# Abstract Linear Algebra with Application to Differential Equations

Dr. William Cook

Spring 2022

# Contents

# Chapter 1

# Real Review

## 1.1 Axioms which Determine $\mathbb{R}$

Without getting too philosophical, much like the natural numbers, for the real numbers it does not matter so much how we formally construct $\mathbb{R}$. What really matters is the formal properties that the real numbers possess. What makes the real numbers stand out is that they are the only *complete ordered field* (up to an appropriate equivalence). What does this mean?

First, the real numbers, denoted $\mathbb{R}$, form a *field*. This means that $\mathbb{R}$ is equipped with two operations: addition is denoted $a + b$ and multiplication is denoted $ab$ for any $a, b \in \mathbb{R}$. To be a field the following properties must hold:

**Closure:** For all $a, b \in \mathbb{R}$, $a + b, ab \in \mathbb{R}$.

**Associativity:** For all $a, b, c \in \mathbb{R}$, $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$.

**Identity:** There are special elements $0, 1 \in \mathbb{R}$ such that $0 \neq 1$ and for all $a \in \mathbb{R}$, $0 + a = a = a + 0$ and $1a = a = a1$.

**Inverses:** For each $a \in \mathbb{R}$ there is some $-a \in \mathbb{R}$ such that $(-a) + a = 0 = a + (-a)$. Also, when $a \neq 0$, there exists $a^{-1} \in \mathbb{R}$ such that $a^{-1}a = 1 = aa^{-1}$.

**Commutativity:** For all $a, b \in \mathbb{R}$, $a + b = b + a$ and $ab = ba$.

**Distribution:** For all $a, b, c \in \mathbb{R}$, $(a + b)c = ac + bc$ and $a(b + c) = ab + ac$.

Next, $\mathbb{R}$ is *totally ordered*. This means that $\mathbb{R}$ is equipped with a relation, denoted $\leq$, such that the following properties hold:

**Reflexive:** For all $a \in \mathbb{R}$, $a \leq a$.

**Antisymmetric:** For all $a, b \in \mathbb{R}$, if $a \leq b$ and $b \leq a$, then $a = b$.

**Transitive:** For all $a, b, c \in \mathbb{R}$, if $a \leq b$ and $b \leq c$, then $a \leq c$.

**Totally Comparability:** For every $a, b \in \mathbb{R}$ we have either $a \leq b$ or $b \leq a$,

To make $\mathbb{R}$ an *ordered field* we must require that its ordering is compatible with $\mathbb{R}$'s field operations:

**Compatibility:** For all $a, b, c \in \mathbb{R}$, if $a \leq b$, then $a + c \leq b + c$ and if $0 \leq a$ and $0 \leq b$, then $0 \leq ab$.

Maybe it is surprising that all of our familiar algebraic equality and inequality manipulations follow from this list of properties. Things such as "negative times negative is positive" and "$a \leq b$ implies $cb \leq ca$ when $c \leq 0$" and "$0 \leq a^2$" follow from these axioms.

Notice that the rational numbers $\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z} \text{ and } b \neq 0\}$ are an ordered field while $\mathbb{C}$ is not (we cannot impose an order on the complex numbers that plays nicely with its arithmetic: $i^2 = -1 < 0$ whereas in an ordered field $x^2 \geq 0$ for all $x$). Completeness is what sets the reals apart from all other ordered fields.

We say that $\mathbb{R}$ is a *complete ordered field* since it is an ordered field with the following property: Suppose $X$ is a non-empty subset of $\mathbb{R}$. In addition, suppose that there is some $M \in \mathbb{R}$ such that $x \leq M$ for all $x \in X$ (i.e., $X$ is bounded above). Then there exists a number $s = \sup(X)$ (called the *supremum* or *least upper bound*) such that $x \leq s$ for all $x \in X$ and given any $m \in \mathbb{R}$ such that $x \leq m$ for all $x \in X$, we have $s \leq m$ (i.e., the supremum is the least possible upper bound of $X$). Briefly, we require:

**Completeness:** Let $X$ be a non-empty subset of $\mathbb{R}$. If $X$ is bounded above, then $\sup(X)$ exists.

**Theorem 1.1** (All Complete Ordered Fields are Isomorphic)**.** *Let $\mathbb{F}$ be a complete ordered field. Then there exists an invertible map $\varphi : \mathbb{R} \to \mathbb{F}$ such that $\varphi(a+b) = \varphi(a) + \varphi(b)$, $\varphi(ab) = \varphi(a)\varphi(b)$, and $a \leq b$ implies $\varphi(a) \leq \varphi(b)$ for all $a, b \in \mathbb{R}$.*

Note that you need to be careful with the term "complete". It can mean different things in different contexts. For example, the complex numbers are *algebraically complete* (every non-constant complex polynomial has a complex root). This is a different kind of completeness. This is made a little trickier by the fact that the completeness of the real numbers can be characterized in a bunch of different ways.

First, a quick technical note, any complete ordered field (i.e., $\mathbb{R}$) has the following property:

**Archimedean Property:** For all $x \in \mathbb{R}$ such that $0 \leq x$ there is a positive integer $n$ such that $x \leq n$.

Although far from complete, here are a few properties equivalent to completeness (in an Arichimedean field)...

**Theorem 1.2.** *Any one of the following properties could replace the completeness axiom in an ordered field with the Archimedean property:*

- ◇ *A supremum (least upper bound) exists for any non-empty set that is bounded above.*
- ◇ *An infimum (greatest lower bound) exists for any non-empty set that is bounded below.*
- ◇ *Every Cauchy sequence converges.*
- ◇ *Every monotone sequence converges.*
- ◇ *Bolzano-Weierstrauss: Every bounded sequence contains an accumulation point.*
- ◇ *Every bounded sequence has a convergent subsequence.*
- ◇ *Given a nested sequence of intervals: $[a_1, b_1] \supseteq [a_2, b_2] \supseteq \cdots$ such that $\lim_{n\to\infty}(b_n - a_n) = 0$, their intersection contains exactly one real number: $\bigcap_{n=1}^{\infty} [a_n, b_n] = \{x\}$.*
- ◇ *Every continuous function which takes on positive and negative values has a root.*
- ◇ *Continuous functions satisfy the conclusion of the intermediate value theorem.*
- ◇ *Every decimal expression: $\pm N.d_1d_2d_3\ldots$ (where $N \in \mathbb{Z}_{\geq 0}$ and $d_j \in \{0, 1, \ldots, 9\}$) represents a real number.*

While these properties determine how the real numbers must behave, this leaves a dangling issue of *do such a system of real numbers actually exist?* Of course the answer is "Yes!" There are several approaches to building the real numbers. One could use decimal expansions, but it's incredibly messy to try state exactly how arithmetic is done and then prove that various properties hold. The two standard methods for constructing the real numbers (both with advantages and disadvantages) are sketched out below. Both constructions assume we have already constructed the rational numbers $\mathbb{Q}$.

**Dedekind Cuts.** Let $\alpha \subseteq \mathbb{Q}$ such that $\alpha$ is non-empty and $\alpha \neq \mathbb{Q}$. Suppose that given $x \in \alpha$, $y \in \mathbb{Q}$, and $y < x$, then $y \in \alpha$ (if $x$ belongs to $\alpha$ so does everything below $x$). Also, if $x \notin \alpha$, $y \in \mathbb{Q}$, and $x < y$, then $y \notin \alpha$ (if $x$ does not belong to $\alpha$ neither does anything above $x$). Such a set $\alpha$ is called a (Dedekind) *cut*. Let $\mathbb{R} = \{\alpha \subseteq \mathbb{Q} \mid \alpha \text{ is a cut}\}$.

Now one defines $\alpha \leq \beta$ if and only if $\alpha \subseteq \beta$. It isn't hard to show that this is a total order on $\mathbb{R}$ and it satisfies the completeness axiom (supremums of bounded sets exist).

Next, define $\alpha + \beta = \{x + y \mid x \in \alpha \text{ and } y \in \beta\}$. It can be shown that $\alpha + \beta$ is a cut whenever $\alpha$ and $\beta$ are and that this operation satisfies all of the needed properties. It turns out that the set of negative rational numbers is a cut and is the 0 in $\mathbb{R}$.

Multiplication is a little tricky. For positive cuts $\alpha, \beta > 0$, one defines $\alpha\beta = \{q \in \mathbb{Q} \mid q \leq xy \text{ for some } x \in \alpha \text{ and } y \in \beta\}$. All other multiplications are defined from the positive case: $\alpha\beta = (-\alpha)(-\beta)$ for $\alpha, \beta < 0$, $\alpha\beta = -[(-\alpha)\beta]$ for $\alpha < 0$ and $\beta > 0$, and $\alpha\beta = -[\alpha(-\beta)]$ for $\alpha > 0$ and $\beta < 0$. It turns out that $\{q \in \mathbb{Q} \mid q < 1\}$ is a cut which takes on the role of 1 in $\mathbb{R}$.

With inequality, addition, and multiplication defined, it can be shown that all necessary properties hold so $\mathbb{R}$ is a complete ordered field.

This construction was developed by Richard Dedekind in 1858 (published in 1872).

**Cauchy Sequences.** Let $\{a_n\}$ be a sequence of rational numbers. If given any $\epsilon \in \mathbb{Q}$ such that $\epsilon > 0$ we have some positive integer $N$ such that $|a_n - a_m| < \epsilon$ for all $m, n \geq N$, we say $\{a_n\}$ is a Cauchy sequence. Moreover, if for each $\epsilon > 0$ there exists some $N$ such that $|a_n| < \epsilon$ for all $n \geq N$, we say that $\{a_n\}$ converges to 0.

Let $\{a_n\}$ and $\{b_n\}$ be Cauchy sequences of rational numbers. Define $\{a_n\} \sim \{b_n\}$ if and only if $\{a_n - b_n\}$ converges to 0. It isn't hard to show that $\sim$ is an equivalence relation. Let $[\{a_n\}]$ be the equivalence class of some Cauchy sequence $\{a_n\}$. Define $\mathbb{R} = \{[\{a_n\}] \mid \{a_n\} \text{ is a Cauchy sequence of rational numbers}\}$ (here the "real numbers" are equivalence classes of rational Cauchy sequences).

For $[\{a_n\}], [\{b_n\}] \in \mathbb{R}$ one defines $[\{a_n\}] + [\{b_n\}] = [\{a_n + b_n\}]$ and $[\{a_n\}] \cdot [\{b_n\}] = [\{a_n \cdot b_n\}]$. One can show that these are well-defined operations that turn $\mathbb{R}$ into a field. One can identify each rational number $q \in \mathbb{Q}$ with the equivalence class of the constant sequence: $q, q, q, \ldots$ (constant sequences are Cauchy).

Finally, define $[\{a_n\}] < [\{b_n\}]$ if and only if for every $\epsilon > 0$ there is some $N$ such that $a_n < b_n$ for all $n \geq N$ (i.e., eventually the terms in $\{a_n\}$ are below the terms in $\{b_n\}$). Again, one can show that this relation is well-defined and that together this inequality relation with addition and multiplication make $\mathbb{R}$ into a complete ordered field.

This construction was somewhat anticipated by Bernard Bolzano (circa 1817) but wasn't really fleshed out completely until work done by Méray, Heine, and Cantor (around 1869–1872). For more detailed history see: http://www-history.mcs.st-and.ac.uk/HistTopics/Real_numbers_2.html

## 1.2 Characterizing $\mathbb{R}$ and $\mathbb{C}$

To get a better feeling for what makes $\mathbb{C}$ (the complex numbers) so special, let's take a look at why in the end we are almost forced to study $\mathbb{R}$ (the real numbers) in the first place.

To begin, we very naturally want to have a way to describe cardinal (more or less: size) and ordinal (more or less: ordering) information. The positive integers, $\mathbb{Z}_{>0} = \{1, 2, \ldots\}$ do both of these things for us. The number 3 both stands in for having 3 things (like "a, b, c" is a list of "3" letters) and being in 3$^{\text{rd}}$ place ("c" is letter number "3" in this list). People have been using these kinds of numbers for as long as there have been people.

Next, people needed to deal with parts of a whole, so they developed fractions. But this wasn't enough, we needed irrational quantities too. For example: In a 45°-45°-90° triangle with legs of length 1, the hypotenuse's length is $\sqrt{2}$. By the time of the Greek's, it was known that this number cannot be expressed as the ratio of two whole numbers. Fast forward and 0 is introduced in India. While negative numbers experienced some acceptance in China, they were mostly refused (in the Western world) until Fibonacci's time. Fibonacci used negative numbers himself and advocated that they were useful in finance (positive = credit, negative = debt).

So by the end of the Renaissance, the Western world saw the need for and usefulness of a number system which allowed addition, subtraction, multiplication, and division. The concept of a field (which came later) is the abstract characterization of such a numeric system.

**Definition 1.3.** Let $\mathbb{F}$ be a non-empty set equipped with two operations: $+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ denoted $a + b$ for $a, b \in \mathbb{F}$ and $\cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ denoted $a \cdot b$ or $ab$ for $a, b \in \mathbb{F}$. We have already required closure: If $a, b \in \mathbb{F}$, then $a + b, ab \in \mathbb{F}$. We also require that the following properties hold:

**Associativity:** For all $a, b, c \in \mathbb{F}$, $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$.

**Identity:** There are special elements $0, 1 \in \mathbb{F}$ such that $0 \neq 1$ and for all $a \in \mathbb{F}$, $0 + a = a = a + 0$ and $1a = a = a1$.

**Inverses:** For each $a \in \mathbb{F}$ there is some $-a \in \mathbb{F}$ such that $(-a) + a = 0 = a + (-a)$. If in addition, $a \neq 0$, there exists $a^{-1} \in \mathbb{F}$ such that $a^{-1}a = 1 = aa^{-1}$.

**Commutativity:** For all $a, b \in \mathbb{F}$, $a + b = b + a$ and $ab = ba$.

**Distribution:** For all $a, b, c \in \mathbb{F}$, $(a + b)c = ac + bc$ and $a(b + c) = ab + ac$.

Such a system, $\mathbb{F}$, is called a *field*.

We can see that the rational numbers ($\mathbb{Q}$), real numbers ($\mathbb{R}$), and complex numbers ($\mathbb{C}$) are all examples of fields. Of course, there are other examples of fields that look less familiar. For example, $\mathbb{Z}_p$ (integers modulo a prime $p$) and $\mathbb{R}(x)$ (rational functions with real coefficients) both form fields. This means that the real numbers must possess other structure which makes them stand out.

**Definition 1.4.** Let $\mathbb{F}$ be a field equipped with a relation $\leq$. Suppose that the following properties hold:

**Reflexive:** For all $a \in \mathbb{F}$, $a \leq a$.

**Antisymmetric:** For all $a, b \in \mathbb{F}$, if $a \leq b$ and $b \leq a$, then $a = b$.

**Transitive:** For all $a, b, c \in \mathbb{F}$, if $a \leq b$ and $b \leq c$, then $a \leq c$.

Then $\leq$ is called a *partial order*. If in addition, for every $a, b \in \mathbb{F}$ we have either $a \leq b$ or $b \leq a$, then $\leq$ is called a *total order*. Suppose that $\leq$ is a total order and for all $a, b, c \in \mathbb{F}$ we have that $a \leq b$ implies $a + c \leq b + c$ as well as $0 \leq a$ and $0 \leq b$ implies that $0 \leq ab$. Then we call $\mathbb{F}$ an *ordered field*.

Define $a < b$ to mean $a \leq b$ but $a \neq 0$ and $a \geq b$ if $b \leq a$ and $a > b$ if $b < a$. We say $a$ is positive if $a > 0$ and negative if $a < 0$. It isn't hard to prove that negative times negative is positive and positive times positive is positive. It isn't hard to show that $1 > 0$. This then implies that $0 = 1 - 1 > 0 - 1 = -1$. I won't go into more details, but essentially the relations $\leq$, $<$, etc. work just like we think they should. Notice that $\mathbb{Q}$ and $\mathbb{R}$ are ordered fields with the usual inequality operators.

It is worth mentioning that once we have an ordering, we also have *topology*: we can discuss limits and continuity. For example: For an ordered field $\mathbb{F}$, we can define intervals such as $(a, b) = \{x \in \mathbb{F} \mid a < x < b\}$, $[a, b] = \{x \in \mathbb{F} \mid a \leq x \leq b\}$, $(a, \infty) = \{x \in \mathbb{F} \mid a < x\}$, etc. *Open* intervals then form a basis for a topology on $\mathbb{F}$. This means we can start to do some *analysis* and not just *algebra*.

Another consequence of being ordered is that $1, 1 + 1 = 2, 1 + 1 + 1 = 3, \ldots$ must all be positive. In particular, $1 + 1 + \cdots + 1 \neq 0$. This means that an ordered field must have *characteristic* 0. For example: This means that the fields $\mathbb{Z}_p$ cannot be ordered in a way compatible with its arithmetic. On the other hand, any field of characteristic 0 0 must contain an isomorphic copy of $\mathbb{Q}$ (the converse is also true).

Now is a good time to mention that $\mathbb{C}$ cannot be ordered either. While $\mathbb{C}$ is a field of characteristic 0, we have a problem with $i$. Suppose that $\mathbb{C}$ were ordered. Then either $i > 0$ or $i < 0$. But in either case, $-1 = i^2 > 0$ (which is impossible). The crux is the problem is that $\mathbb{C}$ has elements other than $\pm 1$ with finite multiplicative order.

Now that we realize $\mathbb{C}$ does not have an ordered field structure, we can see why people balked at using the complex numbers for so long. If we think of *ordering* and *magnitude* as essential to being a *number*, then "things" such as $i = \sqrt{-1}$ cannot be "numbers". This leads to name calling: $i$ is "not real" and/or "imaginary". How sad.

Let us return to characterizing $\mathbb{R}$. So far we've ruled out some fields by looking at orderings, but we still have that both $\mathbb{Q}$ and $\mathbb{R}$ are ordered fields. This is where analysis comes into play. The real numbers have an additional property:

**Definition 1.5.** Let $\mathbb{F}$ be an ordered field and $S \subseteq \mathbb{F}$. If $m \in \mathbb{F}$ and $m \leq x$ for all $x \in S$, we say that $m$ is a *lower bound* for $S$. If $S$ has a lower bound, then $S$ is *bounded below*. Likewise, we could define *upper bound* and *bounded above*. If $S$ is bounded both above and below, then $S$ is *bounded*.

Next, suppose that $g$ is a lower bound for $S$ such that given any other lower bound $m$, we have $m \leq g$. In other words, if $g \leq x$ for all $x \in S$ and if $m \leq x$ for all $x \in S$, then $m \leq g$. Then $g$ is called the *greatest lower bound* or *infimum* of $S$, denoted $\text{glb}(S)$ or $\inf(S)$, (one can show that if $\inf(S)$ exists, it is unique). Likewise, we could define *least upper bound* or *supremum* ($\text{lub}(S) = \sup(S)$) and show that if such a bound exists, it is unique.

We say that an ordered field has the *greatest lower bound property* if for every non-empty set $S$ such that $S$ is bounded below, $\text{glb}(S)$ exists. Likewise, we could define a *least upper bound property*. It turns out that these two properties are equivalent (if one holds, both hold).

Finally, any ordered field having the greatest lower bound (or equivalently least upper bound) property is called a *complete ordered field*.

Notice that if $S = \{r \in \mathbb{Q} \mid \sqrt{2} \leq r\}$, then $\text{glb}(S) = \sqrt{2} \notin \mathbb{Q}$. This shows that $\mathbb{Q}$ does not have the greatest lower bound property – it is *not* a complete ordered field. On the other hand, $\mathbb{R}$ is complete. In fact, this characterizes $\mathbb{R}$: It is the only complete ordered field (up to isomorphism).

**Theorem 1.6.** *Suppose that $\mathbb{F}$ and $\mathbb{K}$ are complete ordered fields. Then there exists a bijection $\varphi : \mathbb{F} \to \mathbb{K}$ such that $\varphi(a+b) = \varphi(a) + \varphi(b)$, $\varphi(ab) = \varphi(a)\varphi(b)$, and $a < b$ implies $\varphi(a) < \varphi(b)$ for all $a, b \in \mathbb{F}$. This means that any two complete ordered fields are isomorphic. We call any such field: $\mathbb{R}$, the real numbers.*

*Proof.* As a sketch of a proof, take the $\mathbb{R}$ defined via Dedekind cuts or some such method and let $\mathbb{F}$ be a complete ordered field. Then we work on defining a map. To make sure $\varphi$ is an isomorphism of fields we must let $\varphi(0) = 0$, $\varphi(1) = 1$, and so $\varphi(2) = \varphi(1+1) = \varphi(1) + \varphi(1) = 1 + 1 = 2$, etc. This eventually shows that $\varphi$ maps $\mathbb{Q}$ in $\mathbb{R}$ to the corresponding copy of $\mathbb{Q}$ in $\mathbb{F}$. So far $\varphi$ preserves orderings. Next, any real number can be defined by a "cut". Pick $r \in \mathbb{R}$ then $r = \inf(S)$ where $S = \{x \in \mathbb{Q} \mid r \leq x\}$. For things to work out, we must define $\varphi(r) = \inf(\varphi(S)) = \inf(\{\varphi(x) \mid x \in S\})$. It is not too difficult to show that since $S$ is bounded below, so is $\varphi(S)$. Thus $\varphi(S)$ must have an infimum (because $\mathbb{F}$ is complete). We now have $\varphi$ defined on all of $\mathbb{R}$. One now shows that it is an order preserving homomorphism and is 1-to-1 and onto.

We now have that $\mathbb{R} \cong \mathbb{F}$ and so by transitivity any two complete ordered fields are isomorphic. □

This now means that whether we construct the real numbers via Dedekind cuts or by equivalence classes of Cauchy sequences of rational numbers or by decimal sequences, these construction yield the same abstract system that we call $\mathbb{R}$.

Now what about $\mathbb{C}$? Well, notice that we cannot solve $x^2 + 1 = 0$ in $\mathbb{R}$. This means that while $\mathbb{R}$ is complete in some topological sense, it is not complete is an algebraic sense. We say that a field is *algebraically closed* if every non-constant polynomial has a root, or equivalently, every non-constant polynomial factors into linear factors. The *Fundamental Theorem of Algebra* (which we will prove later in this course) states that $\mathbb{C}$ is algebraically closed. It turns out that every field has an algebraic closure (every field is contained in an algebraically closed field and the smallest such field is its called its closure). Also, an algebraic closure of a field is unique up to isomorphism.

**Theorem 1.7.** *The complex numbers, $\mathbb{C}$, are characterized as the algebraic closure of a complete order field: If $\bar{\mathbb{F}}$ is the algebraic closure of a complete ordered field $\mathbb{F}$, then $\bar{\mathbb{F}} \cong \mathbb{C}$ where this isomorphism extends an order preserving isomorphism between $\mathbb{F}$ and $\mathbb{R}$.*

This explains why we are naturally led to the study of complex numbers whether we originally wanted to or not!

# Chapter 2

# Abstract Linear Algebra

## 2.1 Independence, Spanning, & Dimension

In this section, we will run through some foundational theory about linear independence, spanning, and dimension. Throughout this section, $V$ will denote a vector space over a field $\mathbb{F}$. Unless otherwise stated, we do not assume that our vector spaces are finite dimensional.

