V)$.

31. Boolean Algebras, Lattices and Rings and Stone's Theorem

A **Boolean algebra** is a set S together with two commutative binary operations $+$ and $\cdot$ on S with **distinct identities** 0 and 1 respectively, and a **unary operation** $'$ on S (that is, a function from S into S) satisfying:

$$a \cdot (b+c) = (a \cdot b) + (a \cdot c) \text{ and } (a \cdot b) + c = (a+c) \cdot (b+c) \ \forall a, b, c \in S.$$

$$a \cdot a' = 0 \text{ and } a + a' = 1 \ \forall a \in S.$$

A Boolean algebra is not an algebra with these operations: the vocabulary is suggested by its relationship to an algebra on a set, which we explore later.

There is complete symmetry in the conditions for $+, 0$ and $\cdot, 1$. So an identity involving these and $'$ and generic members of S is equivalent to the new identity obtained by switching $+$ with $\cdot$ and 0 with 1 in the original identity. These statements will be called dual statements here. Dual statements are true or false together.

$0 = a' \cdot a = (a'+0) \cdot a = a' \cdot a + 0 \cdot a = 0 \cdot a$. So $0 \cdot a$ is always 0. The dual statement, $1 + a = 1 \ \forall a \in S$ is also true.

$0' = 0 + 0' = 1$. The dual statement is $1' = 0$.

$a = 1 \cdot a = (a + a') \cdot a = a \cdot a + a' \cdot a = a \cdot a$. An element which satisfies $a = a \cdot a$ is called **idempotent** with respect to the binary operation. All elements of a Boolean algebra are idempotent with respect to multiplication. The dual statement is $a = a + a \ \forall a \in S$. All elements of a Boolean algebra are idempotent with respect to addition. This implies, for example, that S can never be a group with either operation.

If $a + b = 1$ and $a \cdot b = 0$ then $b = a'$. In other words, any member of S that acts like a' *is* a'. To see this note that under the assumption on b, $b = b+0 = b+a\cdot a' = (b+a)\cdot(b+a') = b+a'$. Similarly $a' = a'+0 = a'+a\cdot b = (a'+a)\cdot(a'+b) = a'+b$. So $b = a'$ as suggested. It now follows immediately that $a'' = a \ \forall a \in S$. So, among other things, $'$ is in $Perm(S)$, and $'$ is its own inverse function. Orbits of $'$ have cardinal number 2.

$$a \cdot (a + b) = (a \cdot a) + (a \cdot b) = a + (a \cdot b) = a \cdot (1 + b) = a.$$

The dual statement is

$$a + (a \cdot b) = a \ \forall a, b \in S.$$

Using the last item and the distributive laws we can show that

$$a \cdot (a + (b + c)) = a \cdot ((a + b) + c)$$
$$\text{and} \quad a' \cdot (a + (b + c)) = a' \cdot ((a + b) + c).$$

Adding left side to left side and right side to right side of these equations we get $a + (b + c) = (a + b) + c$. So addition is an associative operation. The dual statement yields associativity for multiplication. So S is a commutative semigroup with identity with respect to each operation.

It is now straightforward to show that $a' + b'$ acts like (and therefore *is*) the element $(a \cdot b)'$. The dual statement is $(a + b)' = a' \cdot b' \ \forall a, b \in S$. Because of these facts, if you know you have in hand a Boolean algebra, the operations $+$ and $'$ determine $\cdot$, and also the operations $\cdot$ and $'$ determine $+$.

There is further redundancy in these operations. If you have a Boolean algebra in hand, there is a single binary operation that contains enough information to recreate $'$ and $\cdot$, and therefore $+$ too. It is called by Halmos the **Sheffer stroke** and defined by $a|b = a' \cdot b'$.

31.1. ***Exercise.*** *Verify the statements in the preceding paragraphs.*

31.2. ***Exercise.*** *Any algebra $\mathbb{G} \subset \mathbb{P}(X)$ on a nonempty set X is a Boolean algebra with $\cdot$, $+$, $'$, 1 and 0 given by $\cap$, $\cup$, ^{c} , X and $\varnothing$. So there are, in fact, nontrivial and interesting Boolean algebras.*

Exercise 31.2 brings us to the roots of the study of Boolean algebras, which are objects, evidently, possessing many of the properties of algebras on a set.