**Definition 2.1.** Let $c_1, \ldots, c_\ell \in \mathbb{F}$ and $\mathbf{v}_1, \ldots, \mathbf{v}_\ell \in V$. Then $c_1\mathbf{v}_1 + \cdots + c_\ell\mathbf{v}_\ell = \sum_{i=1}^{\ell} c_i\mathbf{v}_i$ is a called a finite *linear combination* of the vectors in $\{\mathbf{v}_1, \ldots, \mathbf{v}_\ell\}$. From now on, we drop the word "finite" and just say linear combination. We call $0\mathbf{v}_1 + \cdots + 0\mathbf{v}_\ell$ the *trivial linear combination* (this always equals the zero vector).

Let $S \subseteq V$. Then $\text{span}(S) = \{c_1\mathbf{v}_1 + \cdots + c_\ell\mathbf{v}_\ell \mid \ell \geq 0 \text{ and } c_1, \ldots, c_\ell \in \mathbb{F} \text{ and } \mathbf{v}_1, \ldots, \mathbf{v}_\ell \in S\}$. In other words, the span of $S$ is the set of all linear combinations of vectors drawn from the set $S$.

We use the convention that the *empty sum* is equal to zero. Thus $\text{span}(\emptyset) = \{0\}$ (i.e., the span of the empty set is the trivial subspace).

Notice that a linear combination of linear combinations is again a linear combination:

$$\begin{aligned} s_1(c_{11}\mathbf{v}_{11} + \cdots + c_{1i_1}\mathbf{v}_{1i_1}) + \cdots + s_\ell(c_{\ell 1}\mathbf{v}_{\ell 1} + \cdots + c_{\ell i_\ell}\mathbf{v}_{\ell i_\ell}) \\ = s_1c_{11}\mathbf{v}_{11} + \cdots + s_1c_{1i_1}\mathbf{v}_{1i_1} + \cdots + s_\ell c_{\ell 1}\mathbf{v}_{\ell 1} + \cdots + s_\ell c_{\ell i_\ell}\mathbf{v}_{\ell i_\ell}. \end{aligned}$$

This implies that $\text{span}(S)$ is always a subspace of $V$. Also, $\text{span}(W) = W$ if and only if $W$ is a subspace. We also note that $S_1 \subseteq S_2$ implies $\text{span}(S_1) \subseteq \text{span}(S_2)$ since any linear combination of $S_1$'s elements would also be a linear combination of $S_2$'s elements. Also, recall that we say $S$ *spans* $V$ if $\text{span}(S) = V$.

**Definition 2.2.** Let $S \subseteq V$. We say that $S$ is *linearly independent* if no vector of $S$ can be written as a linear combination of other vectors in $S$. If some vector can be written as a linear combination of other vectors, we say $S$ is *linearly dependent*. It is easy to show (and this is often taken as a definition) that $S$ is linearly independent if and only if the only linear combination of vectors in $S$ summing to 0 is the trivial linear combination.

Notice that $\emptyset$ is linearly independent since the only linear combination we can form is the empty sum (i.e., a trivial combination). On the other hand, any set containing the zero vector is automatically dependent since 0 is equal to the empty sum and so we have written zero as a linear combination of "other vectors" $S$. Also, note that if $S_1 \subseteq S_2$ and $S_2$ is independent, then $S_1$ must be independent as well since any dependence among $S_1$'s vectors would be a dependence among $S_2$'s vectors. We can see that supersets of spanning sets still span and subsets of independent sets are still independent.

**Lemma 2.3.** *Let $S$ be a linearly independent subset of $V$, $\mathbf{v} \in V$ such that $\mathbf{v} \notin S$. Then $S \cup \{\mathbf{v}\}$ is linearly independent if and only if $\mathbf{v} \notin \text{span}(S)$.*

*Proof.* Suppose $S \cup \{\mathbf{v}\}$ is linearly independent. Then $\mathbf{v}$ cannot depend linearly on $S$. Thus $\mathbf{v} \notin \text{span}(S)$.

Conversely, suppose $\mathbf{v} \notin \text{span}(S)$. Suppose $S \cup \{\mathbf{v}\}$ were linearly dependent. Then we could write $c_1\mathbf{v}_1 + \cdots + c_\ell\mathbf{v}_\ell + s\mathbf{v} = 0$ for some $\mathbf{v}_1, \ldots, \mathbf{v}_\ell \in S$ and scalars $c_1, \ldots, c_\ell, s$ not all zero. Notice that $s \neq 0$ would imply $\mathbf{v} = s^{-1}c_1\mathbf{v}_1 + \cdots + s^{-1}c_\ell\mathbf{v}_\ell \in \text{span}(S)$ (contradiction) so $s = 0$. But then $c_1\mathbf{v}_1 + \cdots + c_\ell\mathbf{v}_\ell = 0$ with not all $c_1, \ldots, c_\ell$. This means $S$ is linearly dependent! (contradiction).

Thus $S \cup \{\mathbf{v}\}$ must be independent. □

**Theorem 2.4.** *Let $S$ be a linearly independent subset of $T$ where $T$ spans $V$. Then there exists some $\beta$ such that $S \subseteq \beta \subseteq T$ where $\beta$ is a basis for $V$. In other words, between any independent and spanning set, we can find a basis.*

*Proof.* Consider the set $\mathcal{S} = \{S' \subseteq V \mid S \subseteq S' \subseteq T \text{ and } S' \text{ is linearly independent}\}$. Notice that $S$ itself belongs to $\mathcal{S}$, so $\mathcal{S}$ is a non-empty set and is partially ordered by the subset relation. Suppose that we have a chain of elements in $\mathcal{S}$, say $\mathcal{C}$: this means that for all $S', S'' \in \mathcal{C}$ either $S' \subseteq S''$ or $S'' \subseteq S'$ (i.e., $\mathcal{C}$ is totally ordered by the subset relation). Consider $C = \cup\mathcal{C}$ (i.e., $C$ is the union of all of the sets in our chain). Now every set in $\mathcal{C}$ contains $S$ and is contained in $T$, so this is true of the union of such sets (i.e., $S \subseteq C \subseteq T$). Suppose $\mathbf{v}_1, \ldots, \mathbf{v}_\ell \in C$ and $c_1, \ldots, c_\ell \in \mathbb{F}$ such that $c_1\mathbf{v}_1 + \cdots + c_\ell\mathbf{v}_\ell = 0$. Then for each $i = 1, \ldots, \ell$, we have $\mathbf{v}_i \in S_i$ for some $S_i \in \mathcal{C}$. But $\mathcal{C}$ is a chain so we can (possibly after relabeling – without loss of generality) assume $S_1 \subseteq S_2 \subseteq \cdots \subseteq S_\ell$. Thus $\mathbf{v}_1, \ldots, \mathbf{v}_\ell \in S_\ell$. But ultimately $S_\ell$ is a set in $\mathcal{S}$ and so is linearly independent. Thus $c_1 = \cdots = c_\ell = 0$. Therefore, $C$ is linearly independent. Therefore, $C \in \mathcal{S}$.

All of this shows that $\mathcal{S}$ is a non-empty set such that every chain is bounded above (by something in $\mathcal{S}$). Thus can apply Zorn's Lemma which states that $\mathcal{S}$ must contain a (possibly non-unique) maximal element. Call such an element $\beta$. We have then that $\beta$ contains $S$, is contained in $T$, and is linearly independent. To finish our proof we just need to establish that $\beta$ spans $V$.

Suppose $T$ is not contained in $\text{span}(\beta)$. This implies there is some $\mathbf{v} \in T$ such that $\mathbf{v} \notin \text{span}(\beta)$. So by Lemma 2.3, $\beta' = \beta \cup \{\mathbf{v}\}$ is linearly independent. But also $S \subseteq \beta \subseteq \beta' \subseteq T$ so $\beta' \in \mathcal{S}$. However, this is impossible because $\beta$ was chosen to be maximal (i.e., it is not contained in something else in $\mathcal{S}$). Therefore, we must conclude that $T \subseteq \text{span}(\beta)$. Therefore, $V = \text{span}(T) \subseteq \text{span}(\beta) \subseteq V$ so that $\text{span}(\beta) = V$. Thus $\beta$ is our desired basis. □

*Note.* We used Zorn's Lemma in a non-trivial way. Zorn's result is equivalent to the Axiom of Choice. In fact, it can be shown that our theorem above is equivalent to the Axiom of Choice (we must use choice in some way to establish our theorem in general).

It is difficult to stress just how important the following corollaries to above theorem are:

**Corollary 2.5.** *Every vector space has a basis. Every linearly independent set can be extended to a basis. Every spanning set can be shrunk down to a basis.*

*Proof.* Applying Theorem 2.4 to the case $S = \emptyset$ and $T = V$ (these are always independent and spanning sets respectively), shows that we must have at least one basis. If $S$ is linearly independent and we let $T = V$, we get that $S$ is contained in some basis (i.e., every independent set can be extended to a basis). Finally, if $T$ is a spanning set and we let $S = \emptyset$, we get a a basis $\beta$ that is contained in $T$ (i.e., spanning sets can be shrunk down to a basis). □

All of this leads us to the following linear algebra philosophy: Bases are small enough spanning sets (small enough to be independent). Likewise, bases are big enough independent sets (big enough to span). We get the impression that independent sets must be no larger than spanning sets. This is true but requires some proof.

**Theorem 2.6** (Exchange Lemma)**.** *Let $\alpha = \{\mathbf{v}_1, \ldots, \mathbf{v}_\ell\}$ be linearly independent and suppose $T$ spans $V$. Then there exists some partition of $T = \{\mathbf{w}_1, \ldots, \mathbf{w}_\ell\} \dot\cup T'$ (i.e., $T$ is a disjoint union of $\{\mathbf{w}_1, \ldots, \mathbf{w}_\ell\}$ and $T'$) such that $T'' = \alpha \cup T'$ still spans $V$. In other words, if we select the right $\mathbf{w}_i$'s, we can swap out $\{\mathbf{w}_1, \ldots, \mathbf{w}_\ell\}$ with $\alpha$ and still span our vector space.*

*Proof.* We proceed by induction. We can obviously swap zero vectors without difficulty, so our base case holds. Now suppose we have replaced $\{\mathbf{w}_1, \ldots, \mathbf{w}_k\}$ by $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ so that $T'' = \{\mathbf{v}_1, \ldots, \mathbf{v}_k\} \dot\cup T'$ spans $V$. Consider $\mathbf{v}_{k+1}$. Since $T''$ spans $V$, $\mathbf{v}_{k+1} = c_1\mathbf{v}_1 + \cdots + c_k\mathbf{v}_k + s_1\mathbf{u}_1 + \cdots + s_m\mathbf{u}_m$ for some $\mathbf{u}_1, \ldots, \mathbf{u}_m \in T'$ and $c_1, \ldots, c_k, s_1, \ldots, s_m \in \mathbb{F}$. Notice that if $s_1 = \cdots = s_m = 0$, then $\mathbf{v}_{k+1} \in \text{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ implying that $\alpha$ is linearly dependent (contradiction).

Therefore, at least one $s_i$ is non-zero, say $s_m \neq 0$. For convenience call $s_m = s$ and $\mathbf{u}_m = \mathbf{u}$. Let $X = c_1\mathbf{v}_1 + \cdots + c_k\mathbf{v}_k + s_1\mathbf{u}_1 + \cdots + s_{m-1}\mathbf{u}_{m-1}$ so we have that $\mathbf{v}_{k+1} = s\mathbf{u} + X$. Let $T' = \{\mathbf{u}\} \dot\cup T_0$ (i.e., $T_0$ is all of $T'$ except $\mathbf{u}$). Notice that $X$ is a linear combination of elements drawn from $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\} \cup T_0$.

Therefore, in any linear combination, if it involves $\mathbf{u}$, we can replace $\mathbf{u}$ with $s^{-1}\mathbf{v}_{k+1} - s^{-1}X$. We now have that any linear combination of elements drawn from $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\} \cup \{\mathbf{u}\} \cup T_0$ can also be written as a linear combination of elements drawn from $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\} \cup \{\mathbf{v}_{k+1}\} \cup T_0$. In other words, we can swap out $\mathbf{w}_{k+1} = \mathbf{u}$ for $\mathbf{v}_{k+1}$ and our set will still span. The theorem now follows from induction. □

**Corollary 2.7.** *If $\alpha$ is a finite linearly independent set and $T$ is a spanning set, then $|\alpha| \leq |T|$. Moreover, if $V$ is spanned by a finite set, it cannot have an infinite linearly independent subset.*

*Proof.* By the Exchange Lemma 2.6, we can replace elements of $T$ with elements of $\alpha$, so $T$ must have at least as many elements as $\alpha$. Now suppose that we have a finite spanning set $T$, say $|T| = m < \infty$. If we had an linearly independent set $\alpha$ with more than $m$ elements, the Exchange Lemma would imply that we could replace $m + 1$ elements of $T$ with the first $m + 1$ elements of $\alpha$. This is absurd. □

**Corollary 2.8.** *If any basis of a vector space is finite, all bases of that space are finite. Moreover, any two finite bases must have the same size.*

*Proof.* Corollary 2.7 states that we cannot have a finite basis (a finite spanning set) and also an infinite basis (an infinite linearly independent subset).

Next, suppose $\alpha$ and $\beta$ are finite bases for $V$. Then since $\alpha$ is finite linearly independent and $\beta$ is a spanning set, our previous corollary says that $|\alpha| \leq |\beta|$. But also, $\beta$ is finite linearly independent and $\alpha$ is a spanning set, so that $|\beta| \leq |\alpha|$. Therefore, $|\alpha| = |\beta|$. □

**Theorem 2.9.** *Any two bases of a vector space must have the same cardinality.*

*Proof.* Let $\beta$ and $\beta'$ be bases for $V$. We already know that either both are infinite or both are finite. If both are finite, the corollary above establishes that $|\beta| = |\beta'|$. Therefore, we suppose that both are infinite and for sake of contradiction that $|\beta| < |\beta'|$.

Consider $\mathbf{v} \in \beta$. Then since $\beta'$ spans $V$, there exists $\mathbf{v}_1, \ldots, \mathbf{v}_\ell \in \beta'$ and $c_1, \ldots, c_\ell \in \mathbb{F}$ such that $\mathbf{v} = c_1\mathbf{v}_1 + \cdots + c_\ell\mathbf{v}_\ell$. Define $F_\mathbf{v} = \{\mathbf{v}_1, \ldots, \mathbf{v}_\ell\}$ and so we have $\mathbf{v} \in \operatorname{span}(F_\mathbf{v})$. Let $\alpha = \bigcup_{\mathbf{v}\in\beta} F_\mathbf{v}$. Then $\alpha$ is a subset of $\beta'$. Moreover, for each $\mathbf{v} \in \beta$ we have $\mathbf{v} \in \operatorname{span}(F_\mathbf{v}) \subseteq \operatorname{span}(\alpha)$ so $\beta \subseteq \operatorname{span}(\alpha)$. Thus since $\beta$ spans $V$, we have $V = \operatorname{span}(\beta) = \operatorname{span}(\alpha)$.

But this is problematic. Since $\alpha$ is a union of finite subsets indexed by $\beta$, we have that $|\alpha| \leq |\beta| \cdot \aleph_0 = |\beta|$ (since $\beta$ is infinite). So $|\alpha| = |\beta| < |\beta'|$. Therefore $\alpha$ must be a proper subsets of $\beta'$. Thus there is some $w \in \beta'$ that does not belong to $\alpha$. Since $\beta'$ is linearly independent, $\alpha \dot\cup \{w\}$ is independent. Therefore, $w \notin \operatorname{span}(\alpha)$. But this means that $\operatorname{span}(\alpha) \neq V$ (contradiction).

Therefore, we must have that $|\beta| = |\beta'|$. □

Given all bases have the same size, we can make the following definition:

**Definition 2.10.** Let $V$ have a basis $\beta$. Then $\dim(V) = |\beta|$ is the *dimension* of $V$.

Finite dimensional spaces are special. For example, we have the following result.

**Proposition 2.11.** *Let $V$ be a vector space of finite dimension $n$. Let $\beta = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be a subset of $V$ of cardinality $n$. Then $\beta$ is linearly independent if and only if $\beta$ spans $V$. In other words, if $\beta$ is either a spanning set or is independent, then it's both hold and we have that $\beta$ is a basis.*

*Proof.* If $\beta$ is linearly independent, then it is contained in a basis, say $\gamma$. But $\beta \subseteq \gamma$ where $|\beta| = |\gamma| = n < \infty$ implies $\beta = \gamma$, so $\beta$ is a basis. Likewise, if $\beta$ spans $V$, then it contains a basis, say $\alpha$. But $\alpha \subseteq \beta$ where $|\alpha| = |\beta| = n < \infty$ implies $\alpha = \beta$, so $\beta$ is a basis. □

Proposition 2.11 does not work for infinite dimensional spaces. For example, $\{1, x^2, x^4, \dots\}$ is a countably infinite, linearly independent subset of the countably infinite dimensional space $\mathbb{R}[x]$, yet it fails to span. On the other hand, $\{2, 1, x, x^2, \dots\}$ is a countably infinite, spanning set for $\mathbb{R}[x]$, yet it fails to be independent. Having one property plus the "right size" isn't enough to force sets to be bases if we work in infinite dimensional spaces.

We are now ready to discuss coordinates. First, we discuss coordinates for finite dimensional spaces. Then we can sketch out how they work for infinite dimensional spaces. Fix an *ordered* basis $\beta = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ for $V$ (we assume $\dim(V) = n < \infty$). Then given $\mathbf{v} \in V$ there exists $c_1, \dots, c_n \in \mathbb{F}$ such that $\mathbf{v} = c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n$. Moreover, suppose we have $b_1, \dots, b_n \in \mathbb{F}$ such that $\mathbf{v} = b_1\mathbf{v}_1 + \cdots + b_n\mathbf{v}_n$ as well. Then $(b_1 - c_1)\mathbf{v}_1 + \cdots + (b_n - c_n)\mathbf{v}_n = 0$. But $\beta$ is linearly independent so $b_1 - c_1 = \cdots = b_n - c_n = 0$. Thus $b_1 = c_1, \dots, b_n = c_n$. In other words, not only is every vector a linear combination of our basis elements, each vector is a linear combination in a *unique* way. Thus we define:

**Definition 2.12.** Let $\beta = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ be an ordered basis for $V$ where $\dim(V) = n < \infty$. Given $\mathbf{v} \in V$, there exists unique scalars $c_1, \dots, c_n \in \mathbb{F}$ such that $\mathbf{v} = c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n$. Let $[\mathbf{v}]_\beta = [c_1\ c_2\ \cdots\ c_n]^T$ (i.e., $[\mathbf{v}]_\beta$ is an $n \times 1$ column vector whose entries are the coefficients in our linear combination). We call $[\mathbf{v}]_\beta$ the *coordinates* of $\mathbf{v}$ relative to the (ordered) basis $\beta$.

Notice that since every vector in $V$ is associated with a unique coordinate vector and every column vector can be used to construct a linear combination, $[\,\cdot\,]_\beta$ gives us a bijection between $V$ and $\mathbb{F}^{n\times 1}$. In fact, it is easy to see that $[\mathbf{v} + \mathbf{w}]_\beta = [\mathbf{v}]_\beta + [\mathbf{w}]_\beta$ and $[s\mathbf{v}]_\beta = s[\mathbf{v}]_\beta$ for all $\mathbf{v}, \mathbf{w} \in V$ and $s \in \mathbb{F}$. Therefore, the coordinate map $[\,\cdot\,]_\beta$ is an invertible linear map (i.e., an isomorphism) between $V$ and $\mathbb{F}^{n\times 1}$.

This means that we can use coordinates to translate between the world of abstract (finite dimensional) vector spaces and the world of column vectors. Typically we translate into coordinates, calculate there, and then translate back.

When $V$ is infinite dimensional, we can still define a notion of coordinates, but they are not nearly as useful. Consider a basis $\beta$ indexed by some set $I$ (i.e., $\beta = \{\mathbf{v}_i \mid i \in I\}$ where $\mathbf{v}_i = \mathbf{v}_j$ if and only if $i = j$). The set of all functions $\mathbb{F}^I = \{f \mid f : I \to \mathbb{F}\}$ can be given the structure of a vector space over $\mathbb{F}$ as follows: $f + g$ is defined to by $(f + g)(i) = f(i) + g(i)$ (we add outputs pointwise) and $sf$ is defined by $(sf)(i) = sf(i)$ for all $i \in I$; $f, g \in \mathbb{F}^I$; and $s \in \mathbb{F}$. Then consider $\widehat{\mathbb{F}^I} = \{f : I \to \mathbb{F} \mid f(i) = 0 \text{ for all but finitely many } i \in I\}$ (i.e., the set of functions of finite support). It is easy to see that $\widehat{\mathbb{F}^I}$ is a subspace of $\mathbb{F}^I$. Now notice that given any $\mathbf{v} \in V$, there exists (unique up to padding out with zeros) $\mathbf{v}_{i_1}, \dots, \mathbf{v}_{i_\ell} \in \beta$ and $c_{i_1}, \dots, c_{i_\ell} \in \mathbb{F}$ such that $\mathbf{v} = c_{i_1}\mathbf{v}_{i_1} + \cdots + c_{i_\ell}\mathbf{v}_{i_\ell}$. We can then define a function $f : I \to \mathbb{F}$ by $f(i_j) = c_{i_j}$ for $j = 1, \dots, \ell$ and $f(i) = 0$ for all other $i \in I$. Then, letting $[\mathbf{v}]_\beta = f$, we have a unique coordinate function associated with each vector in $V$. Once again $[\,\cdot\,]_\beta : V \to \widehat{F^I}$ is an isomorphism. That said, when $I$ is infinite, working with such coordinate functions isn't typically terribly useful.

Finally, a word about direct sums. Let $A, B, C$ be subsets of a vector space $V$. Then $A+B+C = \{\mathbf{a}+\mathbf{b}+\mathbf{c} \mid \mathbf{a} \in A, \mathbf{b} \in B, \mathbf{c} \in C\}$. In other words, $A + B + C$ denotes all possible sums of elements drawn from $A$, $B$, and $C$. More generally, if $W_i$ where $i \in I$ is a collection of subsets, then

$$\sum_{i\in I} W_i = \{\mathbf{w}_{i_1} + \cdots + \mathbf{w}_{i_\ell} \mid i_1, \dots, i_\ell \in I \text{ and } \mathbf{w}_{i_j} \in W_{i_j} \text{ for } j = 1, \dots, \ell\}.$$

In other words, $\sum W_i$ is the set of all finite sums of vectors drawn from $W_i$'s. If $W_i$ is a subspace of $V$ for all $i \in I$, then it is easy to show that $\sum_i W_i$ is a subspace as well.

**Theorem 2.13.** *Let $W_i$ where $i \in I$ be a collection of subspaces of $V$. Then the following are equivalent:*

1. *$\sum_i W_i = V$ and $W_i \cap \left(\sum_{i\neq j} W_j\right) = \{0\}$ for all $i \in I$*
2. *For each $\mathbf{v} \in V$, there exists unique (up to padding with zeros) $\mathbf{w}_{i_j} \in W_{i_j}$ for some $i_1, \dots, i_\ell \in I$ such that $\mathbf{v} = \mathbf{w}_{i_1} + \cdots + \mathbf{w}_{i_\ell}$.*
3. *Given $\beta_i$ is a basis for $W_i$ (for each $i \in I$), the disjoint union $\beta$ of $\beta_i$'s for all $i \in I$ is a basis for $V$.*

*Proof.* I will prove this in the situation we have a finite index set $I$. The general case follows from a very similar argument – but the notation is much more cumbersome. Let $W_1, \ldots, W_\ell$ be our collection of subspaces.

Assume 1 holds. Suppose $\mathbf{v} \in V$. Since $V = W_1 + \cdots + W_\ell$, there exists $\mathbf{w}_i \in W_i$ $(i = 1, \ldots, \ell)$ such that $\mathbf{v} = \mathbf{w}_1 + \cdots + \mathbf{w}_\ell$. Now suppose we also have $\mathbf{v} = u_1 + \cdots + u_\ell$ for some $u_i \in W_i$ $(i = 1, \ldots, \ell)$. Then $(u_1 - \mathbf{w}_1) + \cdots + (u_\ell - \mathbf{w}_\ell) = \mathbf{v} - \mathbf{v} = 0$. Thus $u_i - \mathbf{w}_i = \sum_{j \neq i}(u_j - \mathbf{w}_j)$. The left hand side says $u_i - \mathbf{w}_i \in W_i$. The right hand side says $u_i - \mathbf{w}_i$ belongs to $\sum_{j \neq i} W_j$. Therefore, $u_i - \mathbf{w}_i \in W_i \cap \left(\sum_{i \neq j} W_j\right) = \{0\}$. So $u_i - \mathbf{w}_i = 0$ and thus $u_i = \mathbf{w}_i$ for all $i = 1, \ldots, \ell$. Thus 2 holds.

Now suppose 2 holds. Let $\beta_i$ be a basis for $W_i$ (for $i = 1, \ldots, \ell$). Note that these sets must be disjoint since if not, we would have $\mathbf{w}_i = \mathbf{w}_j$ for some $\mathbf{w}_i \in \beta_i$ and $\mathbf{w}_j \in \beta_j$ and this would violate the uniqueness part of our assumption in 2. Let $\mathbf{v} \in V$. Then by assumption there exists (unique) $\mathbf{w}_i \in W_i$ (for $i = 1, \ldots, \ell$) such that $\mathbf{v} = \mathbf{w}_1 + \cdots + \mathbf{w}_\ell$. Since $\beta_i$ is a basis for $W_i$, there exists $c_{i1}, \ldots, c_{ik_i} \in \mathbb{F}$ and $\mathbf{v}_{i1}, \ldots, \mathbf{v}_{ik_i} \in \beta_i$ such that $\mathbf{w}_i = c_{i1}\mathbf{v}_{i1} + \cdots + c_{ik_i}\mathbf{v}_{ik_i}$. Therefore, $\mathbf{v} = \mathbf{w}_1 + \cdots + \mathbf{w}_\ell = c_{11}\mathbf{v}_{11} + \cdots + c_{1k_1}\mathbf{v}_{1k_1} + \cdots + c_{\ell 1}\mathbf{v}_{\ell 1} + \cdots + c_{\ell k_\ell}\mathbf{v}_{\ell k_\ell}$ is a linear combination of elements in $\beta = \beta_1 \cup \cdots \cup \beta_\ell$. So $\beta$ spans $V$. Now suppose $c_{11}\mathbf{v}_{11} + \cdots + c_{1k_1}\mathbf{v}_{1k_1} + \cdots + c_{\ell 1}\mathbf{v}_{\ell 1} + \cdots + c_{\ell k_\ell}\mathbf{v}_{\ell k_\ell} = 0$ for some choice of $\mathbf{v}_{ij} \in \beta_i$ and $c_{ij} \in \mathbb{F}$. Well, 0 is uniquely represented by $0 + \cdots + 0$. Therefore, for each $i = 1, \ldots, \ell$, since $c_{i1}\mathbf{v}_{i1} + \cdots + c_{ik_i}\mathbf{v}_{ik_i} \in W_i$ and recalling the uniqueness of the $W_i$ component (and that this component is 0), we must have $c_{i1}\mathbf{v}_{i1} + \cdots + c_{ik_i}\mathbf{v}_{ik_i} = 0$. But $\beta_i$ is linearly independent so $c_{ij} = 0$ for each $j = 1, \ldots, k_i$ and all $i = 1, \ldots, \ell$. Therefore, $\beta$ is a linearly independent. Thus it is a basis for $V$ so 3 holds.

Finally suppose 3 holds. Let $\beta_i$ be a basis for $W_i$ (for each $i = 1, \ldots, \ell$) so that the disjoint union $\beta = \beta_1 \cup \cdots \cup \beta_\ell$ is a basis for $V$. We have that $V = \text{span}(\beta) = \text{span}(\beta_1) + \cdots + \text{span}(\beta_\ell) = W_1 + \cdots + W_\ell$. Also, suppose $\mathbf{w} \in W_i \cap \left(\sum_{i \neq j} W_j\right)$ for some $i = 1, \ldots, \ell$. Then $\mathbf{w} = c_1\mathbf{v}_1 + \cdots + c_k\mathbf{v}_k$ for some $c_1, \ldots, c_k \in \mathbb{F}$ and $\mathbf{v}_1, \ldots, \mathbf{v}_k \in \beta_i$ since $\beta_i$ spans $W_i$. But also $\mathbf{w} = s_1\mathbf{w}_1 + \cdots + s_m\mathbf{w}_m$ for some $s_1, \ldots, s_m \in \mathbb{F}$ and $\mathbf{w}_1, \ldots, \mathbf{w}_m \in \cup_{j \neq i}\beta_j$ since $\cup_{j \neq i}\beta_j$ spans $\sum_{j \neq i} W_j$. Therefore, $c_1\mathbf{v}_1 + \cdots + c_k\mathbf{v}_k - s_1\mathbf{w}_1 - \cdots - s_m\mathbf{w}_m = \mathbf{v} - \mathbf{v} = 0$. Since $\beta = \beta_1 \cup \cdots \cup \beta_\ell$ is linearly independent, we must have that $c_1 = \cdots = c_k = s_1 = \cdots = s_m = 0$. In particular, $\mathbf{v} = 0$. This establishes that $W_i \cap \left(\sum_{j \neq i} W_i\right) = \{0\}$. Thus 1 holds. □

**Definition 2.14.** If $W_i$ $(i \in I)$ are a collection of subspaces of $V$ such that any (hence all) of the above statements in the theorem above hold, we say $V$ is a *direct sum* of the $W_i$'s. This is often denoted $V = \bigoplus_{i \in I} W_i$.

In particular, we write $V = W_1 \oplus W_2$ if $V = W_1 + W_2 = \{\mathbf{w}_1 + \mathbf{w}_2 \mid \mathbf{w}_1 \in W_1 \text{ and } \mathbf{w}_2 \in W_2\}$ (i.e., every vector can be written as a sum of a vector in $W_1$ and a vector in $W_2$) as well as $W_1 \cap W_2 = \{0\}$. Likewise, $V = W_1 \oplus W_2 \oplus W_3$ if $V = W_1 + W_2 + W_3$, $W_1 \cap (W_2 + W_3) = \{0\}$, $W_2 \cap (W_1 + W_3) = \{0\}$, and $W_3 \cap (W_1 + W_2) = \{0\}$.

An immediate consequence of the third condition above is that $\dim\left(\bigoplus_{i \in I} W_i\right)$ $= \sum_{i \in I} \dim(W_i)$ (i.e., the dimension of a direct sum of subspaces is the sum of the dimensions of those subspaces). For finite dimensional spaces a kind of converse holds:

**Proposition 2.15.** *Suppose $V$ is finite dimensional and $V = W_1 + \cdots + W_\ell$. Then $V = W_1 \oplus \cdots \oplus W_\ell$ if and only if $\dim(V) = \dim(W_1) + \cdots + \dim(W_\ell)$.*

*Proof.* We already know that if the sum is direct, the dimension equation holds. Conversely suppose that the dimension equation holds. Then taking a basis for each $W_i$ and unioning them, by the assumption $V = W_1 + \cdots + W_\ell$ we must have a spanning set. By the dimension equation, if these bases were not disjoint, we would have a spanning set smaller than $\dim(W_1) + \cdots + \dim(W_\ell) = \dim(V)$ (contradiction). Thus the union of bases is disjoint. Now we see that the union is a (finite) spanning set of the right size, so it must be a basis. Finally, since our (disjoint) union of bases of our subspaces yields a basis for $V$ (direct sum criterion 3), so the sum is direct. □

## 2.2 Composition, Kernels, and Ranges

Consider the linear transformations $S : P_2 \to \mathbb{R}^{2\times 2}$ and $T : \mathbb{R}^{2\times 2} \to \mathbb{R}^2$ defined by

$$S(ct^2 + bt + a) = \begin{bmatrix} a+b & b \\ c & a+c \end{bmatrix},$$
$$T\left(\begin{bmatrix} x & y \\ u & v \end{bmatrix}\right) = (x - y, u - v),$$

respectively. Notice that if we compose these maps we get $T \circ S : P_2 \to \mathbb{R}^2$ where

$$(T \circ S)(ct^2 + bt + a) = T(S(ct^2 + bt + a)) = T\left(\begin{bmatrix} a+b & b \\ c & a+c \end{bmatrix}\right) = (a + b - b, c - (a + c)) = (a, -a).$$

Consider the standard bases: $\beta = \{1, t, t^2\}$, $\delta = \{e_1 = (1, 0), e_2 = (0, 1)\}$, and

$$\gamma = \left\{E_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, E_{12} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, E_{21} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, E_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\right\}$$

for $P_2$, $\mathbb{R}^2$, and $\mathbb{R}^{2\times 2}$ respectively. Let's find coordinate matrices for $S$, $T$, and $T \circ S$.

$$S(1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1E_{11} + 0E_{12} + 0E_{21} + 1E_{22} \implies [S(1)]_\gamma = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

$$S(t) = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = 1E_{11} + 1E_{12} + 0E_{21} + 0E_{22} \implies [S(1)]_\gamma = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$S(t^2) = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} = 0E_{11} + 0E_{12} + 1E_{21} + 1E_{22} \implies [S(1)]_\gamma = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

$$\therefore [S]^\gamma_\beta = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

---

$$T(E_{11}) = (1, 0) = 1e_1 + 0e_2 \implies [T(E_{11})]_\delta = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$
$$T(E_{12}) = (-1, 0) = -1e_1 + 0e_2 \implies [T(E_{12})]_\delta = \begin{bmatrix} -1 \\ 0 \end{bmatrix}$$
$$T(E_{21}) = (0, 1) = 0e_1 + 1e_2 \implies [T(E_{21})]_\delta = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$
$$T(E_{22}) = (0, -1) = 0e_1 - 1e_2 \implies [T(E_{22})]_\delta = \begin{bmatrix} 0 \\ -1 \end{bmatrix}$$

$$\therefore [T]^\delta_\gamma = \begin{bmatrix} 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{bmatrix}.$$

To find a coordinate matrix for $T \circ S$, we could do a direct computation like before...or we can use our work from above:

$$[T \circ S]_\beta^\delta = [T]_\gamma^\delta [S]_\beta^\gamma = \begin{bmatrix} 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ -1 & 0 & 0 \end{bmatrix}.$$

Let's find a basis for the Kernel and Range of $S$, $T$, and $T \circ S$. We know that if $X$ is a linear transformation with corresponding matrix $Y$ then $\text{Null}(Y)$ is a coordinate representation of $\text{Ker}(X)$ and $\text{Col}(Y)$ is a coordinate representation of $\text{Range}(X)$.

For $S$, we have

$$[S]_\beta^\gamma = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \overset{\text{RREF}}{\sim} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}.$$

Thus, $\text{Null}([S]_\beta^\gamma) = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \right\}$, and so $\text{Ker}(S) = \{0\}$ which means $S$ is 1-to-1 and $\text{Nullity}(S) = 0$. Next, we see that every column of the coordinate matrix is a pivot column so that $\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \right\}$ is a basis for $\text{Col}([S]_\beta^\gamma)$. These coordinate vectors correspond to the following set (which is a basis for $\text{Range}(S)$): $\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \right\}$ which is a basis for $\text{Range}(S)$. Thus $\text{Rank}(S) = 3$ (obviously $S$ is not onto).

For $T$, we have

$$[T]_\gamma^\delta = \begin{bmatrix} 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{bmatrix}.$$

Labeling variables $x_1$, $x_2$, $x_3$, and $x_4$, we have the equations: $x_1 - x_2 = 0$ and $x_3 - x_4 = 0$. $x_2$ and $x_4$ are free, so let $x_2 = s$ and $x_4 = t$ we get:

$$\begin{array}{rcl} x_1 &=& s \\ x_2 &=& s \\ x_3 &=& t \\ x_4 &=& t \end{array} \implies \mathbf{x} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} s + \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} t.$$

Thus, $\left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \right\}$ is a basis for $\text{Null}([T]_\gamma^\delta)$ which corresponds to: $\left\{ \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \right\}$ (a basis for $\text{Ker}(T)$). Therefore, $T$ is not 1-to-1 and $\text{Nullity}(T) = 2$. Next, the first and third columns of our coordinate matrix are pivot columns so that $\left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$ is a basis for $\text{Col}([T]_\gamma^\delta)$. These coordinate vectors correspond to $\{(1,0),(0,1)\}$ (the standard basis for $\mathbb{R}^2$). Therefore, $\text{Range}(T) = \mathbb{R}^2$ and $\text{Rank}(T) = 2$.

Finally, for $T \circ S$, we have

$$[T \circ S]_\beta^\delta = \begin{bmatrix} 1 & 0 & 0 \\ -1 & 0 & 0 \end{bmatrix} \overset{\text{RREF}}{\sim} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

If we label variables $x_1$, $x_2$, and $x_3$, we see that the matrix says: $x_1 = 0$. Thus $x_2$ and $x_3$ are free, say $x_2 = s$ and $x_3 = t$ so we get:

$$\begin{array}{rcl} x_1 &=& 0 \\ x_2 &=& s \\ x_3 &=& t \end{array} \implies \mathbf{x} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} s + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} t.$$

Therefore, $\left\{ \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}$ is a basis for Null($[T \circ S]_\beta^\delta$). These coordinate vectors correspond to: $\{t, t^2\}$ which is a basis for Ker$(T \circ S)$. From this we see that $T \circ S$ is not 1-to-1 and Nullity$(T \circ S) = 2$.

## 2.3 Coordinates vs. Coordinate Matrices

Let's explore the linear transformation $T : \mathbb{R}^{2\times 2} \to P_1 = \{ax + b \mid a, b \in \mathbb{R}\}$ defined by

$$T\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = (a + 2b - c)x + (a + d).$$

Let's prove $T$ is linear by showing that $T$ preserves addition and scalar multiplication.

$$\begin{aligned} T\left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}\right) &= T\left(\begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix}\right) \\ &= ((a_1 + a_2) + 2(b_1 + b_2) - (c_1 + c_2))x + ((a_1 + a_2) + (d_1 + d_2)) \\ &= ((a_1 + 2b_1 - c_1)x + (a_1 + d_1)) + ((a_2 + 2b_2 - c_2)x + (a_2 + d_2)) \\ &= T\left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}\right) + T\left(\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}\right). \\ T\left(s\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) &= T\left(\begin{bmatrix} sa & sb \\ sc & sd \end{bmatrix}\right) \\ &= (sa + 2sb - sc)x + (sa + sd) = s((a + 2b - c)x + (a + d)) \\ &= s\, T\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right). \end{aligned}$$

Next, Let's find the standard coordinate matrix for $T$. Let $\alpha = \{E_{11}, E_{12}, E_{21}, E_{22}\}$ and $\beta = \{1, x\}$. These are the standard bases for $\mathbb{R}^{2\times 2}$ and $P_1$. To find the coordinate matrix we plug each $\alpha$ (input basis) vector into our map: $T(E_{11}) = (1+2(0)-0)x+(1+0) = x+1$, $T(E_{12}) = (0+2(1)-0)x+(0+0) = 2x$, $T(E_{21}) = (0+2(0)-1)x+(0+0) = -x$, $T(E_{22}) = (0 + 2(0) - 0)x + (0 + 1) = 1$. Then we write these in terms of $\beta$ (output basis) coordinates (note the order of $\beta$ – constant term then coefficient of $x$):

$$[T]_\alpha^\beta = \begin{bmatrix} [T(E_{11})]_\beta & [T(E_{12})]_\beta & [T(E_{21})]_\beta & [T(E_{22})]_\beta \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 2 & -1 & 0 \end{bmatrix}.$$

Now, let's find the standard basis of $T$. Keep the same bases $\alpha$ and $\beta$. The map that sends the $j$-th $\alpha$ (input basis) vector to the $i$-th $\beta$ (output basis) vector and all other input vectors to $\mathbf{0}$ is called $T_{ij}$. In particular,

$$\begin{aligned} &T_{11}(E_{11}) = 1, \quad T_{11}(E_{12}) = 0, \quad T_{11}(E_{21}) = 0, \quad T_{11}(E_{22}) = 0, \\ &T_{12}(E_{11}) = 0, \quad T_{12}(E_{12}) = 1, \quad T_{12}(E_{21}) = 0, \quad T_{12}(E_{22}) = 0, \\ &T_{13}(E_{11}) = 0, \quad T_{13}(E_{12}) = 0, \quad T_{13}(E_{21}) = 1, \quad T_{13}(E_{22}) = 0, \\ &T_{14}(E_{11}) = 0, \quad T_{14}(E_{12}) = 0, \quad T_{14}(E_{21}) = 0, \quad T_{14}(E_{22}) = 1, \\ &T_{21}(E_{11}) = x, \quad T_{21}(E_{12}) = 0, \quad T_{21}(E_{21}) = 0, \quad T_{21}(E_{22}) = 0, \\ &T_{22}(E_{11}) = 0, \quad T_{22}(E_{12}) = x, \quad T_{22}(E_{21}) = 0, \quad T_{22}(E_{22}) = 0, \\ &T_{23}(E_{11}) = 0, \quad T_{23}(E_{12}) = 0, \quad T_{23}(E_{21}) = x, \quad T_{23}(E_{22}) = 0, \\ &T_{24}(E_{11}) = 0, \quad T_{24}(E_{12}) = 0, \quad T_{24}(E_{21}) = 0, \quad T_{24}(E_{22}) = x \end{aligned}$$

These maps are rigged up so that $[T_{ij}]_\alpha^\beta = E_{ij}$. So just as $\{E_{11}, E_{12}, E_{13}, E_{14}, E_{21}, E_{22}, E_{23}, E_{24}\}$ is a basis for $\mathbb{R}^{2\times 4}$, we have that $\gamma = \{T_{11}, T_{12}, T_{13}, T_{14}, T_{21}, T_{22}, T_{23}, T_{24}\}$ is a basis for the space of linear transformations from $\mathbb{R}^{2\times 4}$ to $P_1$ (that is $\mathcal{L}(\mathbb{R}^{2\times 2}, P_1) = \text{Hom}_{\mathbb{R}}(\mathbb{R}^{2\times 2}, P_1)$).

For example, notice that $(T_{11} + T_{14} + T_{21} + 2T_{22} - T_{23})(E_{11}) = T_{11}(E_{11}) + T_{14}(E_{11}) + T_{21}(E_{11}) + 2T_{22}(E_{11}) - T_{23}(E_{11}) = 1 + 0 + x + 2(0) - 0 = 1 + x = T(E_{11})$. In fact, $T_{11} + T_{14} + T_{21} + 2T_{22} - T_{23}$ and $T$ match on all the $\alpha$ basis vectors. Therefore, $T = T_{11} + T_{14} + T_{21} + 2T_{22} - T_{23}$.

Our coordinate isomorphisms are compatible with this as well. Notice that $[T]_\alpha^\beta = E_{11} + E_{14} + E_{21} + 2E_{22} - E_{23}$ (changing the $T_{ij}$'s to $E'_{ij}s$).

Therefore, in $\gamma$ coordinates we have

$$T \text{ as a vector in } \mathcal{L}(\mathbb{R}^{2\times 2}, P_1) : [T]_\gamma = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 2 \\ -1 \\ 0 \end{bmatrix}$$

compared with

$$T \text{ as a coordinate matrix} : [T]_\alpha^\beta = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 2 & -1 & 0 \end{bmatrix}.$$

Let $V$ be an $n$-dimensional space (over $\mathbb{F}$) with basis $\alpha = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ and let $W$ be an $m$-dimensional space (over $\mathbb{F}$) with basis $\beta = \{\mathbf{w}_1, \ldots, \mathbf{w}_m\}$. For each $1 \leq k \leq n$, define

$$T_{ij}(\mathbf{v}_k) = \delta_{jk}\mathbf{w}_i = \begin{cases} \mathbf{w}_i & j = k \\ \mathbf{0} & j \neq k \end{cases}.$$

This is the map that sends input basis vector $j$ to output basis vector $i$ and then kills the rest of the input vectors.

We have that $\gamma = \{T_{11}, \ldots, T_{1n}, T_{21}, \ldots, T_{2n}, \ldots, T_{m1}, \ldots, T_{mn}\}$ is a basis for $\mathcal{L}(V, W) = \text{Hom}_{\mathbb{F}}(V, W)$ (the space of all linear maps from $V$ to $W$).

Let $T : V \to W$ be a linear map (i.e. $T \in \mathcal{L}(V, W) = \text{Hom}_{\mathbb{F}}(V, W)$). Let $A = (a_{ij}) = [T]_\alpha^\beta$. This means that $T(\mathbf{v}_k) = \sum_{i=1}^{m} a_{ik}\mathbf{w}_i$ (the $k$-th column of $A = [T]_\alpha^\beta$ is given by the coordinates of $T(\mathbf{v}_k)$).