31.3. ***Exercise.*** *Suppose S is a Boolean algebra. Verify the following facts in order.*

(i) If $ab = a$ then $a + b = ab + b = (a + 1)b = b$.

(ii) If $a + b = b$ then $ab = a(a + b) = a^2 + ab = a + ab = a$.

(iii) Define $a \leq b$ if and only if $ab = a$ or, equivalently, $a + b = b$. Show that $a \leq a$. Show that if $a \leq b$ and $b \leq c$ then $a \leq c$. Show that if $a \leq b$ and $b \leq a$ then $a = b$. So $\leq$ is a partial order on S.

(iv) $a \cdot b = a \wedge b$. Greatest lower bounds of pairs of elements always exist and are found by multiplication.

(v) $a + b = a \vee b$. Least upper bounds of pairs of elements always exist, and are found by addition.

(vi) So S is a lattice with this partial order. The lattice has least member 0 and greatest member 1.

In the last exercise we showed that if S is a Boolean algebra the operations can be used to create an order on S. This order has several properties.

First, it is a lattice. It has a greatest element denoted 1 and a (different) least element denoted 0. Second, the lattice is **complemented**: that is, there is for each $a \in S$ a member $a' \in S$ for which $a \wedge a' = 0$ and $a \vee a' = 1$. Third, the lattice is **distributive**: that is, for all a, b and $c \in S$

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \text{ and } a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

Any complemented distributive lattice with distinct greatest and least elements is called a **Boolean lattice**.

31.4. ***Exercise.*** *Verify that any Boolean lattice is a Boolean algebra with operations $\wedge$ as multiplication and $\vee$ as addition.*

A **Boolean ring** is a nontrivial ring $(S, \oplus, \cdot)$ with identity and for which all elements are idempotent with respect to multiplication.

31.5. ***Exercise.*** *Suppose $(S, \oplus, \cdot)$ is a Boolean ring.*

(i) Expand $1 \oplus a = (1 \oplus a)^2$ and use idempotenency to conclude that $a \oplus a = 0$ $\forall a \in S$.

(ii) Expand $a \oplus b = (a \oplus b)^2$ and use idempotenency to conclude that $0 = ab \oplus ba$. From (i), ab is its own additive inverse so $ab = ba$. Boolean rings are commutative.

31.6. ***Exercise.*** *A Boolean ring is a commutative $\mathbb{Z}_2$-algebra.*

From Exercise 25.8 we see that, since $x^2 = x$ for every x in the Boolean ring S, every prime ideal in S is maximal.

In Exercise 31.7 we recognize Boolean rings as objects characterized by some of the properties of algebras on a set.

31.7. ***Exercise.*** *If $\mathbb{G} \subset \mathbb{P}(X)$ is an algebra on X define for $A,\ B \in \mathbb{G}$ the set $A \triangle B = (A \cap B^c) \cup (B \cap A^c) = (A - B) \cup (B - A) = (A \cup B) - (A \cap B)$, also known as the **symmetric difference** of A and B. Then $(\mathbb{G}, \triangle, \cap)$ is a Boolean ring.*

*We note specifically that a Boolean ring of subsets of X with these set operations is **distinct from** the concept of a ring in X as defined in Section 10. For one thing $A \triangle B \neq A - B$. Also a ring in X need not contain X, so the operation $\cap$ need not have identity.*

31.8. ***Exercise.*** *(i) Given any Boolean ring $(S, \oplus, \cdot)$ define the binary operation $\uplus$ by $a \uplus b = a \oplus b \oplus (a \cdot b)$ and define a unary operation * by $a^\star = 1 \oplus a$.*

Using the properties of Boolean rings (including $a \cdot a = a$ and $a \oplus a = 0$) show that $(S, \uplus, \cdot, ^\star)$ is a Boolean algebra with the same identities.

(ii) If $(S, +, \cdot, ')$ is any Boolean algebra define the binary operation $\boxplus$ on S by $a \boxplus b = (a'b) + (ab')$. The operation $\boxplus$ is obviously commutative. Using various of the properties of Boolean algebras developed above you will find it is associative too. The operation $\cdot$ distributes over $\boxplus$. So $(S, \boxplus, \cdot)$ is a Boolean ring with the same identities.