Consider $S = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}T_{ij}$. Then, we have that $S(\mathbf{v}_k) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}T_{ij}(\mathbf{v}_k) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}\delta_{jk}\mathbf{w}_i = \sum_{i=1}^{m} a_{ik}\mathbf{w}_i$ (only the $j = k$ terms survive). Therefore, $S(\mathbf{v}_k) = T(\mathbf{v}_k)$ for $1 \leq k \leq n$. Since $S$ and $T$ match on a basis, $S = T$. We have that $T = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}T_{ij}$. In other words, the $\gamma$-coordinates of $T$ are exactly the entries of $A = [T]_\alpha^\beta$ (its coordinate matrix), i.e.,

$$[T]_\alpha^\beta = A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \implies [T]_\gamma = \begin{bmatrix} a_{11} \\ \vdots \\ a_{1n} \\ a_{21} \\ \vdots \\ a_{2n} \\ \vdots \\ a_{m1} \\ \vdots \\ a_{mn} \end{bmatrix}.$$

## 2.4 Coordinate Matrices Examples

Let's explore coordinate representations of matrices and changes of basis. Let $T : \mathbb{R}^2 \to \mathbb{R}^2$ be defined by $T(x, y) = (3x+2y, 4y)$. We will consider the relationships between matrix representations of $T$ in coordinate systems associated with the following bases:

$$\begin{aligned} \alpha &= \{(1,0),(0,1)\}, \quad \text{(The standard basis)} \\ \beta &= \{(1,1),(-2,3)\}, \\ \beta' &= \{(1,-1),(0,1)\}. \end{aligned}$$

First, let's compute $[T]_\alpha$ (the standard matrix of $T$), $[T]_\beta$, and $[T]_{\beta'}$.

$$\begin{aligned} T((1,0)) = (3,0) = 3(1,0) + 0(0,1) \quad &\implies \quad [T((1,0))]_\alpha = \begin{bmatrix} 3 \\ 0 \end{bmatrix} \\ T((0,1)) = (2,4) = 2(1,0) + 4(0,1) \quad &\implies \quad [T((0,1))]_\alpha = \begin{bmatrix} 2 \\ 4 \end{bmatrix} \\ \therefore [T]_\alpha = \left[ \; [T((1,0))]_\alpha \mid [T((0,1))]_\alpha \; \right] &= \begin{bmatrix} 3 & 2 \\ 0 & 4 \end{bmatrix} = A. \end{aligned}$$

---

$$\begin{aligned} T((1,1)) = (5,4) = \tfrac{23}{5}(1,1) - \tfrac{1}{5}(-2,3) \quad &\implies \quad [T((1,1))]_\beta = \begin{bmatrix} 23/5 \\ -1/5 \end{bmatrix} \\ T((-2,3)) = (0,12) = \tfrac{24}{5}(1,1) + \tfrac{12}{5}(-2,3) \quad &\implies \quad [T((-2,3))]_\beta = \begin{bmatrix} 24/5 \\ 12/5 \end{bmatrix} \\ \therefore [T]_\beta = \left[ \; [T((1,1))]_\beta \quad [T((-2,3))]_\beta \; \right] &= \frac{1}{5}\begin{bmatrix} 23 & 24 \\ -1 & 12 \end{bmatrix} = B. \end{aligned}$$

---

$$\begin{aligned} T((1,-1)) = (1,-4) = 1(1,-1) - 3(0,1) \quad &\implies \quad [T((1,-1))]_{\beta'} = \begin{bmatrix} 1 \\ -3 \end{bmatrix} \\ T((0,1)) = (2,4) = 2(1,-1) + 6(0,1) \quad &\implies \quad [T((1,-1))]_{\beta'} = \begin{bmatrix} 2 \\ 6 \end{bmatrix} \\ \therefore [T]_{\beta'} = \left[ \; [T((1,-1))]_{\beta'} \quad [T((0,1))]_{\beta'} \; \right] &= \begin{bmatrix} 1 & 2 \\ -3 & 6 \end{bmatrix} = C. \end{aligned}$$

Next, let's compute change of basis matrices. To convert from $\beta$-coordinates to $\alpha$-coordinates and then from $\beta'$-coordinates to $\alpha$-coordinates.

$$\begin{aligned} (1,1) = 1(1,0) + 1(0,1) \quad &\implies \quad [(1,1)]_\alpha = \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\ (-2,3) = -2(1,0) + 3(0,1) \quad &\implies \quad [(-2,3)]_\alpha = \begin{bmatrix} -2 \\ 3 \end{bmatrix} \end{aligned}$$

Therefore, we can change from $\beta$ to $\alpha$ coordinates with the following matrix:

$$[I]_\beta^\alpha = \begin{bmatrix} 1 & -2 \\ 1 & 3 \end{bmatrix} = P.$$

$$\begin{aligned} (1,-1) = 1(1,0) - 1(0,1) \quad &\implies \quad [(1,-1)]_\alpha = \begin{bmatrix} 1 \\ -1 \end{bmatrix} \\ (0,1) = 0(1,0) + 1(0,1) \quad &\implies \quad [(0,1)]_\alpha = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \end{aligned}$$

Therefore, we can change from $\beta'$ to $\alpha$ coordinates with the following matrix:

$$[I]_{\beta'}^{\alpha} = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} = Q.$$

To change from $\beta$ to $\beta'$ coordinates we can follow: $\beta \to \alpha \to \beta'$, thus

$$[I]_{\beta}^{\beta'} = [I]_{\alpha}^{\beta'}[I]_{\beta}^{\alpha} = Q^{-1}P = \begin{bmatrix} 1 & -2 \\ 2 & 1 \end{bmatrix}.^{1}$$

Notice the following:

$$[T]_{\beta} = [I]_{\alpha}^{\beta}[T]_{\alpha}[I]_{\beta}^{\alpha} = P^{-1}AP = B$$

---

$$[T]_{\beta'} = [I]_{\alpha}^{\beta'}[T]_{\alpha}[I]_{\beta'}^{\alpha} = Q^{-1}AQ = C$$

---

$$[T]_{\beta}^{\beta'} = [I]_{\beta}^{\beta'}[T]_{\beta} = \begin{bmatrix} 1 & -2 \\ 2 & 1 \end{bmatrix} \frac{1}{5} \begin{bmatrix} 23 & 24 \\ -1 & 12 \end{bmatrix} = \begin{bmatrix} 5 & 0 \\ 9 & 12 \end{bmatrix}$$

$$\text{or } [T]_{\beta}^{\beta'} = [I]_{\alpha}^{\beta'}[T]_{\alpha}[I]_{\beta}^{\alpha} = Q^{-1}AP = \begin{bmatrix} 5 & 0 \\ 9 & 12 \end{bmatrix}.$$

Finally, let $\mathbf{v} = (-1, 3)$ then $[\mathbf{v}]_{\alpha} = \begin{bmatrix} -1 \\ 3 \end{bmatrix}$ so that $[\mathbf{v}]_{\beta'} = [I]_{\alpha}^{\beta'}[\mathbf{v}]_{\alpha} = Q^{-1}\begin{bmatrix} -1 \\ 3 \end{bmatrix} = \begin{bmatrix} -1 \\ 2 \end{bmatrix}$. Also, $[\mathbf{v}]_{\beta} = [I]_{\alpha}^{\beta}[\mathbf{v}]_{\alpha} = P^{-1}\begin{bmatrix} -1 \\ 3 \end{bmatrix} = \begin{bmatrix} 3/5 \\ 4/5 \end{bmatrix}$.

$$[T(\mathbf{v})]_{\beta'} = [T]_{\beta}^{\beta'}[\mathbf{v}]_{\beta} = \begin{bmatrix} 5 & 0 \\ 9 & 12 \end{bmatrix} \begin{bmatrix} 3/5 \\ 4/5 \end{bmatrix} = \begin{bmatrix} 3 \\ 15 \end{bmatrix}$$

On the other hand, $T(\mathbf{v}) = T((-1, 3)) = (3, 12)$ and $[T(\mathbf{v})]_{\beta'} = [I]_{\alpha}^{\beta'}\begin{bmatrix} 3 \\ 12 \end{bmatrix} = Q^{-1}\begin{bmatrix} 3 \\ 12 \end{bmatrix} = \begin{bmatrix} 3 \\ 15 \end{bmatrix}$.

## 2.5 Computing with Bases Examples

This is an extended example of computing with bases. Let us begin with a subspace $W$ of $\mathbb{R}^5$:

$$W = \left\{ \begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{bmatrix} \in \mathbb{R}^5 \;\middle|\; \begin{aligned} v_1 + 2v_2 - v_3 + v_4 + 5v_5 &= 0, \\ v_3 + v_4 - 2v_5 &= 0, \\ -v_1 - 2v_2 + 2v_3 - 7v_5 &= 0 \end{aligned} \right\}.$$

We might immediately notice that the elements of $W$ satisfy a system of homogeneous equations. In particular, for any $\mathbf{v} \in W$ we have

$$A\mathbf{v} = \begin{bmatrix} 1 & 2 & -1 & 1 & 5 \\ 0 & 0 & 1 & 1 & -2 \\ -1 & -2 & 2 & 0 & -7 \end{bmatrix} \mathbf{v} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

Therefore, $W = \text{Null}(A)$. So $W$ is indeed a subspace of $\mathbb{R}^5$.

To find a basis for $W$, we should find the RREF of $A$ and solve the system $A\mathbf{x} = \mathbf{0}$:

[1] Or directly, $(1, 1) = 1(1, -1) + 2(0, 1)$ and $(-2, 3) = -2(1, -1) + 1(0, 1)$.

$$\begin{bmatrix} 1 & 2 & -1 & 1 & 5 \\ 0 & 0 & 1 & 1 & -2 \\ -1 & -2 & 2 & 0 & -7 \end{bmatrix} \overset{\text{RREF}}{\sim} \begin{bmatrix} 1 & 2 & 0 & 2 & 3 \\ 0 & 0 & 1 & 1 & -2 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\begin{array}{rcll} x_1 &=& -2r-2s-3t & \\ x_2 &=& r & \\ x_3 &=& -s+2t & \Longrightarrow \mathbf{x} = \begin{bmatrix} -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} r + \begin{bmatrix} -2 \\ 0 \\ -1 \\ 1 \\ 0 \end{bmatrix} s + \begin{bmatrix} -3 \\ 0 \\ 2 \\ 0 \\ 1 \end{bmatrix} t \\ x_4 &=& s & \\ x_5 &=& t & \end{array}$$

$$\therefore W = \text{span}\left\{ \begin{bmatrix} -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} -2 \\ 0 \\ -1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} -3 \\ 0 \\ 2 \\ 0 \\ 1 \end{bmatrix} \right\} = \text{Col}\,(B) \text{ where } B = \begin{bmatrix} -2 & -2 & -3 \\ 1 & 0 & 0 \\ 0 & -1 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Moreover, these 3 vectors form a basis for $W$, so we now know that $\dim(W) = 3$. Also, notice that $W = \text{Null}(A) = \text{Col}(B)$, so $W$ can be viewed as both a null space and a column space. While not obvious, it is true that <u>all</u> subspaces of $\mathbb{R}^n$ can be viewed as both null spaces and column spaces if we pick the right matrices.

Let's ask the question: "Is $\mathbf{w} = \begin{bmatrix} 1 \\ 2 \\ 3 \\ 2 \\ 1 \end{bmatrix} \in W$ ?" There are 2 basic techniques for checking.

<u>Way 1</u>: Since $W$ is a nullspace, we can see if "$A\mathbf{w} = \mathbf{0}$" is satisfied. So $\mathbf{w} \notin W$ because

$$A\mathbf{w} = \begin{bmatrix} 1 & 2 & -1 & 1 & 5 \\ 0 & 0 & 1 & 1 & -2 \\ -1 & -2 & 2 & 0 & -7 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 3 \\ 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 9 \\ 3 \\ -6 \end{bmatrix} \neq \mathbf{0}.$$

<u>Way 2</u>: We can use the basis that we found above to check is our vector belongs to $W$. This is a lot more work than our previous technique. However, if we have a subspace described as the "span" of a set of vectors, we are more-or-less forced to check this way. Specifically, we will adjoin the vector in question to the spanning set (which is actually a basis in this case) and then row reduce:

$$[B : \mathbf{w}] = \left[\begin{array}{ccc:c} -2 & -2 & -3 & 1 \\ 1 & 0 & 0 & 2 \\ 0 & -1 & 2 & 3 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 \end{array}\right] \overset{\text{RREF}}{\sim} \left[\begin{array}{ccc:c} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right].$$

Since the final column is a pivot column, the final column is **not** contained in the span of the previous columns. Therefore, $\mathbf{w} \notin W$.

This illustrates that null space membership is easier to check than column space membership.

Next, let's show that $S = \{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$ is a subset of $W$ where $\mathbf{a} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ -1 \\ 0 \end{bmatrix}$, $\mathbf{b} = \begin{bmatrix} 2 \\ -2 \\ -1 \\ 1 \\ 0 \end{bmatrix}$, and $\mathbf{c} = \begin{bmatrix} 8 \\ -4 \\ 0 \\ 0 \\ 0 \end{bmatrix}$. Again let's do this 2 ways (first the easy way, then the hard way).

A quick check shows $A\mathbf{a} = \mathbf{0}$, $A\mathbf{b} = \mathbf{0}$, and $A\mathbf{c} = \mathbf{0}$ so $\mathbf{a}, \mathbf{b}, \mathbf{c} \in W$. So $S \subset W$ ($S$ is contained in $W$).

Alternatively, we can adjoin our three vectors to the spanning set from before and row reduce:

$$[B : \mathbf{a}\ \mathbf{b}\ \mathbf{c}] = \left[\begin{array}{ccc:ccc} -2 & -2 & -3 & 0 & 2 & 8 \\ 1 & 0 & 0 & 1 & -2 & -4 \\ 0 & -1 & 2 & 1 & -1 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{array}\right] \overset{\text{RREF}}{\sim} \left[\begin{array}{ccc:ccc} 1 & 0 & 0 & 1 & -2 & -4 \\ 0 & 1 & 0 & -1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right].$$

So we put our "known" vectors to the left and the vectors to "test" to the right. Since there are no "new" pivot columns (coming from our test vectors), they must all lie in the span of our known vectors. In particular, $\mathbf{a}$ is just the difference between the first two vectors, $\mathbf{b}$ is $-2$ times the first vector plus the second vector, and $\mathbf{c}$ is just $-4$ times the first vector. Thus the new vectors are all elements of $W$. Hence $S \subset W$.

We already know that $S$ is a subset of $W$. But is $S$ a linearly independent set? And, can we extend all (or part) of $S$ to a basis for $W$? To answer both of these questions (at the same time) we should put the vectors from $S$ into a matrix and adjoin a known basis for $W$. To guarantee that the vectors in $S$ are placed in the basis we are trying to compute, we should place them on the left (this gives them preferential treatment).

$$\left[\begin{array}{ccc:ccc} 0 & 2 & 8 & -2 & -2 & -3 \\ 1 & -2 & -4 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 & -1 & 2 \\ -1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right] \overset{\text{RREF}}{\sim} \left[\begin{array}{ccc:ccc} 1 & 0 & 4 & -1 & -2 & 0 \\ 0 & 1 & 4 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

Notice that the third column is <u>not</u> a pivot column. In fact, the linear correspondence says that it is 4 times the first column plus 4 times the second. Thus $S$ is linearly dependent.

Next, notice that the fourth and fifth columns are also linear combinations of the first two columns. So they are also redundant. However, the last column is a pivot column, so it is not contained in the span of the first two columns. Adding this vector to the first two will yield a basis for $W$.

$\beta = \left\{ \begin{bmatrix} 0 \\ 1 \\ 1 \\ -1 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ -2 \\ -1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} -3 \\ 0 \\ 2 \\ 0 \\ 1 \end{bmatrix} \right\}$ is a basis for $W$ (which includes as much of $S$ as possible).

Let's note one last thing. If we had listed the vectors from $S$ in a different order, we would end up with a different basis:

$$\left[\begin{array}{ccc:ccc} 8 & 0 & 2 & -2 & -2 & -3 \\ -4 & 1 & -2 & 1 & 0 & 0 \\ 0 & 1 & -1 & 0 & -1 & 2 \\ 0 & -1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right] \overset{\text{RREF}}{\sim} \left[\begin{array}{ccc:ccc} 1 & 0 & 1/4 & -1/4 & -1/4 & 0 \\ 0 & 1 & -1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

$$\implies \beta = \left\{ \begin{bmatrix} 8 \\ -4 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \\ -1 \\ 0 \end{bmatrix}, \begin{bmatrix} -3 \\ 0 \\ 2 \\ 0 \\ 1 \end{bmatrix} \right\}.$$

This is also a basis for $W$ and it also includes two vectors from $S$, but not the same vectors as before. This is due to our change in "preferences" (the change in the order in which we listed the vectors).

## 2.6 Dual Spaces

In this section, we will run through some basics about dual spaces. Throughout this section, $V$ will denote a vector space over a field $\mathbb{F}$. Unless otherwise stated, we do not assume that our vector spaces are finite dimensional.

**Definition 2.16.** $V^* = \{f : V \to \mathbb{F} \mid f \text{ is linear}\}$ is called the *dual space* of $V$. In other notations: $V^* = \text{Hom}(V, \mathbb{F}) = \mathcal{L}(V, \mathbb{F})$. Elements of $V^*$ are called *linear functionals* or *dual vectors*.

For example, let $f(x, y, z) = x + 3y - z$. Then $f \in (\mathbb{R}^3)^*$ ($f$ is a linear functional aka a dual vector) since $f$ is a linear function from $\mathbb{R}^3$ to $\mathbb{R}$.

Dual spaces are particularly useful when dealing with finite dimensional spaces. Suppose $V$ is finite dimensional (say $\dim(V) = n < \infty$) with basis $\alpha = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$.

**Definition 2.17.** Let $\alpha^* = \{\mathbf{v}_1^*, \ldots, \mathbf{v}_n^*\}$ where $\mathbf{v}_i^* \left( \sum_{j=1}^{n} c_j \mathbf{v}_j \right) = \sum_{j=1}^{n} c_j \delta_{ij} = c_i$ for any $c_1, \ldots, c_n \in \mathbb{F}$. In other words, let $\mathbf{v}_i^*(\mathbf{v}_j) = \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$ (i.e., the Kronecker delta aka the components of the identity matrix) and extend linearly. Then $\alpha^*$ is a set of dual vectors in $V^*$. It is called the *dual basis* associated with $\alpha$.

Notice that $\mathbf{v}_i^*$ is nothing more than the $i^{\text{th}}$ coordinate function. In particular, if $\pi_i : \mathbb{F}^{n \times 1} \to \mathbb{F}$ is the $i^{\text{th}}$ projection: $\pi_i \left( [c_1 \; c_2 \; \cdots \; c_n]^T \right) = c_i$, then $\mathbf{v}_i^* = \pi_i \circ [\,\cdot\,]_\alpha$ (i.e., the $i^{\text{th}}$ dual basis vector takes the $\alpha$-coordinates of a vector and kicks out the $i^{\text{th}}$ one).

**Theorem 2.18.** *Given a finite dimensional vector space $V$ with basis $\alpha = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$, its dual basis $\alpha^* = \{\mathbf{v}_1^*, \ldots, \mathbf{v}_n^*\}$ is in fact a basis for $V^*$. Consequently* $\dim(V) = \dim(V^*)$.

*Proof.* Instead of assuming the result: $\dim(V^*) = \dim(\text{Hom}(V, \mathbb{F})) = \dim(V) \cdot \dim(\mathbb{F}) = \dim(V) \cdot 1 = \dim(V)$, I will show that $\alpha^*$ is both linearly independent and that it spans $V^*$.

Suppose $\sum_{i=1}^{n} s_i \mathbf{v}_i^* = 0$. Plug in the $j^{\text{th}}$ basis vector: $\sum_{i=1}^{n} s_i \mathbf{v}_i^*(\mathbf{v}_j) = 0(\mathbf{v}_j)$ and get $\sum_{i=1}^{n} s_i \delta_{ij} = 0$. So since $\delta_{ij} = 0$ unless $i = j$, $0 + \cdots + 0 + s_j \cdot 1 + 0 + \cdots + 0 = 0$ and we have $s_j = 0$. Thus the $\mathbf{v}_i^*$'s are linearly independent.

Now suppose $f \in V^*$. We claim that $f = \sum_{i=1}^{n} f(\mathbf{v}_i) \mathbf{v}_i^*$. To show two linear transformations are equal, it is enough to show that they coincide on a basis. Notice that $\sum_{i=1}^{n} f(\mathbf{v}_i) \mathbf{v}_i^*(\mathbf{v}_j) = \sum_{i=1}^{n} f(\mathbf{v}_i) \delta_{ij} = f(\mathbf{v}_j)$. Therefore, $f$ and $\sum_{i=1}^{n} f(\mathbf{v}_i) \mathbf{v}_i^*$ match on $\alpha$ so that they are equal. This shows that the $\mathbf{v}_i^*$'s span $V^*$. □

The last calculation in the proof shows something even more interesting. The $\alpha^*$-coordinates of $f$ are precisely $[f(\mathbf{v}_1) \; f(\mathbf{v}_2) \; \cdots \; f(\mathbf{v}_n)]^T$. In other words, just as $\mathbf{v}_i^*$ is the $i^{\text{th}}$ coordinate function relative to $\alpha$, "plugging $f$ into $\mathbf{v}_i$" (i.e, $f \mapsto f(\mathbf{v}_i)$) shows that $\mathbf{v}_i$ is the $i^{\text{th}}$ coordinate function relative to $\alpha^*$. Thus the first scent of *duality*.

Let's make this more transparent. Given $\mathbf{v} \in V$ and $f \in V^*$, one can compute the scalar $f(\mathbf{v})$. We ask the question, "Are we plugging $\mathbf{v}$ into $f$ or $f$ into $\mathbf{v}$?" We can think about $f(\mathbf{v})$ either way. Consider $\mathbf{v}^{**} : V^* \to \mathbb{F}$ defined by $\mathbf{v}^{**}(f) = f(\mathbf{v})$. Notice that for any $f, g \in V^*$ and $s \in \mathbb{F}$, we have $\mathbf{v}^{**}(f + g) = (f + g)(\mathbf{v}) = f(\mathbf{v}) + g(\mathbf{v}) = \mathbf{v}^{**}(f) + \mathbf{v}^{**}(g)$ and $\mathbf{v}^{**}(sf) = (sf)(\mathbf{v}) = s\, f(\mathbf{v}) = s\, \mathbf{v}^{**}(f)$. Therefore, $\mathbf{v}^{**}$ is a linear map from $V^*$ to $\mathbb{F}$. In other words, $\mathbf{v}^{**} \in V^{**}$ (i.e., $\mathbf{v}^{**}$ belongs to the so-called *double dual* of $V$).

**Theorem 2.19.** *Consider the evaluation mapping* $\text{ev} : V \to V^{**}$ *defined by* $\mathbf{v} \mapsto \mathbf{v}^{**}$ *so that for any* $f \in V^*$, $(\text{ev}(\mathbf{v}))(f) = \mathbf{v}^{**}(f) = f(\mathbf{v})$. *Thus* $\text{ev}(\mathbf{v})$ *is just evaluating dual vectors at* $\mathbf{v}$. *Then* ev *is a monomorphism (i.e., a one-to-one linear transformation). Moreover, if* $\dim(V) < \infty$, *then* ev *is an isomorphism and* $V \cong V^{**}$.

*Proof.* Let $s \in \mathbb{F}$, $f \in V^*$, and $\mathbf{u}, \mathbf{v} \in V$. We already know that $\text{ev}(\mathbf{v}) = \mathbf{v}^{**} \in V^{**}$. Let us show that the evaluation map is linear: $\text{ev}(\mathbf{u} + \mathbf{v})(f) = f(\mathbf{u} + \mathbf{v}) = f(\mathbf{u}) + f(\mathbf{v}) = \text{ev}(\mathbf{u})(f) + \text{ev}(\mathbf{v})(f) = (\text{ev}(\mathbf{u}) + \text{ev}(\mathbf{v}))(f)$. Since these functions coincide on every input $f$, we conclude that $\text{ev}(\mathbf{u} + \mathbf{v}) = \text{ev}(\mathbf{u}) + \text{ev}(\mathbf{v})$. Likewise, $\text{ev}(s\mathbf{v})(f) = f(sv) = sf(\mathbf{v}) = s\text{ev}(\mathbf{v})(f)$ so $\text{ev}(s\mathbf{v}) = s\text{ev}(\mathbf{v})$. Therefore, ev is linear.

Next, suppose $\text{ev}(\mathbf{v}) = 0$. Therefore, $f(\mathbf{v}) = \text{ev}(\mathbf{v})(f) = 0(f) = 0$ for all $f \in V^*$. Thus $f = 0$ and so ev has a trivial kernel which implies it is one-to-one.

Finally, if $\dim(V) < \infty$, then $\dim(V) = \dim(V^*) = \dim(V^{**})$ so our one-to-one linear transformation is automatically onto and thus is an isomorphism. □

This map is never onto when $V$ is infinite dimensional. In fact, we state the following theorem without proof (see IX.5 Theorem 2 – page 247 – in Nathan Jacobson's Lectures in Abstract Algebra Volume II):

**Theorem 2.20.** *Suppose $V$ is an* infinite *dimensional vector space (over $\mathbb{F}$). Then* $\dim(V^*) = |\mathbb{F}|^{\dim(V)}$. *In particular,* $\dim(V) < \dim(V^*)$, *so $V \ncong V^*$.*

For example, working over $\mathbb{R}$, $\dim((\mathbb{R}[x])^*) = |\mathbb{R}|^{\dim(\mathbb{R}[x])} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0}$. So the dual space of the (countable dimensional) space of real polynomials is continuum dimensional.

Before going over some concrete examples, we will discuss matrix entries and transpose maps.

Fix *finite dimensional* vector spaces (over $\mathbb{F}$) called $V$ and $W$. Let $\alpha = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be a basis for $V$ and $\beta = \{\mathbf{w}_1, \ldots, \mathbf{w}_m\}$ a basis for $W$. In addition, let $T : V \to W$ be a linear transformation from $V$ to $W$. Recall that $[T]_\alpha^\beta$ is the coordinate matrix of $T$ (relative to $\alpha$ and $\beta$). Its $j^{\text{th}}$ column is given by the $\beta$-coordinate vector $[T(\mathbf{v}_j)]_\beta$. Therefore...

**Corollary 2.21.** $\mathbf{w}_i^*(T(\mathbf{v}_j))$ *(i.e., the $i^{th}$ $\beta$-coordinate of $T(\mathbf{v}_j)$) is precisely the $(i,j)$-entry of the matrix $[T]_\alpha^\beta$.*

**Definition 2.22.** Let $T^* : W^* \to V^*$ be defined by $T^*(f) = f \circ T$ for all $f \in W^*$. Then $T^*$ is called the *transpose* map of $T$. Sometimes this is denoted $T^t$.

Notice that given $f \in W^*$, we have $f : W \to \mathbb{F}$ and $T : V \to W$ so $T \circ f : V \to \mathbb{F}$ makes sense. Next, suppose $\mathbf{u}, \mathbf{v} \in V$ and $s \in \mathbb{F}$, then since $f$ and $T$ preserve addition, $(T \circ f)(\mathbf{u}+\mathbf{v}) = T(f(\mathbf{u}+\mathbf{v})) = T(f(\mathbf{u}) + f(\mathbf{v})) = T(f(\mathbf{u}))+T(f(\mathbf{v})) = (T \circ f)(\mathbf{u})+(T \circ f)(\mathbf{v})$. Likewise, $(T \circ f)(s\mathbf{v}) = T(f(s\mathbf{v})) = T(s\, f(\mathbf{v})) = s\, T(f(\mathbf{v})) = s\, (T \circ f)(\mathbf{v})$. Therefore, $T \circ f$ is linear and thus does in fact belong to $V^*$.

Next, suppose $f, g \in V^*$ and $s \in \mathbb{F}$. Then $T^*(f+g) = (f+g) \circ T = f \circ T + g \circ T = T^*(f) + T^*(g)$ and $T^*(s\, f) = (s\, f) \circ T = s\, (f \circ T) = s\, T^*(f)$ because of how we define addition and scalar multiplication of linear maps. Therefore, $T^*$ is in fact a linear transformation between $W^*$ and $V^*$.

Let us calculate the coordinate matrix of the transpose map. Notice that given bases $\alpha$ for $V$ and $\beta$ for $W$, we have dual basis $\beta^*$ for $W^*$ and $\alpha^*$ for $V^*$, so asking what $[T^*]_{\beta^*}^{\alpha^*}$ is actually makes sense.

By Corollary 2.21, we know that the $(i,j)$-entry of $[T^*]_{\beta^*}^{\alpha^*}$ is given by
$\mathbf{v}_i^{**}(T^*(\mathbf{w}_j^*)) = (T^*(\mathbf{w}_j^*))(\mathbf{v}_i) = (\mathbf{w}_j^* \circ T)(\mathbf{v}_i) = \mathbf{w}_j^*(T(\mathbf{v}_i))$. This is precisely the $(j,i)$-entry of $[T]_\alpha^\beta$. Therefore...

**Corollary 2.23.** $[T^*]_{\beta^*}^{\alpha^*} = ([T]_\alpha^\beta)^T$ *(i.e., matrix of the transpose map is the transpose of the original map's matrix).*

As a consequence, given bases $\alpha$ and $\beta$ for some finite dimensional vector space $V$, the change of basis matrix $[I]_{\alpha^*}^{\beta^*}$ for $V^*$ is just the transpose of the change of basis matrix $[I]_\beta^\alpha$ for $V$.

**Example 2.24.** By writing $\alpha = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\} = \{(1,1,1), (1,-1,0), (0,0,1)\}$ in standard coordinates and row reducing, we could see that $\alpha$ is a linearly independent subset of $\mathbb{R}^3$ and so it's a basis (since it has 3 elements). Let $\text{std} = \{e_1, e_2, e_3\} = \{(1,0,0), (0,1,0), (0,0,1)\}$ be our standard basis.

Therefore, $[I]_\alpha^{\text{std}} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & -1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$ and so (by technology) we have $[I]_{\text{std}}^\alpha = ([I]_\alpha^{\text{std}})^{-1} = \begin{bmatrix} 1/2 & 1/2 & 0 \\ 1/2 & -1/2 & 0 \\ -1/2 & -1/2 & 1 \end{bmatrix}$. Therefore, $[I]_{\alpha^*}^{\text{std}^*} = (([I]_\alpha^{\text{std}})^{-1})^T = ([I]_{\text{std}}^\alpha)^T = \begin{bmatrix} 1/2 & 1/2 & 0 \\ 1/2 & -1/2 & 0 \\ -1/2 & -1/2 & 1 \end{bmatrix}^T = \begin{bmatrix} 1/2 & 1/2 & -1/2 \\ 1/2 & -1/2 & -1/2 \\ 0 & 0 & 1 \end{bmatrix}$. What does this mean?

Well, $\text{std}^*$ are the standard coordinate functions. For example, $e_2^*(x,y,z) = y$ (the second coordinate). Our change of basis matrix above says, for example, that the $\text{std}^*$ coordinates of $\mathbf{v}_1^*$ are $[1/2\ 1/2\ 0]^T$. Therefore, $\mathbf{v}_1^* = \frac{1}{2}e_1^* + \frac{1}{2}e_2^*$. Thus $\mathbf{v}_1^*(x,y,z) = \frac{1}{2}x + \frac{1}{2}y$. Likewise, $\mathbf{v}_2^*(x,y,z) = \frac{1}{2}x - \frac{1}{2}y$ and $\mathbf{v}_3^*(x,y,z) = -\frac{1}{2}x - \frac{1}{2}y + z$.

For example, notice that $\mathbf{v}_1^*(\mathbf{v}_1) = \mathbf{v}_1^*(1,1,1) = \frac{1}{2}\cdot 1 + \frac{1}{2}\cdot 1 = 1$, $\mathbf{v}_1^*(\mathbf{v}_2) = \mathbf{v}_1^*(1,-1,0) = \frac{1}{2}\cdot 1 + \frac{1}{2}\cdot(-1) = 0$, and $\mathbf{v}_1^*(\mathbf{v}_3) = \mathbf{v}_1^*(0,0,1) = 0$ as expected.

Also, we could compute the $\alpha$-coordinates of $\mathbf{v} = (1,2,3)$ using our change of basis matrix: $[I]_{\text{std}}^{\alpha}[\mathbf{v}]_{\text{std}} = \begin{bmatrix} 1/2 & 1/2 & 0 \\ 1/2 & -1/2 & 0 \\ -1/2 & -1/2 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 3/2 \\ -1/2 \\ 3/2 \end{bmatrix}$. Alternatively, $\mathbf{v}$'s $\alpha$-coordinates are the values of the $\alpha^*$ functionals applied to $\mathbf{v}$: $\mathbf{v}_1^*(\mathbf{v}) = \mathbf{v}_1^*(1,2,3) = \frac{1}{2}1 + \frac{1}{2}2 = \frac{3}{2}$, $\mathbf{v}_2^*(\mathbf{v}) = \mathbf{v}_2^*(1,2,3) = \frac{1}{2}1 - \frac{1}{2}2 = -\frac{1}{2}$, and $\mathbf{v}_3^*(\mathbf{v}) = \mathbf{v}_3^*(1,2,3) = -\frac{1}{2}1 - \frac{1}{2}2 + 1\cdot 3 = \frac{3}{2}$. Double checking: $\frac{3}{2}\mathbf{v}_1 - \frac{1}{2}\mathbf{v}_2 + \frac{3}{2}\mathbf{v}_3 = \frac{3}{2}(1,1,1) - \frac{1}{2}(1,-1,0) + \frac{3}{2}(0,0,1) = (1,2,3)$.

**Example 2.25.** Let $T : P_2 \to \mathbb{R}^{2\times 2}$ be defined by

$$T(ax^2 + bx + c) = \begin{bmatrix} a+b & a+2b+c \\ 0 & 3c \end{bmatrix}.$$

Let $\alpha = \{1, x, x^2\}$ and $\beta = \{E_{11}, E_{12}, E_{21}, E_{22}\}$ be the standard bases for $P_2$ and $\mathbb{R}^{2\times 2}$. Then we have...

$$[T]_{\alpha}^{\beta} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 2 & 1 \\ 0 & 0 & 0 \\ 3 & 0 & 0 \end{bmatrix} \implies [T]_{\beta^*}^{\alpha^*} = ([T]_{\alpha}^{\beta})^T = \begin{bmatrix} 0 & 1 & 0 & 3 \\ 1 & 2 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}.$$

For example, given $M\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = a + 2b + 3c + 4d$ (i.e., $M = E_{11}^* + 2E_{12}^* + 3E_{21}^* + 4E_{22}^* \in (\mathbb{R}^{2\times 2})^*$), then $T^*(M) = M \circ T$ is defined by $(M \circ T)(ax^2 + bx + c) = 3a + 5b + 14c$ since...

$$[T^*]_{\beta^*}^{\alpha^*}[M]_{\beta^*} = \begin{bmatrix} 0 & 1 & 0 & 3 \\ 1 & 2 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix} = \begin{bmatrix} 14 \\ 5 \\ 3 \end{bmatrix}.^2$$

## 2.7 Eigenvectors and Eigenvalues

Let $V$ be a vector space over $\mathbb{R}$ (or $\mathbb{C}$) such that $\dim(V) = n < \infty$. Let $T : V \to V$ be a linear transformation (since we are mapping from $V$ to itself, we could refer to $T$ as a linear operator).

**Definition 2.26.** Let $\mathbf{v} \in V$ such that $\mathbf{v} \neq 0$ and $T(\mathbf{v}) = \lambda\mathbf{v}$. Then $\mathbf{v}$ is an *eigenvector* for $T$ with *eigenvalue* $\lambda$. Moreover, we say that $\lambda \in \mathbb{R}$ (or $\mathbb{C}$) is an *eigenvalue* for $T$ if $T$ has an eigenvector with eigenvalue $\lambda$.

*Note.* While 0 can be an eigenvalue, $\mathbf{0}$ is not allowed to be an eigenvector. Otherwise, since $T(\mathbf{0}) = \mathbf{0} = \lambda\mathbf{0}$, we would have that every scalar is an eigenvalue of $T$ and $\mathbf{0}$ would have every scalar as its eigenvalue.

**Definition 2.27.** Let $f(t) = \det(T - tI)$. Then $f(t)$ is called the *characteristic polynomial* of $T$.[3]

*Note.* $\lambda$ is an eigenvalue of $T \iff$ there exists a non-zero vector $\mathbf{v}$ such that $T(\mathbf{v}) = \lambda\mathbf{v} \iff$ there exists a non-zero vector $\mathbf{v}$ such that $(T - \lambda I)(\mathbf{v}) = \mathbf{0} \iff \text{Ker}(T - \lambda I) \neq \mathbf{0} \iff T - \lambda I$ is not one-to-one $\iff T - \lambda I$ is not invertible $\iff \det(T - \lambda I) \neq 0$. We have just proved...

**Theorem 2.28.** *$\lambda$ is an eigenvalue of $T \iff$ $\lambda$ is a root of the characteristic polynomial of $T$, i.e., $f(\lambda) = \det(T - \lambda I) = 0$.*

[2] Keep in mind that $\beta$ goes from constant *up to* quadratic.

[3] This is the definition of Lay. Other texts define $g(t) = \det(tI - T)$ to be the characteristic polynomial. Notice that $f(t) = (-1)^n g(t)$ where $n = \dim(V)$. So for even-sized and odd-sized matrices, $f = g$ and $f = -g$ respectively.

Let $f(t)$ be the characteristic polynomial of $T$. Then $f(t)$ is a polynomial of degree $n$ whose leading coefficient is $(-1)^n$. In addition, $f(0) = \det(T)$ (the constant term is just the determinant of $T$). Also, the coefficient of $t^{n-1}$ in $f(t)$ is $(-1)^{n-1}\text{tr}(T)$, i.e., $\pm$ the trace of $T$.

**Definition 2.29.** Factor $T$'s characteristic polynomial (over $\mathbb{C}$):

$$f(t) = (-1)^n(t-\lambda_1)^{m_1}(t-\lambda_2)^{m_2}\cdots(t-\lambda_k)^{m_k}$$

where $\lambda_i \neq \lambda_j$ for $i \neq j$ and $m_i > 0$. Then the roots of $f(t)$ (i.e., the eigenvalues of $T$) are $\lambda_1, \ldots, \lambda_k$. We say that the *algebraic multiplicity* of $\lambda_i$ is $m_i$ (the number of factors $(t-\lambda_i)$ appearing in the characteristic polynomial). Notice that the sum of the algebraic multiplicities is $n = \dim(V)$ (the degree of the characteristic polynimial).

*Note.* More accurately, if we are working over $\mathbb{R}$, the non-real roots are not actually eigenvalues.

**Definition 2.30.** Let $E_\lambda = \text{Ker}(T-\lambda I) = \{\mathbf{v} \in V \mid T(\mathbf{v}) = \lambda\mathbf{v}\} = \mathbf{0} \cup \{\mathbf{v} \in V \mid \mathbf{v} \text{ is an eigenvector of } T \text{ with eigenvalue } \lambda\}$. If $E_\lambda \neq \{\mathbf{0}\}$ (i.e., $\lambda$ is an eigenvalue), then we call $E_\lambda$ an *eigenspace* of $T$. Notice that $E_\lambda$ is a subspace of $V$ since it is the kernal of a linear transformation.

**Definition 2.31.** $\dim(E\lambda) = \dim(\text{Ker}(T-\lambda I)) = \text{Nullity}(T-\lambda I)$ is called the *geometric multiplicity* of $\lambda$. This is the number of linearly independent eigenvectors with eigenvalue $\lambda$. Notice that if $\lambda$ is an eigenvalue, then $E_\lambda$ cannot be the zero subspace. Thus geometric multiplicities of eigenvalues are always at least 1.

**Theorem 2.32.** *Let $\lambda$ be an eigenvalue of $T$ with algebraic multiplicity $m$ and geometric multiplicity $g$. Then $1 \leq g \leq m$.*

**Theorem 2.33.** *Eigenvectors with different eigenvalues are linearly independent. Moreover, If $S_i$ is a linearly independent set of eigenvectors with eigenvalue $\lambda_i$ and $\lambda_i \neq \lambda_j$ for $i \neq j$, then $S_1 \dot\cup S_2 \dot\cup \ldots \dot\cup S_k$ is a linearly independent set.*

**Definition 2.34.** $T$ is *diagonalizable* if there is a basis for $V$ consisting of eigenvectors for $T$. Notice if $\beta$ is such a basis, then $[T]_\beta$ is a diagonal matrix.

**Corollary 2.35.** *$T$ is diagonalizable (over $\mathbb{R}$) if and only if the eigenvalues of $T$ all belong to $\mathbb{R}$ (i.e., the characteristic polynomial completely factors over $\mathbb{R}$) and the geometric and algebraic multiplicities of each eigenvalue match.*

## 2.8 Jordan Form

Since we compute with coordinates and coordinate matrices, when dealing with a linear transformation, it is natural to ask, "What is the nicest/simplest possible coordinate matrix representing our transformation?" If we are allowed to specify both the domain and codomain basis, the answer is quite simple.

**Proposition 2.36.** *Let $T : V \to W$ be a linear transformation between two finite dimensional vector spaces over some field. Then there is a basis $\alpha$ for $V$ and basis $\beta$ for $W$ such that $[T]_\alpha^\beta = \begin{bmatrix} 0 & I \\ 0 & 0 \end{bmatrix}$ where the zeros are appropriately sized zero matrices and $I$ is an $r \times r$ identity matrix where $r = \text{Rank}(T)$.*

*Proof.* Let $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be a basis for $\text{Ker}(T)$. This is a linearly independent subset of $V$ so we can extend it to a basis for $V$: $\alpha = \{\mathbf{v}_1, \ldots, \mathbf{v}_n, \mathbf{u}_1, \ldots, \mathbf{u}_r\}$. We have that $T(V) = T\big(\text{span}(\alpha)\big) = \text{span}\big(T(\alpha)\big) = \text{span}\{T(\mathbf{v}_1) \ldots, T(\mathbf{v}_n), T(\mathbf{u}_1), \ldots, T(\mathbf{u}_r)\} = \text{span}\{T(\mathbf{u}_1), \ldots, T(\mathbf{u}_r)\}$ since $T(\mathbf{v}_i) = \mathbf{0}$ for $i = 1, \ldots, n$. Suppose $c_1T(\mathbf{u}_1)+\cdots+c_rT(\mathbf{u}_r) = \mathbf{0}$ so that $T(c_1\mathbf{u}_1+\cdots+c_r\mathbf{u}_r) = \mathbf{0}$. Thus $c_1\mathbf{u}_1+\cdots+c_r\mathbf{u}_r \in \text{Ker}(T)$. This means that $c_1\mathbf{u}_1+\cdots+c_r\mathbf{u}_r = a_1\mathbf{v}_1+\cdots+a_n\mathbf{v}_n$ for some scalars $a_1, \ldots, a_n$. But then $c_1\mathbf{u}_1+\cdots+c_r\mathbf{u}_r-a_1\mathbf{v}_1-\cdots-a_n\mathbf{v}_n = \mathbf{0}$ and so $c_1 = \cdots = c_r = -a_1 = \cdots = -a_n = 0$ since $\alpha = \{\mathbf{v}_1, \ldots, \mathbf{v}_n, \mathbf{u}_1, \ldots, \mathbf{u}_r\}$ is linearly independent. Therefore, $\{T(\mathbf{u}_1), \ldots, T(\mathbf{u}_r)\}$ is linearly indpendent. This is a basis for the range of $T$ so that $r = \text{Rank}(T)$. We extend this linearly independent subset of the codomain $W$ to a basis for $W$, say $\beta = \{T(\mathbf{u}_1), \ldots, T(\mathbf{u}_r), \mathbf{w}_1, \ldots, \mathbf{w}_m\}$. Then $T(\mathbf{v}_i) = \mathbf{0}$ for $i = 1, \ldots, n$ implies that the first $n$ columns of $[T]_\alpha^\beta$ are filled with zeros. Evaluating $T$ on the rest of $\alpha$ (i.e., plugging in $\mathbf{u}_j$ for $j = 1, \ldots, r$) we have $T(\mathbf{u}_j)$. Since this is the $j$-th element in of $\beta$, the $(n+j)$-th column of $[T]_\alpha^\beta$ has a 1 in the $j$-th row and zeros elsewhere. Thus $[T]_\alpha^\beta$ has the form we promised. $\square$

This above result is nice enough, but in the case that $T$ is a linear operator (i.e., $T : V \to V$) it seems strange to have different bases for the domain ($= V$) and codomain (also $= V$). Thus we ask, "What is a nicest/simplest possible coordinate matrix $[T]_\beta^\beta$ for a linear operator $T : V \to V$?" This is a much more difficult problem. In fact, our field starts playing a role in this problem. If the characteristic polynomial of $T$ splits (i.e., factors into linear factors), we can demand $[T]_\beta^\beta$ be in *Jordan Form*. This is almost diagonal. However, if the characteristic polynomial does not split and we don't want to enlarge our field of scalars, we have to resort to *Rational Canonical Form* (based on so-called invariant factors) or *Primary Rational Canonical Form* (based on elementary divisors). We shall not pursue these forms here.

For the following, assume $T : V \to V$ is a linear operator on a finite dimensional vector space $V$ over a field $\mathbb{F}$, say $\dim(V) = n$. Moreover, assume that the characteristic polynomial splits (over $\mathbb{F}$): $\det(tI - T) = (t-\lambda_1)^{a_1} \cdots (t-\lambda_\ell)^{a_\ell}$ where we assume that $\lambda_i \neq \lambda_j$ for $i \neq j$ and $a_i > 0$.

Recall that $a_j$ is the algebraic multiplicity of the eigenvalue $\lambda_j$. Let $E_\lambda = \text{Ker}(T - \lambda I) = \{\mathbf{v} \in V \mid T(\mathbf{v}) = \lambda\mathbf{v}\}$ be the *eigenspace* associated with $\lambda$. We call $g_\lambda = \dim(E_\lambda)$ the *geometric multiplicity* of $\lambda$. Notice that $g_\lambda > 0$ if and only if $\lambda$ is an eigenvalue. If (and it turns out – only if) $g_j = a_j$ for all $j = 1, \ldots, \ell$, we have a basis of eigenvectors, $\beta$, and $[T]_\beta^\beta$ is a diagonal matrix with the eigenvalues appearing on the diagonal (each repeated according to its algebraic multiplicity). We now seek to have a basis of vectors that are close to being eigenvectors so our coordinate matrix is close to being diagonal.

**Definition 2.37.** Let $K_\lambda = \{\mathbf{v} \in V \mid (T - \lambda I)^k(\mathbf{v}) = \mathbf{0} \text{ for some } k > 0\}$. We call $K_\lambda$ a *generalized eigenspace* associated with $\lambda$. Its nonzero members (if it has any) are called *generalized eigenvectors*.

*Note.* Let $\mathbf{v} \neq \mathbf{0}$ and $\mathbf{v} \in K_\lambda$. Let $k$ be the smallest positive integer such that $(T - \lambda I)^k(\mathbf{v}) = \mathbf{0}$. Then $\mathbf{w} = (T - \lambda I)^{k-1}(\mathbf{v}) \neq \mathbf{0}$ but $(T - \lambda I)(\mathbf{w}) = (T - \lambda I)^k(\mathbf{v}) = \mathbf{0}$. This means $\mathbf{w}$ is an eigenvector with eigenvalue $\lambda$. In other words, $K_\lambda \neq \{\mathbf{0}\}$ if and only if $\lambda$ is an eigenvalue.

In fact, $\{\mathbf{0}\} = \text{Ker}(I) = \text{Ker}(T-\lambda I)^0 \subseteq E_\lambda = \text{Ker}(T-\lambda I) \subseteq \text{Ker}(T-\lambda I)^2 \subseteq \text{Ker}(T-\lambda I)^3 \subseteq \cdots \subseteq \bigcup_{k=1}^\infty \text{Ker}(T-\lambda I)^k = K_\lambda$ since a lower power of $T - \lambda I$ killing a vector implies that any higher power does as well. Recall that $V$ is finite dimensional. This implies that our *chain* of subspaces $\cdots \subseteq \text{Ker}(T - \lambda I)^k \subseteq \text{Ker}(T - \lambda I)^{k+1} \subseteq \cdots$ cannot grow forever (each proper containment implies a growth in dimension which is capped at $\dim(V) = n$). In particular, $K_\lambda = \text{Ker}(T - \lambda I)^n$. In fact, we can do much better. Once we know about Jordan form, it is obvious that $K_{\lambda_j} = \text{Ker}(T - \lambda_j I)^m$ where $m$ is the size of the largest Jordan block associated with $\lambda_j$.