(iii) These processes are inverse to each other and provide an identification between Boolean algebras and Boolean rings (check this.) So Boolean algebras, Boolean lattices and Boolean rings are simply different ways of packaging the same structure.

The examples of Boolean rings, lattices and algebras from above were given as certain subsets of a power set. In fact we will see that *every* Boolean algebra can be identified with an algebra on *some* set X and every Boolean lattice can be identified with a Boolean lattice of sets with containment order. We will show this by proving that every Boolean ring is ring isomorphic to the collection of those subsets of a compact T_2 topological space which are both open and closed, with symmetric difference and intersection as ring operations.

31.9. ***Exercise.*** *Let $\mathbb{G} \subset \mathbb{P}(\mathbb{Z})$ denote the finite subsets of $\mathbb{Z}$ together with their complements, the **cofinite** subsets of $\mathbb{Z}$. Then $\mathbb{G}$ is a Boolean algebra, lattice and ring using the set operations and relations defined above. $\mathbb{G}$ is also infinite, but countably infinite. So $\mathbb{G}$ cannot be ring isomorphic to the full power set on any set.*

31.10. ***Exercise.*** *Suppose that $\mathbb{T} \subset \mathbb{P}(X)$ is a topology on a nonempty set X. Let $\mathbb{G}$ denote the collection of sets which are both open and closed with respect to this topology. Show that $\mathbb{G}$ is a Boolean algebra, lattice and ring using the set operations and relations defined above.*

In the following exercises we presume $(S, \oplus, \cdot)$ to be a Boolean ring.

Where convenient we will (and you may) denote $1 \oplus a$ by a' and $a \oplus b \oplus ab = a + b$. Also $a \oplus a = 0 = a \cdot a'$ and $a \cdot a = a + a = a$ and $a \oplus a' = 1 = a + a'$.

We will invoke results from Section 26 concerning the prime spectrum $Spec(S)$ of S consisting of the set of prime ideals of S endowed with the Zariski topology. We saw there that when S is *any* ring, $Spec(S)$ is compact and T_0. When S is a Boolean ring more is true.

31.11. ***Exercise.*** *Any finite union $Out(a_1) \cup \cdots \cup Out(a_n)$ is the basic open set $Out(a_1 + \cdots + a_n)$.*

To prove this, show $Out(c) \cup Out(d) = Out(c \oplus d \oplus cd)$ and proceed by induction. It is obvious that $Out(c) \cup Out(d) \supset Out(c \oplus d \oplus cd)$. On the other hand, no ideal lacking c could contain $c \oplus d \oplus cd$. If it did, then $c(c \oplus d \oplus cd) = cc \oplus cd \oplus ccd = c$ would be in the ideal, an instant contradiction.

31.12. ***Exercise.*** *Each basic open set $Out(a)$ is both open and closed. (hint: $Out(a) \cup Out(a') = Out(a \oplus a' \oplus aa') = Out(1) = Spec(S)$ and $Out(a) \cap Out(a') = Out(aa') = Out(0) = \varnothing$.*

31.13. ***Exercise.*** *$Spec(S)$ is a compact T_2 space. (hint: Suppose P and Q are distinct prime (and hence maximal) ideals. So $P + Q = S$ so there is $p \in P$ for which $p' \in Q$.)*

31.14. ***Exercise.*** *All sets in $Spec(S)$ which are both open and closed are basic open sets. (hint: A set A which is open is a union of basic open sets. If it is also closed then this collection plus $Spec(S) - A$ form an open cover of $Spec(S)$. Extract a finite subcover, throw away $Spec(S) - A$ and apply Exercise 31.11.)*

31.15. ***Exercise.*** *Let $\mathbb{G}$ denote the Boolean ring of subsets of $Spec(S)$ which are both open and closed with respect to the Zariski topology with intersection and symmetric difference operations. Prove* ***Stone's Theorem****: S is ring isomorphic to $\mathbb{G}$.*

31.16. ***Exercise.*** *Consider the resolution of the identity from page 102. Look at the set consisting of all 2^L sums of the form $\sum_{i=1}^{L} a_i e_i$ where a_i is either 0 or 1. This set is a Boolean ring with ordinary multiplication and addition $\oplus$ given by $f \oplus g = f + g - fg$. If $m(x)$ factors into distinct unrepeated linear factors this Boolean ring is isomorphic to the power set on the spectrum with intersection and symmetric difference operations.*

Index