**Theorem 2.38.** *Our vector space is the direct sum of generalized eigenspaces: $V = K_{\lambda_1} \oplus K_{\lambda_2} \oplus \cdots \oplus K_{\lambda_\ell}$. In particular, $V$ has a basis of generalized eigenvectors. Moreover, $K_{\lambda_j} = \text{Ker}(T - \lambda_j I)^{a_j}$ and $\dim(K_{\lambda_j}) = a_j$ (the algebraic multiplicity of $\lambda_j$) for each $j = 1, \ldots, \ell$.*

*Proof.* First, we show that the generalized eigenspaces form a direct sum. For each $i = 1, \ldots, \ell$, let $k_i$ be a positive integer such that $K_{\lambda_i} = \text{Ker}(T - \lambda_i)^{k_i}$. Let $\mathbf{v} \in K_{\lambda_j} \cap \left(\sum_{i \neq j} K_{\lambda_i}\right)$. Now $(t - \lambda_j)^{k_j}$ and $\prod_{i \neq j}(t - \lambda_i)^{k_i}$ are relatively prime polynomials. Thus, by the extended Euclidean algorithm, there exists polynomials $f(t)$ and $g(t)$ such that $f(t)(t - \lambda_j)^{k_j} + g(t)\prod_{i \neq j}(t - \lambda_i)^{k_i} = 1$. Therefore, $\mathbf{v} = I(\mathbf{v}) = f(T)(T - \lambda_j I)^{k_j}(\mathbf{v}) + g(T)\prod_{i \neq j}(T - \lambda_i I)^{k_i}(\mathbf{v}) = f(T)(\mathbf{0}) + g(T)(\mathbf{0}) = \mathbf{0}$ since vectors in $K_{\lambda_j}$ are killed by $(T - \lambda_j I)^{k_j}$ and vectors in $\sum_{i \neq j} K_{\lambda_i}$ are killed by $\prod_{i \neq j}(T - \lambda_i I)^{k_i}$. Therefore, $K_{\lambda_j} \cap \left(\sum_{i \neq j} K_{\lambda_i}\right) = \{\mathbf{0}\}$ and thus our sum is direct.

Next, for some $1 \leq j \leq \ell$, let $W = (T - \lambda_j I)^{k_j}(V)$ (i.e., $K_{\lambda_j}$ is the kernel and $W$ is the image of $(T - \lambda_j I)^{k_j}$). Let $\mathbf{v} \in K_{\lambda_j} \cap W$. Since $\mathbf{v} \in W$, there exists some $\mathbf{w} \in V$ such that $(T - \lambda_j I)^{k_j}(\mathbf{w}) = \mathbf{v}$. Therefore, by the definition of $\mathbf{w}$ and since $\mathbf{v}$ lies in the kernel of $(T - \lambda_j I)^{k_j}$, we have $(T - \lambda_j I)^{2k_j}(\mathbf{w}) = (T - \lambda_j I)^{k_j}[(T - \lambda_j I)^{k_j}(\mathbf{w})] = (T - \lambda_j I)^{k_j}(\mathbf{v}) = \mathbf{0}$. Thus $\mathbf{w} \in \text{Ker}(T - \lambda_j I)^{2k_j} = \text{Ker}(T - \lambda_j I)^{k_j} = K_{\lambda_j}$. In other words, $\mathbf{v} = (T - \lambda_j I)^{k_j}(\mathbf{w}) = \mathbf{0}$. Thus $K_{\lambda_j} \cap W = \{\mathbf{0}\}$. Notice that $\dim(K_{\lambda_j}) + \dim(W) = \text{Nullity}(T - \lambda_j I)^{k_j} + \text{Rank}(T - \lambda_j I)^{k_j} = \dim(V)$. Therefore, $V = K_{\lambda_j} \oplus W$. Also, notice that since $T$ commutes with $(T - \lambda_j I)^{k_j}$, we have both $T(K_{\lambda_j}) \subseteq K_{\lambda_j}$ and $T(W) \subseteq W$ (i.e., our decomposition is $T$-invariant).

Let $T_1$ be the restriction of $T$ to $K_{\lambda_j}$ and $T_2$ be the restriction of $T$ to $W$. Since $K_{\lambda_j} \cap W = \{\mathbf{0}\}$ and $K_{\lambda_j}$ contains all of the eigenvectors associated with eigenvalue $\lambda_j$, we have that $\lambda_j$ is not an eigenvalue of $T_2$. Also, since $K_{\lambda_j} \cap K_{\lambda_i} = \{\mathbf{0}\}$ for $i \neq j$ (because the generalized eigenspaces form a direct sum), we have that $\lambda_j$ is the only

eigenvalue of $T_1$. Next, because $V = K_{\lambda_j} \oplus W$ (and these subspaces are $T$-invariant), the characteristic polynomial of $T$ is the product of the characteristic polynomials of $T_1$ and $T_2$. But $\lambda_j$ is the only eigenvalue of $T_1$ and it is not an eigenvalue of $T_2$. Therefore, the characteristic polynomial of $T_1$ only has $t - \lambda_j$ factors and $T_2$'s characteristic polynomial cannot have any $t - \lambda_j$ factors. Thus the characteristic polynomial of $T_1$ must be $(t - \lambda_j)^{a_j}$ and the characteristic polynomial of $T_2$ must be $\prod_{i \neq j}(t - \lambda_i)^{a_i}$. Consequently, $\dim(K_{\lambda_j})$ (i.e., the dimension of the domain of $T_1$) must be $a_j$ (i.e., the degree of $T_1$'s characteristic polynomial).

Finally, we have $\dim(K_{\lambda_1} \oplus K_{\lambda_2} \oplus \cdots \oplus K_{\lambda_\ell}) = \dim(K_{\lambda_1}) + \cdots + \dim(K_{\lambda_\ell}) = a_1 + \cdots + a_\ell$ (i.e., the degree of the characteristic polynomial of $T$). Thus $\dim(K_{\lambda_1} \oplus K_{\lambda_2} \oplus \cdots \oplus K_{\lambda_\ell}) = n = \dim(V)$. Therefore, $K_{\lambda_1} \oplus K_{\lambda_2} \oplus \cdots \oplus K_{\lambda_\ell} = V$ and so the theorem follows. □

**Corollary 2.39.** *We have $1 \leq g_j \leq a_j$ (i.e., the geometric multiplicity never exceeds the algebraic mulitiplicity) since $E_{\lambda_j} \subseteq K_{\lambda_j}$. Also, $E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_\ell}$ (i.e., eigenspaces form a direct sum) since $E_{\lambda_j} \cap \left(\sum_{i \neq j} E_{\lambda_i}\right) \subseteq K_{\lambda_j} \cap \left(\sum_{i \neq j} K_{\lambda_i}\right) = \{\mathbf{0}\}$.*

We note that since $T$ commutes with $(T - \lambda I)^k$ for any positive integer $k$, we have $\text{Ker}(T - \lambda I)^k$ is $T$-invariant. In particular, eigenspaces and generalized eigenspaces are $T$-invariant. This means that if we create a basis for $V$ by (disjoint) unioning bases for our generalized eigenspaces, our coordinate matrix will be block diagonal with $a_j \times a_j$ blocks ($j = 1, \ldots, \ell$).

To finish developing Jordan form we need to seek nicely structured bases for our generalized eigenspaces. In particular, we wish to form bases consisting of *chains* of generalized eigenvectors: $\mathbf{v}, (T-\lambda I)(\mathbf{v}), (T-\lambda I)^2(\mathbf{v}), \ldots, (T-\lambda I)^{k-1}(\mathbf{v})$ where $\mathbf{v} \in K_\lambda$ and $(T - \lambda I)^k(\mathbf{v}) = \mathbf{0}$. First, we recall a short proof by Mark Wildon establishing the existence a basis for $K_\lambda$ consisting of such chains. Then we will put this together with our previous theorem to establish the existence of our Jordan canonical form.

**Theorem 2.40.** *The generalized eigenspace $K_\lambda$ has a basis consisting of chains of generalized eigenvectors.*

*Proof.* First, restrict $T - \lambda I$ to the domain $K_\lambda$ (this is possible since $K_\lambda$ is $(T - \lambda I)$-invariant). We proceed by induction on the dimension on the domain of our linear operator. The zero dimensional base case is trivial: If $K_\lambda = \{\mathbf{0}\}$, then $\lambda$ is not an eigenvalue. Its basis is the empty set and thus the theorem is vacuously satisfied. Suppose $K_\lambda \neq \{\mathbf{0}\}$ and let $a$ be the algebraic multiplicity of $\lambda$ (i.e., $\dim(K_\lambda) = a$) so that $K_\lambda = \text{Ker}(T - \lambda I)^a$. Assume the theorem holds for all spaces of dimension less than $a$.

Notice that $(T - \lambda I)(K_\lambda)$ is properly contained in $K_\lambda$ since otherwise $K_\lambda = (T - \lambda I)(K_\lambda) = (T - \lambda I)^2(K_\lambda) = \cdots = (T - \lambda I)^a(K_\lambda) = \{\mathbf{0}\}$ (contradiction). Also, if $T - \lambda I = 0$ on $K_\lambda$, then $K_\lambda = E_\lambda$ and we have a basis of eigenvectors (and thus are done since eigenvectors are chains of length 1).

Therefore, we may assume that $(T - \lambda I)(K_\lambda)$ is non-zero and properly contained in $K_\lambda$. We apply an inductive hypothesis to $(T-\lambda I)(K_\lambda)$ and find $\mathbf{v}_1, \ldots, \mathbf{v}_m \in (T-\lambda I)(K_\lambda)$ so that $\mathbf{v}_1, (T-\lambda I)(\mathbf{v}_1), \ldots, (T-\lambda I)^{b_1-1}(\mathbf{v}_1), \ldots, \mathbf{v}_m$, $(T-\lambda I)(\mathbf{v}_m), \ldots, (T-\lambda I)^{b_m}(\mathbf{v}_m)$ is a basis of chains of generalized eigenvectors for $(T-\lambda I)(K_\lambda)$ and $(T-\lambda I)^{b_j}(\mathbf{v}_j) = \mathbf{0}$ for $j = 1, \ldots, m$. Consequently, $\dim((T - \lambda I)(K_\lambda)) = b_1 + \cdots + b_m$.

Notice $\mathbf{v}_j \in (T - \lambda I)(K_\lambda)$ implies we may choose some $\mathbf{u}_j \in K_\lambda$ such that $(T - \lambda I)(\mathbf{u}_j) = \mathbf{v}_j$ (so now $\mathbf{v}_j, \ldots,$ $(T - \lambda I)^{b_j-1}(\mathbf{v}_j)$ becomes $(T - \lambda I)(\mathbf{u}_j), \ldots, (T - \lambda I)^{b_j})(\mathbf{u}_j)$). Clearly $\text{Ker}(T - \lambda I)$ contains the linearly indpendent vectors $(T - \lambda I)^{b_1}(\mathbf{u}_1), \ldots, (T - \lambda I)^{b_m}(\mathbf{u}_m)$ (formerly called $(T - \lambda I)^{b_1-1}(\mathbf{v}_1), \ldots, (T - \lambda I)^{b_m-1}(\mathbf{v}_m)$). We extend this set to a basis for $\text{Ker}(T - \lambda I)$ by adjoining $\mathbf{w}_1, \ldots, \mathbf{w}_p$.

*Claim:* $\mathbf{u}_1, (T-\lambda I)(\mathbf{u}_1), \ldots, (T-\lambda I)^{b_1}(\mathbf{u}_1), \ldots, \mathbf{u}_m, (T-\lambda I)(\mathbf{u}_m), \ldots, (T-\lambda I)^{b_m}(\mathbf{u}_m), \mathbf{w}_1, \ldots, \mathbf{w}_p$ is a basis for $K_\lambda$ consisting of chains of generalized eigenvectors. Notice that $(T-\lambda)^{b_i+1}(\mathbf{u}_i) = \mathbf{0}$ for $i = 1, \ldots, m$ and $(T-\lambda I)(\mathbf{w}_q) = \mathbf{0}$ for $q = 1, \ldots, p$. Suppose $\sum_{i=1}^m \sum_{j=0}^{b_i} c_{ij}(T - \lambda I)^j(\mathbf{u}_i) + \sum_q d_q \mathbf{w}_q = \mathbf{0}$. Applying $T - \lambda I$ to this equation, we kill off the terms coming from elements of $\text{Ker}(T-\lambda I)$. We are left with $\sum_{i=1}^m \sum_{j=0}^{b_i-1} c_{ij}(T-\lambda I)^{j+1}(\mathbf{u}_i) = \mathbf{0}$. But this is just a linear combination of vectors coming from our basis for $(T - \lambda I)(K_\lambda)$. Therefore, $c_{ij} = 0$ for all $i = 1, \ldots, m$ and $j = 0, \ldots, b_i - 1$. Thus our equation is becomes: $c_{1b_1}(T-\lambda I)^{b_1}(\mathbf{u}_1) + \cdots + c_{mb_m}(T-\lambda I)^{b_m}(\mathbf{u}_m) + d_1\mathbf{w}_1 + \cdots + d_p\mathbf{w}_p = \mathbf{0}$. But these form a basis for $\text{Ker}(T - \lambda I)$ and thus the rest of our scalar coefficients are zero.

Therefore, our set is linearly independent. Finally, notice that our proposed basis has $(b_1+1)+\cdots+(b_m+1)+p = b_1+\cdots+b_m+m+p$ vectors in it. We already noted that $\dim\big((T-\lambda I)(K_\lambda)\big) = b_1+\cdots+b_m$ and from our construction

of $\mathbf{w}_q$'s we have $\dim\big(\mathrm{Ker}(T-\lambda I)\big) = m+p$. Therefore, by the rank nullity theorem, $\dim(K_\lambda) = b_1+\cdots+b_m+m+p$. Thus our set also spans $K_\lambda$. This establishes our claim. □

These theorems put together tells us that $V$ has a basis consisting of chains of generalized eigenvectors. Once again, since $T$ commutes with $T-\lambda I$, it is not hard to see that the span of a chain of generalized eigenvectors is a $T$-invariant subspace of $V$. Thus if we use a basis consisting of chains of generlized eigenvectors our coordinate matrix will be block diagonal with each block corresponding to some chain. Let us see what such a block looks like. To that end suppose $\mathbf{v}_1 = (T-\lambda I)^{k-1}(\mathbf{v}), \ldots, \mathbf{v}_{k-1} = (T-\lambda I)(\mathbf{v}), \mathbf{v}_1 = \mathbf{v}$ is a chain of generalized eigenvectors with $(T-\lambda I)^k(\mathbf{v}) = \mathbf{0}$. You may notice that we are writing our chains backwards from our previous convention. Also, for convenience let $\mathbf{v}_0 = \mathbf{0}$. Notice that $(T-\lambda I)(\mathbf{v}_j) = \mathbf{v}_{j-1}$. Therefore, $T(\mathbf{v}_j) = \mathbf{v}_{j-1} + \lambda\mathbf{v}_j$. Thus the $j$-th column of our block will have a 1 in the $(j-1)$-st row and a$\lambda$ in its $j$-th row – unless we are looking at the very first column where: $T(\mathbf{v}_1) = \lambda\mathbf{v}_1 + \mathbf{v}_0 = \lambda\mathbf{v}_1$ so the first column is just a $\lambda$ followed by zeros. We get the following matrix:

$$J_\lambda = \begin{bmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & \cdots & 0 & 0 \\ 0 & 0 & \lambda & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda \end{bmatrix} = \begin{bmatrix} \lambda & 0 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 0 & \cdots & 0 & 0 \\ 0 & 0 & \lambda & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda & 0 \\ 0 & 0 & 0 & \cdots & 0 & \lambda \end{bmatrix} + \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{bmatrix} = \lambda I_k + N_k\,.$$

It is interesting to note that $(N_k)^k = 0$ so that $N_k$ is *nilpotent*. More precisely $(N_k)^{k-1} \neq 0$ but $(N_k)^k = 0$ so it is nilpotent of degree $k$. Obviously the diagonal part (i.e., $\lambda I$) and the nilpontent part of our Jordan block commute with each other. In general, if $\beta$ is a basis consisting of chains of generalized eigenvectors, we get

$$[T]_\beta^\beta = J = \begin{bmatrix} J_1 & 0 & \cdots & 0 \\ 0 & J_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_s \end{bmatrix}$$

where $J_1, J_2, \ldots, J_k$ are the Jordan blocks corresponding to our various chains of generalized eigenvectors. This is called a *Jordan form* for $T$. Notice that since each block can be written as a sum of a diagonal and nilpotent part, we can write $J = D + N$ where $D$ is diagonal and $N$ is nilpotent (its degree of nilpotency will be $k$ if the size of the largest Jordan block is $k \times k$). It isn't hard to show that the diagonal and nilpotent parts of $J$ commute: $DN = ND$. So while it is not always possible to diagonalize our linear operator, under the condition our characteristic polynomial splits, we can get close to diagonalizing. We are off by a nilpotent part and better yet, that part commutes with our diagonal part.

The question of whether Jordan form is unique is wrapped up with computing the Jordan form of a matrix. To determine the Jordan form we need to determine the number and length of our chains associated with each eigenvalue. Notice that each chain starts with an eigenvector. Thus $\dim(E_\lambda) = \dim\big(\mathrm{Ker}(T-\lambda I)\big)$ is equal to the number of chains associated with $\lambda$. More generally, let $n_k = \dim\big(\mathrm{Ker}(T-\lambda I)^k\big)$. Let us call $\mathbf{v}$ such that $(T-\lambda I)^k(\mathbf{v}) = \mathbf{0}$ but $(T-\lambda I)^{k-1}(\mathbf{v}) \neq \mathbf{0}$ a generalized eigenvector of degree $k$ (so eigenvectors have degree 1 and the zero vector has degree 0). Then $n_0 = 0$, $n_1$ is the number of independent eigenvectors, $n_2$ is the number of independent eigenvectors plus generalized eigenvectors of degree 2. In general, $n_k$ is the number of linearly independent eigenvectors of degree at most $k$. Notice that a $k$-chain is made up from one generalized eigenvector of each degree from 1 up to $k$. Thus the numbers $n_1, n_2, \ldots$ will let us determine how many chains we have (and how long they are). In particular, these numbers completely determine our Jordan block structure associated with $\lambda$. Putting this together, we have that our Jordan form is uniquely determined up to rearraging the order of our Jordan blocks.

**Example 2.41.** Consider $B = \begin{bmatrix} 2 & -1 & -1 & 0 & -1 \\ 7 & 7 & 2 & 1 & 3 \\ -4 & -2 & 2 & 0 & -2 \\ 2 & 1 & 1 & 4 & 1 \\ 1 & 1 & 2 & -1 & 5 \end{bmatrix}$. We can use software to find that $\det(tI - B) = (t-4)^5$.

Therefore, the only eigenvalue of $B$ is $\lambda = 4$. Next, we compute the nullity of powers of $B - 4I$: $n_0 = 0$, $n_1 = \text{Nullity}(B-4I) = 3$, $n_2 = \text{Nullity}(B-4I)^2 = 4$, $n_3 = \text{Nullity}(B-4I)^3 = 5$, $n_4 = \text{Nullity}(B-4I)^2 = 5$ (in fact, $n_k = 5$ for all $k \geq 3$). This means we have 3 chains of generalized eigenvectors. But only one of them is longer than 1 vector long. This chain then also extends to length 3. So we have two 1-chains and one 3-chain. Therefore, the Jordan form of $B$ is $J = \begin{bmatrix} 4 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 4 & 1 & 0 \\ 0 & 0 & 0 & 4 & 1 \\ 0 & 0 & 0 & 0 & 4 \end{bmatrix}$.

The task of finding a matrix $P$ such that $P^{-1}BP = J$ is considerbly more difficult. This amounts to actually finding our chains of generalized eigenvectors. We simply find one chain at a time and then when finding a new chain, make sure it is independent from the previously found ones. We start with our longest chain. We need a vector $\mathbf{v}_1$ such that $(B-4I)^3\mathbf{v}_1 = \mathbf{0}$ but $(B-4I)^2\mathbf{v}_1 \neq \mathbf{0}$. This is easy since $(B-4I)^3$ is the zero matrix. Examining $(B-4I)^2$, we see that $\mathbf{v}_3 = [1\ 0\ 0\ 0\ 0]^T$ will do the job. Then let $\mathbf{v}_2 = (B-4I)\mathbf{v}_3 = [-2\ 7\ -4\ 2\ 1]^T$ and $\mathbf{v}_1 = (B-4I)\mathbf{v}_2 = [0\ 4\ 0\ 0\ -4]^T$. Our next longest chains are the only remaining chains (of length 1). To find these we need to find vectors such that $(B-4I)\mathbf{x} = \mathbf{0}$ but $(B-4I)^0\mathbf{x} = \mathbf{x} \neq \mathbf{0}$ and they must be independent from our other vector at this level (i.e., independent from $\mathbf{v}_1$). Thus we find a basis for $\text{Ker}(B-4I)$ and then extend $\{\mathbf{v}_1\}$ (a linearly indpendent set) to a basis. The extension part is gives us our missing vectors. We find that $\mathbf{u}_1 = [1\ -3\ 1\ 0\ 0]^T$, $\mathbf{w}_1 = [-1\ 2\ 0\ 1\ 0]^T$, and a multiple of $\mathbf{v}_1$ form a basis for $\text{Ker}(B-4I)$. Thus the first two vectors are our desired extension. Therefore: $\{\mathbf{u}_1, \mathbf{w}_1, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ is our basis of chains of generalized eigenvectors. Thus letting $P = \begin{bmatrix} 1 & -1 & 0 & -2 & 1 \\ -3 & 2 & 4 & 7 & 0 \\ 1 & 0 & 0 & -4 & 0 \\ 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & -4 & 1 & 0 \end{bmatrix}$, we find that $P^{-1}BP = J$ (since we organized our chains so they had length 1, length 1, then length 3).

Since finding the Jordan form of a matrix is relatively easy, but finding the change of basis matrix is hard, we will pass this task off to software. In Maple, after loading the linear algebra package (i.e., `with(LinearAlgebra):`) and defining your matrix (e.g. `A`), you can find a transition matrix with the command `P := JordanForm(A,output='Q');`. Then `J := P^(-1).A.P;` will be your Jordan form.

Finding $P$ – An Algorithm:

(I) Compute the characteristic polynomial and determine all eigenvalues, $\lambda$, and their algebraic multiplicities, $a$.

(II) For each eigenvalue $\lambda$:

(1) Compute the nullity of $\text{Ker}(T-\lambda I)^k$ (call it $n_k$) for $k = 1, 2, \ldots$ until $n_k = n_{k+1}$ (this must happen by $n_a$). The last number in this list is $\dim(K_\lambda)$. Use these numbers to determine the number of and length of each chain of generalized eigenvectors.

(2) Let $W = \text{span}(\text{previously found basis vectors})$ (initially $W = \{\mathbf{0}\}$).

(3) Determine the largest positive integer $k$ such that $\text{Ker}(T-\lambda I)^{k-1}+W$ is properly contained in $\text{Ker}(T-\lambda I)^k$.

(4) Pick some $\mathbf{v} \in \text{Ker}(T-\lambda I)^k$ such that $\mathbf{v} \notin \text{Ker}(T-\lambda I)^{k-1} + W$.

(5) Add $(T-\lambda I)^{k-1}(\mathbf{v}), (T-\lambda I)^{k-2}(\mathbf{v}), \ldots, (T-\lambda I)(\mathbf{v}), \mathbf{v}$ to your basis.

(6) If you have not found $\dim(K_\lambda)$ vectors, go back to (2).

(III) Assemble the (coordinate representations) of each basis vector found for each generalized eigenspace in some order (making sure to keep chains together and in the order listed in (5)) into your matrix $P$.

This leaves many questions. One big one might be, "Why do we care?" In the end, having a standard form is incredibly useful. If you want to test a theorem about linear operators, you most likely just need to think about how

it works in the case your matrix is in Jordan form. For example, we already know that $\det(A)$ is the product of the eigenvalues of $A$ (counting multiplicity) and $\mathrm{tr}(A)$ is the sum. This is obvious from the Jordan form. Notice that the number of Jordan blocks counts the number of linearly independent eigenvectors. Our matrix is diagonalizable if and only if all of our Jordan blocks are $1 \times 1$.

If we let $f(t) = \det(tI - A)$ (i.e., the characteristic polynomial of $A$), then the Cayley-Hamilton Theorem states that $f(A) = 0$ (you cannot just plug $t = A$ into the definition to prove this – why?). Thus $A$ is a root of a polynomial of degree $n$ (given $A$ is $n \times n$). One might ask what the minimum degree polynomial might be. The *minimal polynomial* for $A$ is the monic (=leading coefficient is 1) polynomial $m(t)$ such that $m(A) = 0$ and $A$ is not the root of any lower degree polynomial. It isn't hard to see from the Jordan form of $A$, if the size of the largest Jordan block associated with $\lambda_i$ is $m_i \times m_i$ (for each eigenvalue $\lambda_i$), then $m(t) = (t - \lambda_1)^{m_1} \cdots (t - \lambda_\ell)^{m_\ell}$. Not only does this imply that the minimal polynomial divides the characteristic polynomial, but it also reveal the theorem: $A$ is diagonalizable if and only if its minimal polynomial has no repeated roots.

Finally, Jordan form is useful if one wants to define functions of matrices. Suppose you have a function $f(x)$ defined via a power series: $f(x) = c_0 + c_1 x + c_2 x^2 + \cdots = \sum_{k=0}^{\infty} c_k x^k$. Notice that if $A = PJP^{-1}$ then $A^k = (PJP^{-1}) \cdots (PJP^{-1}) = PJP^{-1}PJP^{-1} \cdots PJP^{-1} = PJ \cdots JP^{-1} = PJ^k P^{-1}$. Thus (excusing sum analytic/convergence type issues), $f(A) = \sum_{k=0}^{\infty} c_k A^k = \sum_{k=0}^{\infty} c_k P J^k P^{-1} = P \left( \sum_{k=0}^{\infty} c_k J^k \right) P^{-1} = Pf(J)P^{-1}$. Therefore, if you can sort out how to evaluate your function on a Jordan block, you can figure out how to evaluate it on any matrix.

In particular, $e^x = 1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + \cdots = \sum_{k=0}^{\infty} \frac{x^k}{k!}$. One can show that if $x$ and $y$ are commuting formal variables, then $e^{x+y} = e^x e^y$. Notice that $J = D + N$ where $D$ and $N$ are the diagonal and nilpotent parts of the Jordan form $J$. But $D$ and $N$ commute! Thus $e^J = e^{D+N} = e^D e^N$. Since computing powers of a diagonal matrix just amounts to computing powers of its diagonals, applying a function to a diagonal matrix just amounts to applying that function to its diagonals. Thus we can easily compute $e^D$. On the other hand, a high enough power of a nilpotent matrix is zero, so a power series $f(N)$ is actually a finite sum (a polynomial in $N$). Thus we can compute $e^N$. Therefore, we can effectively compute $e^A = Pe^J P^{-1} = Pe^D e^N P^{-1}$ (although there are easier ways to compute $e^A$.) Why it this useful? The answer is differential equations and much more.

# Chapter 3

# Differential Equations Applications

## 3.1 Variation of Parameters

Here we will explore how to solve linear differential equations using variation of parameters. This will be developed by considering an equivalent first order linear system of differential equations.

Recall that any system of differential equations can be converted into a first order system by giving names to all but the highest order derivatives and then replacing those derivatives with the first derivative of the new name for the next to highest order derivative. For example: Given $z''' + y'' = 0$ and $y'z = y^3$, let $x_1 = y$, $x_2 = y'$, $x_3 = z$, $x_4 = z'$, and $x_5 = z''$. Then our equivalent system is $x_1' = x_2$, $x_3' = x_4$, $x_4' = x_5$ (to encode the relations between variables) and $x_5' + x_2' = 0$, $x_1'x_3 = (x_1)^3$ (encoding the original equations).

Using this trick on an $n$-th order (homogeneous) linear differential equation will yield a system of $n$ first order (homogeneous) linear differential equations. In particular,

$$y^{(n)} + a_{n-1}(t)y^{(n-1)} + \cdots + a_2(t)y'' + a_1(t)y' + a_0(t)y = g(t) \tag{3.1}$$

becomes

$$\begin{bmatrix} x_1'(t) \\ x_2'(t) \\ \vdots \\ x_{n-2}'(t) \\ x_{n-1}'(t) \\ x_n'(t) \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -a_{n-1}(t) & -a_{n-2}(t) & -a_{n-3}(t) & \cdots & -a_1(t) & -a_0(t) \end{bmatrix} \begin{bmatrix} x_1(t) \\ x_2(t) \\ \vdots \\ x_{n-2}(t) \\ x_{n-1}(t) \\ x_n(t) \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ g(t) \end{bmatrix} \tag{3.2}$$

where $x_1 = y$, $x_2 = x_1'$ $(= y')$, $x_3 = x_2'$ $(= y'')$, $\ldots$, $x_n = x_{n-1}'$ $(= y^{(n-1)})$. Briefly, we write $\mathbf{x}'(t) = A(t)\mathbf{x}(t) + \mathbf{g}(t)$.

Now let $\mathbf{x}'(t) = A(t)\mathbf{x}(t) + \mathbf{g}(t)$ be an arbitrary first order linear system (of $n$ equations). First, we need to solve the (homogeneous) companion equation $\mathbf{x}'(t) = A(t)\mathbf{x}(t)$. Unfortunately, this is impossible in general. However, in some cases we can write down potentially useful formula using the matrix exponential.

### Homogeneous Systems: The Matrix Exponential

First, consider two matrices $A$ and $B$ whose entries are functions in $t$ and whose product $AB$ is defined (i.e., the number of columns of $A$ matches the number of rows of $B$). The $(i,j)$-entry of $AB$ is $\sum_{k=1}^{n} a_{ik}b_{kj}$. Differentiating this an applying the product rule, we get $\sum_{k=1}^{n} a_{ik}'b_{kj} + \sum_{k=1}^{n} a_{ik}b_{kj}'$. In other words, the $(i,j)$-entry of $(AB)'$ is the $(i,j)$-entry of $A'B + AB'$. Thus $(AB)' = A'B + AB'$ so the product rule still holds for matrices.

Next, let $A$ be an $n \times n$ matrix. In addition suppose that $A$ commutes with its derivative $A'$ (we differentiate matrices one entry at a time just like vector valued functions in multivariable calculus). Notice that the derivative of $A^0 = I$ is 0 (since all of the entries are constant). Suppose for some positive integer $k$, we have $(A^k)' = kA^{k-1}A'$ (which equals $kA'A^{k-1}$ since $A$ and $A'$ commute). Then $(A^{k+1})' = (A^kA)' = (A^k)'A + A^kA' = kA^{k-1}A'A + A^kA' = kA^{k-1}AA' + A^kA' = (k+1)A^kA'$. Therefore, as long as $A$ and $A'$ commute, we have $(A^n)' = nA^{n-1}A' = nA'A^{n-1}$ for all positive integers $n$ (i.e., the power rule for non-negative integer powers).

Define $\exp(A) = \sum_{k=0}^{\infty} \frac{A^k}{k!} = I + A + \frac{A^2}{2} + \frac{A^3}{3!} + \cdots$. While we will skip over convergence concerns, just know that this matrix exponential converges for all complex matrices $A$ and does so in essentially the best possible way. Thus we can freely interchange limits and do all kinds of things that normally make analysts cringe. Suppose that $A$ is a matrix of functions and $A$ commutes with $A'$. Then $(\exp(A))' = \left(\sum_{k=0}^{\infty} \frac{A^k}{k!}\right)' = \sum_{k=0}^{\infty} \frac{(A^k)'}{k!} = \sum_{k=0}^{\infty} \frac{kA^{k-1}A'}{k!} = \sum_{k=1}^{\infty} \frac{A^{k-1}}{(k-1)!}A' = \sum_{\ell=0}^{\infty} \frac{A^\ell}{\ell!}A' = \exp(A)A'$ (and likewise also $= A'\exp(A)$).

The above calculation shows that, given $A(t)$ and $\int_{t_0}^{t} A(u)\,du$ commute, if we let $M(t) = \exp\left(\int_{t_0}^{t} A(u)\,du\right)$, then $M'(t) = A(t)M(t)$. In other words, each column of $M(t)$ is a solution of our companion equation $\mathbf{x}'(t) = A(t)\mathbf{x}(t)$. Moreover, $M(t_0) = \exp\left(\int_{t_0}^{t_0} A(u)\,du\right) = \exp(0) = I$ so that the $j$-th column of $M(t)$ solves the initial value problem $\mathbf{x}'(t) = A(t)\mathbf{x}(t)$ where $\mathbf{x}(t_0) = \mathbf{e}_j$ (the $j$-th standard unit vector). Also, if $\mathbf{x}(t) = M(t)\mathbf{x}_0$ , then we solve the initial value problem with initial condition $\mathbf{x}(t_0) = M(t_0)\mathbf{x}_0 = I\mathbf{x}_0 = \mathbf{x}_0$.

We note here that a (square) matrix whose columns are linearly independent solutions of $\mathbf{x}'(t) = A(t)\mathbf{x}(t)$ is called a *fundamental matrix* for that homogeneous system. It can be shown that when $A$ and $B$ commute, we have $\exp(A+B) = \exp(A)\exp(B)$. Thus since $A$ and $-A$ commute, we have $\exp(A)\exp(-A) = \exp(A-A) = \exp(0) = I$ and so $(\exp(A))^{-1} = \exp(-A)$. In particular, matrix exponentials are always invertible. Therefore, $M(t) = \exp\left(\int_{t_0}^{t} A(u)\,du\right)$ is a fundamental matrix for $\mathbf{x}'(t) = A(t)\mathbf{x}(t)$ (if we know that $A(t)$ and $\int_{t_0}^{t} A(u)\,du$ commute).

A note of interest, if $M(t)$ is any fundamental matrix for $\mathbf{x}'(t) = A(t)\mathbf{x}(t)$, then $B(t) = M(t)M(t_0)^{-1}$ is also a fundamental matrix but then $B(t_0) = M(t_0)M(t_0)^{-1} = I$. Thus, assuming $A(t)$ commutes with its antiderivative, $B(t)$ solves the same initial value problem as $\exp\left(\int_{t_0}^{t} A(u)\,du\right)$. Therefore, by the uniqueness part of the existence uniqueness theorem (of solutions of linear systems of differential equations), we must have that $M(t)M(t_0)^{-1} = \exp\left(\int_{t_0}^{t} A(u)\,du\right)$.

As a special case, when $A$ is constant, $\int_{t_0}^{t} A\,du = Au\Big|_{t_0}^{t} = A(t-t_0)$, so $M(t) = \exp(A(t-t_0))$ is a fundamental matrix for $\mathbf{x}'(t) = A\mathbf{x}(t)$. In this case, we can effectively compute the matrix exponential using the Jordan form (say $P^{-1}AP = J = D + N$, then $\exp(A(t-t_0)) = P\exp(D(t-t_0))\exp(N(t-t_0))P^{-1}$ and exponentiating diagonal and nilpotent matrices is easy).

As an even more special case, still supposing $A$ is constant, notice that if $\mathbf{x}(t) = e^{\lambda t}\mathbf{v}$ where $A\mathbf{v} = \lambda\mathbf{v}$, then $\mathbf{x}(t)$ solves our homogeneous system. This means that if we have $n$ linearly independent eigenvectors for $A$, we'll get $n$ linearly independent solutions of $\mathbf{x}'(t) = A\mathbf{x}(t)$. In other words, when $A$ is diagonalizable (this is the case considered in most undergraduate differential equations courses), then we can construct a fundamental matrix $M(t)$ whose columns are of the form $e^{\lambda t}\mathbf{v}$ where $\mathbf{v}$ is an eigenvector with eigenvalue $\lambda$. From our note of interest above, if $M(t)$ is such a fundamental matrix, then $M(t)M(t_0)^{-1} = \exp(A(t-t_0))$. So in some sense, the matrix exponential is sort of a normalized fundamental matrix.

## Non-Homogeneous Systems: Variation of Parameters

Suppose we begin with a fundamental matrix $M(t)$ for the companion equation $\mathbf{x}'(t) = A(t)\mathbf{x}(t)$ related to our system $\mathbf{x}'(t) = A(t)\mathbf{x}(t) + \mathbf{g}(t)$. We know that $\mathbf{x}(t) = M(t)\mathbf{c}$ (where $\mathbf{c}$ is an arbitrary constant vector) is a general solution of our companion equation. Thus if we replace $\mathbf{c}$ with a vector of non-constant functions $\mathbf{v}(t)$, we should get solutions for some non-homogeneous system. To that end suppose $\mathbf{x}(t) = M(t)\mathbf{v}(t)$ solves $\mathbf{x}'(t) = A(t)\mathbf{x}(t) + \mathbf{g}(t)$. Then $\mathbf{x}'(t) = (M(t)\mathbf{v}(t))' = M'(t)\mathbf{v}(t) + M(t)\mathbf{v}'(t)$, but $(M(t)\mathbf{v}(t))' = \mathbf{x}'(t) = A(t)\mathbf{x}(t) + \mathbf{g}(t) = A(t)M(t)\mathbf{v}(t) + \mathbf{g}(t)$. Taking into consideration that $M(t)$ is a fundamental matrix for the companion equation (so that $M'(t) = A(t)M(t)$), we have $A(t)M(t)\mathbf{v}(t) + M(t)\mathbf{v}'(t) = A(t)M(t)\mathbf{v}(t) + \mathbf{g}(t)$. Thus $M(t)\mathbf{v}'(t) = \mathbf{g}(t)$ and since $M(t)$ is invertible: $\mathbf{v}'(t) = M(t)^{-1}\mathbf{g}(t)$.

Therefore, letting $\mathbf{v}(t) = \displaystyle\int_{t_0}^{t} M(u)^{-1}\mathbf{g}(u)\,du$, we have that $\mathbf{x}(t) = M(t)\mathbf{v}(t) = M(t)\displaystyle\int_{t_0}^{t} M(u)^{-1}\mathbf{g}(u)\,du$ is a solution of our non-homogeneous system. Moreover, letting $\mathbf{x}(t) = M(t)\mathbf{v}(t) = M(t)\left(\displaystyle\int_{t_0}^{t} M(u)^{-1}\mathbf{g}(u)\,du + \mathbf{c}\right)$ (i.e., adding in a general solution of the companion equation: $M(t)\mathbf{c}$), we get a general solution of our system. Also, noting that $\mathbf{x}(t_0) = M(t_0)\left(\displaystyle\int_{t_0}^{t_0} M(u)^{-1}\mathbf{g}(u)\,du + \mathbf{c}\right) = M(t_0)\mathbf{c}$, we have that $\mathbf{x}(t) = M(t)\left(\displaystyle\int_{t_0}^{t} M(u)^{-1}\mathbf{g}(u)\,du + M(t_0)^{-1}\mathbf{x}_0\right)$ is the solution of the initial value problem $\mathbf{x}'(t) = A(t)\mathbf{x}(t) + \mathbf{g}(t)$ with $\mathbf{x}(t_0) = \mathbf{x}_0$. Thus if we can solve the companion problem, then we can effectively solve the non-homogeneous problem too.

As a special case, notice that when $A(t)$ commutes with its derivative, we can let $M(t) = \exp\left(\displaystyle\int_{t_0}^{t} A(u)\,du\right)$ and so $M(t)^{-1} = \exp\left(-\displaystyle\int_{t_0}^{t} A(u)\,du\right)$. Thus $\mathbf{x}(t) = \exp\left(\displaystyle\int_{t_0}^{t} A(u)\,du\right)\left(\displaystyle\int_{t_0}^{t} \exp\left(-\int_{t_0}^{w} A(u)\,du\right)\mathbf{g}(w)\,dw + \mathbf{x}_0\right)$ solves the initial value problem $\mathbf{x}'(t) = A(t)\mathbf{x}(t) + \mathbf{g}(t)$ with $\mathbf{x}(t_0) = \mathbf{x}_0$. This is the exact same formula as our solution for a single first order linear equation (the exponential of the integral of $A(t)$ is our integrating factor).

## Cramer's Rule, Matrix Inverses, and the Wronskian

Before we get back our original problem of solving $n$-th order linear differential equations, we take care of a computational issue: How do we invert a matrix – especially if its entries are functions? One possible answer is Cramer's Rule. This formula allows one to explicitly solve linear systems when the coefficient matrix is invertible.

Consider a linear system $A\mathbf{x} = \mathbf{b}$ where $A$ is a square matrix. Let $A = [\ \mathbf{a}_1\ \mathbf{a}_2\ \cdots\ \mathbf{a}_n\ ]$ where $\mathbf{a}_j$ is the $j$-th column of $A$. Also, let $A_j = [\ \mathbf{a}_1\ \cdots\ \mathbf{a}_{j-1}\ \mathbf{b}\ \mathbf{a}_{j+1}\ \cdots\ \mathbf{a}_n\ ]$ be the matrix $A$ with its $j$-th column replaced by $\mathbf{b}$. Also, let $\mathbf{x} = [x_1\ x_2\ \cdots\ x_n]^T$ be a solution of our linear system. Then $\mathbf{a}_1x_1 + \cdots + \mathbf{a}_nx_n = A\mathbf{x} = \mathbf{b}$.

Next, let's take a determinant:

$$\begin{aligned}\det A_j = \det[\ \mathbf{a}_1\ \cdots\ \mathbf{a}_{j-1}\ \mathbf{b}\ \mathbf{a}_{j+1}\ \cdots\ \mathbf{a}_n\ ] &= \det\left[\ \mathbf{a}_1\ \cdots\ \mathbf{a}_{j-1}\ \sum_{k=1}^{n} x_k\mathbf{a}_k\ \mathbf{a}_{j+1}\ \cdots\ \mathbf{a}_n\ \right] \\ &= \sum_{k=1}^{n} x_k \det[\ \mathbf{a}_1\ \cdots\ \mathbf{a}_{j-1}\ \mathbf{a}_k\ \mathbf{a}_{j+1}\ \cdots\ \mathbf{a}_n\ ]\end{aligned}$$

where we can take the sum out because determinants are multilinear in their columns. Now determinants are not just multilinear but also alternating in their columns. This means that if a column is repeated, the determinant is zero. Therefore, the only determinant in our sum above that survives is the one where $k = j$ (so we don't have a repeated column). Therefore, $\det A_j = x_j \det[\ \mathbf{a}_1\ \cdots\ \mathbf{a}_{j-1}\ \mathbf{a}_j\ \mathbf{a}_{j+1}\ \cdots\ \mathbf{a}_n\ ] = x_j \det A$. Thus, if $\det A$ is invertible, we have that $\mathbf{x} = [x_1\ x_2\ \cdots\ x_n]^T$ solves $A\mathbf{x} = \mathbf{b}$ if we let $x_i = \dfrac{\det A_j}{\det A}$ for each $i = 1, \ldots, n$. This is Cramer's Rule.

**Example 3.1.** Suppose we have a system $ax + by = p$ and $cx + dy = q$ where this system has a unqiue solution.

Then Cramer tells us that $x = \dfrac{\det\begin{bmatrix} p & b \\ q & d \end{bmatrix}}{\det\begin{bmatrix} a & b \\ c & d \end{bmatrix}} = \dfrac{pd-bq}{ad-bc}$ and $y = \dfrac{\det\begin{bmatrix} a & p \\ c & q \end{bmatrix}}{\det\begin{bmatrix} a & b \\ c & d \end{bmatrix}} = \dfrac{aq-cp}{ad-bc}$.

Notice that if $\mathbf{e}_i$ is the $i$-th standard unit vector (i.e., the $i$-th column of the identity matrix), then solving $A\mathbf{x} = \mathbf{e}_i$ we have $\mathbf{x}$'s $j$-th entry must satisfy the equation, $\det A_j = x_j \det A$. Notice here that $A_j = [\ \mathbf{a}_1\ \cdots\ \mathbf{a}_{j-1}\ \mathbf{e}_i\ \mathbf{a}_{j+1}\ \cdots\ \mathbf{a}_n\ ]$. The determinant of this matrix could be computed by expanding down the $j$-th column. We would sum a bunch of zeros until we got to row $i$ (where $\mathbf{e}_i$ has the non-zero entry 1) and get $(-1)^{i+j}$ times the subdeterminant obtained by deleting row $i$ and column $j$. In other words, if we let $A_{ij}$ be the matrix $A$ with row $i$ and column $j$ struck out, then this determinant is nothing more than $(-1)^{i+j}\det A_{ij}$. Therefore, a solution of $A\mathbf{x} = \mathbf{e}_i$ will have an $j$-th entry satisfying $(-1)^{i+1}\det A_{ij} = x_j \det A$.

Create a square matrix $C$ and let its $(i,j)$-entry be $c_{ij} = (-1)^{i+1}\det A_{ij}$. Then the $i$-th row of $C$ is $\det A$ times a solution of $A\mathbf{x} = \mathbf{e}_i$. This implies that $AC^T = (\det A)I$. Similarly, $C^T A = (\det A)I$. The matrix $C^T$ is called the *classical adjoint transpose*. If $\det A$ is invertible, we have $A^{-1} = \dfrac{1}{\det A}C^T$. This gives us an explicit formula for the inverse of a matrix. We can compute it using additions, subtractions, multiplications of the entries of $A$ followed by a single division (by the determinant of $A$).

Heading back to the problem of solving an $n$-th order linear equation, let $y_1, \ldots, y_n$ be a fundamental solution set for the companion equation of (3.1) (i.e., $y^{(n)} + a_{n-1}(t)y^{(n-1)} + \cdots + a_1(t)y' + a_0 y = 0$). These solutions correspond to solutions of the companion equations of (3.2) (i.e., $\mathbf{x}'(t) = A(t)\mathbf{x}(t)$). In fact, since $x_1 = y$, $x_2 = y'$, $\ldots x_n = y^{(n-1)}$, we have that our fundamental solution set corresponds to the fundamental matrix:

$$M(t) = \begin{bmatrix} y_1 & y_2 & \cdots & y_n \\ y_1' & y_2' & \cdots & y_n' \\ \vdots & \vdots & & \vdots \\ y_1^{(n-1)} & y_2^{(n-1)} & \cdots & y_n^{(n-1)} \end{bmatrix}. \tag{3.3}$$

Conversely, the top row of a fundamental matrix for $\mathbf{x}'(t) = A(t)\mathbf{x}(t)$ yields a fundamental solution set for the companion equation of our $n$-th order linear differential equation.

Consider actually implementing our variation of parameters formulas, we now know that the classical adjoint transpose (essential a bunch of determinants) can take a fundamental matrix and compute its inverse. However, let us focus on the case arising from an $n$-th order linear equation. Here we really aren't interested in the entire column vector $\mathbf{x}(t)$. Instead we really just want the first entry since $y = x_1$. To that end, we ask what is $\mathbf{v}' = M^{-1}\mathbf{g}$? Well, by Cramer's rule, the $i$-th entry of $\mathbf{v}'$ (i.e., of the solution of $M\mathbf{v}' = \mathbf{g}$) is nothing more than

$$v_i'(t) = \frac{\det\begin{bmatrix} y_1 & \cdots & y_{i-1} & 0 & y_{i+1} & \cdots & y_n \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ y_1^{(n-2)} & \cdots & y_{i-1}^{(n-2)} & 0 & y_{i+1}^{(n-2)} & \cdots & y_n^{(n-2)} \\ y_1^{(n-1)} & \cdots & y_{i-1}^{(n-1)} & g(t) & y_{i+1}^{(n-1)} & \cdots & y_n^{(n-1)} \end{bmatrix}}{\det M(t)} = \frac{(-1)^{i+n} g(t) \det M_{ni}(t)}{\det M(t)}$$

where $M_{ni}(t)$ is the matrix $M(t)$ with its $n$-th row and $i$-th column struck out. Notice $M_{ni}(t)$ is a matrix filled with $y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_n$ and their derivatives up to order $n-2$. This leads to a definition.

**Definition 3.2.** Let $z_1, \ldots, z_k$ be functions. Then

$$W[z_1, z_2, \ldots, z_k] = \det\begin{bmatrix} z_1 & z_2 & \cdots & z_k \\ z_1' & z_2' & \cdots & z_k' \\ \vdots & \vdots & & \vdots \\ z_1^{(k-1)} & z_2^{(k-1)} & \cdots & z_k^{(k-1)} \end{bmatrix}$$

is called the *Wronskian* of the functions $z_1, \ldots, z_k$. More precisely, Wronskian might refer to the matrix and Wronskian determinant refer to its determinant.[1]

Using this new notation, after integrating, we have that

$$v_i(t) = \int_{t_0}^{t} \frac{(-1)^{i+n} g(u)\, W[y_1(u), \ldots, y_{i-1}(u), y_{i+1}(u), \ldots, y_n(u)]}{W[y_1(u), \ldots, y_n(u)]}\, du$$

Therefore, $y = v_1(t)y_1(t) + \cdots + v_n(t)y_n(t)$ is a solution of (3.1). Adding in a general solution of the companion equation yields a general solution of (3.1).

**Example 3.3.** Suppose we solved the companion equation of $y'' + a_1(t)y' + a_0(t)y = g(t)$ and found linearly independent solutions $y_1$ and $y_2$. Then $W[y_1, y_2] = \det \begin{bmatrix} y_1 & y_2 \\ y_1' & y_2' \end{bmatrix} = y_1y_2' - y_1'y_2$. Notice that $W[z] = z$. Therefore,

$$v_1(t) = \int_{t_0}^{t} \frac{(-1)^{1+2} g(u) W[y_2]}{W[y_1, y_2]}\, du = -\int_{t_0}^{t} \frac{g(u)y_2(u)}{y_1(u)y_2'(u) - y_1'(u)y_2(u)}\, du$$

and

$$v_2(t) = \int_{t_0}^{t} \frac{(-1)^{2+2} g(u) W[y_1]}{W[y_1, y_2]}\, du = \int_{t_0}^{t} \frac{g(u)y_1(u)}{y_1(u)y_2'(u) - y_1'(u)y_2(u)}\, du\,.$$

We have $y(t) = v_1(t)y_1(t) + v_2(t)y_2(t) + C_1y_1(t) + C_2y_2(t)$ is a general solution of our equation.

## Liouville's Formula

An interesting fact about the Wronskian of a fundamental solution set is that it is non-zero on its entire domain. First, we let $M(t)$ be a fundamental matrix for some homogeneous system $\mathbf{x}'(t) = A(t)\mathbf{x}$. Let $W = \det M(t)$. In the special case that our system came from an $n$-th order linear equation, we called $W$ the Wronskian of our solution set. We still call it a Wronskian in this more general setting.

Let $y_{ij}(t)$ be the $(i,j)$-entry in $M(t)$. Then $W = \det M(t) = \sum_{\sigma \in S_n} (-1)^\sigma y_{1\sigma(1)} \cdots y_{n\sigma(n)}$ where $S_n$ is the group of permutations on $n$ things and $(-1)^\sigma$ is the sign of the permutation $\sigma$ (i.e., it is 1 when $\sigma$ is even and $-1$ when odd). Take the derivative of $W$ and apply the product rule: $W' = \sum_{\sigma \in S_n} (-1)^\sigma (y_{1\sigma(1)} \cdots y_{n\sigma(n)})'$ $= \sum_{\sigma \in S_n} (-1)^\sigma y'_{1\sigma(1)} \cdots y_{n\sigma(n)} + \cdots + \sum_{\sigma \in S_n} (-1)^\sigma y_{1\sigma(1)} \cdots y'_{n\sigma(n)}$ (we are successively differentiating each row). Let $M_i$ denote $M$ with the $i$-th row replaced by its determinants (so that $W' = \det M_1 + \cdots + \det M_n$).

Fix some $i$ and focus on $M_i$. Notice that $M_i$'s entries are $y_{kj}$ $(k \neq i)$ and $y'_{ij}$ for any $j$. Now $M(t)$ is a fundamental matrix so that $M'(t) = A(t)M(t)$. This implies $y'_{ij} = \sum_{k=1}^{n} a_{ik}(t)y_{kj}$ for any $j$. If we add $-a_{ik}$ times row $k$ to row $i$ for all $k \neq i$, the resulting matrix's $(i,j)$-entry would be $y'_{ij} - \sum_{k=1,\ldots,i-1,i+1,\ldots,n} a_{ik}(t)y_{kj} = a_{ii}y_{ij}$ (for any $j$). In other words, by adding multiples of various rows to row $i$, we obtain a matrix identical to $M$ except its $i$-th row is scaled by $a_{ii}$. Therefore, since adding multiples of rows to other rows does not change determinants and scaling a row just scales the determinant, we have $\det M_i = a_{ii} \det M$.

We have now shown that $W' = \det M_1 + \cdots + \det M_n = a_{11} \det M + \cdots + a_{nn} \det M = (a_{11} + \cdots + a_{nn}) \det M = \operatorname{tr}(A)\, W$. This is a first order (and actually separable) linear differential equation. We solve and get $W = Ce^{\int \operatorname{tr}(A(t))}$. Or more precisely, $W(t) = W(t_0) \exp\left( \int_{t_0}^{t} \operatorname{tr}(A(u))\, du \right)$. Since $M(t)$ is a fundamental matrix, its columns are linearly independent. Also note that $M(t_0)$ is invertible so that $W(t_0) = \det M(t_0)$ is non-zero.

[1] This is the same abuse of language as is commonplace when dealing with Jacobians.

When our system comes from an $n$-th order linear differential equation, this formula takes on a special form and is called *Abel's formula*. Notice that the trace of the coefficient matrix $A(t)$ in (3.2) is $0 + \cdots + 0 - a_0(t) = -a_0(t)$. Therefore, for a fundamental solution set $y_1, \ldots, y_n$, we have $W[y_1, \ldots, y_n] = W[y_1, \ldots, y_n](t_0) \cdot \exp\left(\int_{t_0}^{t} -a_0(u)\, du\right)$.

# Chapter 4

# Extra Algebra

## 4.1 Elementary Functions and Liouville's Theorem

**Definition 4.1.** Let $R$ be a commutative ring with 1. We call a map $\partial : R \to R$ a *derivation* if $\partial(a+b) = \partial(a)+\partial(b)$ and $\partial(ab) = \partial(a)b + a\partial(b)$ for all $a, b \in R$. A ring equipped with a particular derivative is called a *differential ring*. For convenience, we write $\partial(a) = a'$ (just like in calculus). If $R$ is a differential ring and an integral domain, it is a *differential integral domain*. If $R$ is a differential ring and a field, it is a *differential field*.

Let $R$ be a differential ring.

- $\diamond$ $1' = (1\cdot 1)' = 1'\cdot 1 + 1\cdot 1'$ so $1' = 1'+1'$ and so $0 = 1'$. Notice that $\partial$ is a group homomorphism (consider $R$ as an abelian group under addition), so $\partial(na) = n\partial(a)$ for all $a \in R$ and $n \in \mathbb{Z}$. Therefore, $\partial(n1) = n\partial(1) = n0 = 0$. Thus everything in the prime subring is a *constant* (i.e. has derivative zero).
- $\diamond$ Given $a \in R$, notice that $(a^2)' = (a \cdot a)' = a'a + aa' = 2aa'$. In fact, we can prove (using induction), that

$$a^n = na^{n-1}a' \text{ for any } n \in \mathbb{Z}_{\geq 0} \qquad \text{(The power rule)}$$

- $\diamond$ Let $a \in R^\times$ ($a$ is a unit). Then $0 = 1' = (aa^{-1})' = a'a^{-1} + a(a^{-1})'$ so $a(a^{-1})' = -a^{-1}a'$. Dividing by $a$, we get that $(a^{-1})' = -a^{-2}a'$. Again, using induction, we have that $a^n = na^{n-1}$ for all $n \in \mathbb{Z}$ (if $a^{-1}$ exists).
- $\diamond$ Let $a \in R$ and $b \in R^\times$. Then $(ab^{-1})' = a'b^{-1} + a(b^{-1})' = a'b^{-1} + a(-b^{-2}b')$. Therefore,

$$\partial\left(\frac{a}{b}\right) = \frac{a'b - ab'}{b^2} \qquad \text{(The quotient rule)}$$

This then implies that if $\mathbb{Q} \subseteq R$, every element of $\mathbb{Q}$ is a constant.

*Note.* If $R$ is a differential integral domain, then $R$'s field of fractions $\mathbb{F}$ can be turned into a differential field in a unique way. We define $\partial(a/b)$ via the quotient rule. It is a simple exercise to show that this is well defined, extends the definition of $\partial$ from $R$ to $\mathbb{F}$, and there is no other way to do this.

**Definition 4.2.** A *differential subring* of a differential ring $R$, is a subring (containing 1) which is closed under differentiation. Thus $S \subseteq R$ is a differential subring if $1 \in S$, $a, b \in S$ implies that $a - b, ab \in S$ and $a \in S$ implies that $a' \in S$.

Likewise, a *differential ideal* of $R$ is an ideal that is closed under differentiation. If $I$ is a differential ideal of $R$, $R/I$ becomes a differential ring if we define $\partial(a + I) = \partial(a) + I$ (it's easy to show that this is well defined).

A *differential homomorphism* between two differential rings $R, S$ is a map $\varphi : R \to S$ which is a ring homomorphism (i.e. $\varphi(a+b) = \varphi(a)+\varphi(b)$, $\varphi(ab) = \varphi(a)\varphi(b)$, and $\varphi(1) = 1$) that preserves differentiation (i.e. $\varphi(a') = \varphi(a)'$). It's easy to show that the kernel of a differential homomorphism, $\ker(\varphi) = \{x \in R \mid \varphi(x) = 0\}$, is a differential ideal of the domain. Also, the image is a differential subring of the codomain and the isomorphism theorems all hold.

**Lemma 4.3.** *Let $R$ be a differential ring. $C = \ker(\partial) = \{x \in R \mid x' = 0\}$ is a differential subring of $R$ (call the constants of $R$). Moreover, if $R$ is a differential field, then $C$ is a (differential) field.*

*Proof.* First, $1 \in C$ since $1' = 0$. Next, suppose $a, b \in C$. Then $(a-b)' = a' - b' = 0 - 0 = 0$ and $(ab)' = a'b + ab' = 0b + a0 = 0$ so $a - b, ab \in C$. Finally, for all $a \in C$, $a' = 0 \in C$. So $C$ is a differential subring.

Suppose that $R$ is a field. Let $a \in C$ such that $a \neq 0$. Then $(a^{-1})' = -a^{-2}a' = -a^{-2}0 = 0$ so $a^{-1} \in C$. Thus $C$ is a field. □

**Example 4.4.** Any commutative ring with 1 is a differential ring when given the derivation $\partial = 0$. In particular, $\mathbb{Q}$ is a differential ring with $\partial = 0$ and by some of the above discussion, this is our only choice!

The field of rational functions with real coefficients, $\mathbb{R}(x)$, is a differential field when given $\partial = \dfrac{d}{dx}$ (the usual derivative). Here the field of constants is $\mathbb{R}$ (as we would expect).

It is interesting (and strange) to consider that $\mathbb{Q}(\pi)$ (which is isomorphic to $\mathbb{Q}(x)$) is a differential field when given the derivation $\partial =$ "$d/d\pi$". In other words, $\pi' = 1$ and $(\pi^3)' = 3\pi^2$ etc. This indicates that $\mathbb{R}$ can be turned into a differential field in many very strange ways.

**Lemma 4.5.** *Let $\mathbb{F}$ be a differential field of characteristic 0 and let $\mathbb{K}/\mathbb{F}$ be an algebraic extension (as regular old fields). The derivation on $\mathbb{F}$ can be extended to a derivative on $\mathbb{K}$ in exactly one way (i.e. $\mathbb{K}$ can be turned into a differential field and this can only be done in one way).*

*Proof.* [Sketch] I'll just show uniqueness. For a complete proof see [Crespo & Hajto] Proposition 5.3.1.

Let $\alpha \in \mathbb{K}$ and let $f(x) \in \mathbb{F}[x]$ be the minimal polynomial for $\alpha$ over $\mathbb{F}$ (every element in an algebraic extension is *by definition* algebraic). Let $Df(x)$ be the formal derivative of our polynomial $f(x)$ (treating the coefficients like constants). Then $f(x)$ and $Df(x)$ are relatively prime ($f(x)$ is irreducible and $Df(x)$ has lower degree and is non-zero since $\mathbb{F}$ has characteristic 0). This means that $Df(\alpha) \neq 0$.

Consider $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Then $(f(x))' = nx^{n-1}x' + (a'_{n-1}x^{n-1} + (n-1)a_{n-1}x^{n-2}x') + \cdots + (a'_1x + a_1x') + a'_0$. Therefore, $(f(x))' = Df(x)x' + g(x)$ where $g(x) = a'_{n-1}x^{n-1} + \cdots + a'_1x + a'_0$. Now $\alpha$ is the root of $f(x)$, so we must have $(f(\alpha))' = 0$. In other words, $0 = Df(\alpha)\alpha' + g(\alpha)$. So the only consistent way to define $\alpha'$ is $\dfrac{g(\alpha)}{Df(\alpha)}$. □

**Example 4.6.** We know that the only derivation on $\mathbb{Q}$ is zero. Consider $\sqrt{5} \in \mathbb{Q}[\sqrt{5}]$. As in the above proof, we can figure out what the derivative of $\sqrt{5}$ must be from its minimal polynomial. $(\sqrt{5})^2 - 5 = 0$ so $2(\sqrt{5})(\sqrt{5})' - 0 = 0$ and thus $(\sqrt{5})' = 0/(2\sqrt{5}) = 0$ (as we might have guessed).

**Definition 4.7.** Let $\mathbb{F}$ be a differential field. We call $\mathbb{F}(t)/\mathbb{F}$ a *logarithmic* extension if there exists some $s \in \mathbb{F}$ such that $t' = \dfrac{s'}{s}$. Similarly we call $\mathbb{F}(t)/\mathbb{F}$ an *exponential* extension if there exists some $s \in \mathbb{F}$ such that $t' = ts'$.

These definitions mimic the defining properties of the natural logarithm and the exponential function. Suppose that $t' = \dfrac{s'}{s}$ and we could "integrate". Then $t = \int t' = \ln(s)$. Likewise, solving the "differential equation" $t' = ts'$ yields $t = e^s$. The above definitions yield formal characterizations of these functions without requiring us to work with actual fields of functions (or real or complex variables).

**Definition 4.8.** Let $\mathbb{F}$ be a differential field with field of constants $C$ ($= \ker(\partial)$). A differential field extension $\mathbb{E}/\mathbb{F}$ is an *elementary* extension if there exists a tower of differential fields

$$\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \cdots \subseteq \mathbb{F}_\ell = \mathbb{E}$$

where all $\mathbb{F}_j$ have the same field of constants and each extension $\mathbb{F}_{j+1}/\mathbb{F}_j$ is each an algebraic, logarithmic, or exponential extension.

If $\mathbb{F} = \mathbb{C}(x)$ (thought of as actual rational functions in a single complex variable), then $\mathcal{E}$ is defined to be the collection of all complex functions which lie in some elementary extension of $\mathbb{C}(x)$ (we allow these functions to have domains which aren't all of $\mathbb{C}$). $\mathcal{E}$ is the field of elementary functions.

**Example 4.9.** Essentially elementary functions are the functions that can be built from $\mathbb{C}$ and $f(x) = x$ using algebra, exponentiation, and taking logarithms. For example: $f(x) = \sqrt{\dfrac{e^{\sqrt[3]{x^5+1}} - 7}{\ln(x^{15} + \sqrt{x^4 - 1}) + \ln(e^{1/x} - 6)}}$ is an elementary function.

Keep in mind that elementary functions also include some functions which may be unfamiliar to us. For example: The Bring radical is $\mathrm{BR}(a)$ is the unique real root of the polynomial $x^5 + x + a$ (then extend $\mathrm{BR}(a)$ analytically to a function of a complex variable). Because $Y = \mathrm{BR}(x)$ is a root of the equation $Y^5 + Y + x = 0$, we have that $\mathbb{C}(x)(\mathrm{BR}(x))$ is an elementary extension of $\mathbb{C}(x)$ and so $\mathrm{BR}(x)$ is an elementary function. By the way, for $Y = \mathrm{BR}(x)$, $0 = (Y^5 + Y + x)' = 5Y^4Y' + Y' + 1$ so $Y' = -\dfrac{1}{5Y^4 + 1}$. Thus $\mathrm{BR}'(x) = -\dfrac{1}{5 \cdot \mathrm{BR}(x)^4 + 1}$.

**Example 4.10.** What about trigonometric functions? The trig functions can be built from log's and exponential's. For example: $\sin(x) = \dfrac{e^{ix} - e^{-ix}}{2i}$ and $\cos(x) = \dfrac{e^{ix} + e^{-ix}}{2}$. Then $\tan(x)$, $\sec(x)$, $\csc(x)$, and $\cot(x)$ can be built from sine and cosine. Inverse trig functions? For example: $\arcsin(x) = -i\ln(ix + \sqrt{1 - x^2})$, $\arccos(x) = -i\ln(x + \sqrt{x^2 - 1})$, and $\arctan(x) = \dfrac{i}{2}(\ln(1 - ix) - \ln(1 + ix))$. The other inverse functions have similar looking formulas.

This means that functions like $f(x) = e^{\tan(\sqrt{x})}\ln(\sin(x) + \sec^5(e^{\sqrt{x}}))$ are elementary.

Now let's prove Liouville's theorem which characterizes which functions live in an elementary extension. We will follow the proof as presented in [Rosenlicht].

**Lemma 4.11.** *Let $\mathbb{F}$ be a differential field with differential field extension $\mathbb{F}(t)$. Suppose that $\mathbb{F}(t)$ and $\mathbb{F}$ have the same constants (i.e. the kernels of the derivations match) and that $t$ is transcendental over $\mathbb{F}$.*

- ◇ *Let $t' \in \mathbb{F}$ and $f(t) \in \mathbb{F}[t]$ with $\deg(f(t)) > 0$. Then $(f(t))' \in \mathbb{F}[t]$ and $\deg(f(t)) = \deg((f(t))')$ if and only if the leading coefficient of $f(t)$ is non-constant. If the leading coefficient of $f(t)$ is constant, then $\deg((f(t))') = \deg(f(t)) - 1$.*
- ◇ *Let $t'/t \in \mathbb{F}$. Then for all $a \in \mathbb{F}^\times$, $n \in \mathbb{Z}_{\neq 0}$, $(at^n)' = ht^n$ for some $h \in \mathbb{F}^\times$. Moreover, if $f(t) \in \mathbb{F}[t]$ with $\deg(f(t)) > 0$, then $\deg(f(t)) = \deg((f(t))')$. Also, $(f(t))' = cf(t)$ for some $c \in \mathbb{F} \iff f(t)$ is a monomial.*

*Proof.* Let $f(t) = a_nt^n + a_{n-1}t^{n-1} + \cdots + a_0 \in \mathbb{F}[t]$ with $a_n \neq 0$ so that $\deg(f(t)) = n > 0$.

For item 1, $(f(t))' = a_n't^n + (na_nt' + a_{n-1}')t^{n-1} + ((n-1)a_{n-1}t' + a_{n-2}')t^{n-2} + \cdots + (a_1t' + a_0')$. Notice that the coefficients all lie in $\mathbb{F}$ since we have assumed $t' \in \mathbb{F}$ (if $a_j \in \mathbb{F}$, then $a_j' \in \mathbb{F}$ because $\mathbb{F}$ is a differential field).

Recall that $a_n$ is non-constant $\iff$ $a_n' \neq 0$ (by definition). Thus the degree does not drop if and only if the leading coefficient is not constant. In the case that it is, we have $a_n' = 0$. Suppose that $(na_nt' + a_{n-1}') = 0$ (i.e. the coefficient of $t^{n-1}$ is zero). This implies that $(na_nt + a_{n-1})' = na_n't + na_nt' + a_{n-1}' = na_nt' + a_{n-1}' = 0$ (we are assuming $a_n' = 0$). Therefore, $na_nt + a_{n-1} = c$ for some constant $c \in \mathbb{F}$. Since $na_n \neq 0$ and $na_n, a_{n-1} \in \mathbb{F}$, we have shown that $t$ is algebraic over $\mathbb{F}$ (contradicting our hypothesis that $t$ is transcendental over $\mathbb{F}$). Thus $(na_nt' + a_{n-1}') \neq 0$ and so the degree of $(f(t))'$ is $n - 1$.

For item 2, let $t'/t = b \in \mathbb{F}$. Let $a \in \mathbb{F}^\times$. Then $(at^n)' = a't^n + nat^{n-1}t' = (a' + nab)t^n$ since $t' = bt$. If $a' + nab = 0$, then $at^n$ would be constant. So $t$ would satisfy the polynomial $aX^n + c$ for the constant $c = -at^n$. Since $a \neq 0$ and $a, c \in \mathbb{F}$, this would mean that $t$ is algebraic over $\mathbb{F}$ (again, a contradiction). Therefore, $a' + nab \neq 0$ (i.e. $(at^n)' = ht^n$ where $h = a' + nab \in \mathbb{F}^\times$).

Notice that our calculation above shows that each non-zero term of $f(t)$ yields a non-zero term (of the same degree) in $(f(t))'$. Thus $\deg(f(t)) = \deg((f(t))')$. Also, if $f(t)$ is a non-zero monomial, say $f(t) = at^n$, the above calculation says that $(at^n)' = ht^n$ so $(f(t))' = cf(t)$ where $c = h/a \in \mathbb{F}^\times$.

Conversely, suppose that $(f(t))' = cf(t)$ for some $c \in \mathbb{F}$. Then the above calculations say that $c = h/a_j = (a_j' + ja_jb)/a_j$ for all $a_j \neq 0$. Suppose that $a_m, a_\ell \neq 0$ (where $m \neq \ell$). Then $\dfrac{a_m' + ma_mb}{a_m} = \dfrac{a_\ell' + \ell a_\ell b}{a_\ell}$. That means $(a_\ell' + \ell a_\ell b)a_m = (a_m' + ma_mb)a_\ell$. Therefore, $\left(\dfrac{a_mt^m}{a_\ell t^\ell}\right)' = \dfrac{(a_m' + ma_mb)a_\ell t^{m+\ell} - (a_\ell' + \ell a_\ell b)a_mt^{m+\ell}}{a_\ell^2 t^{2\ell}} = 0$. Thus

$\frac{a_m t^m}{a_\ell t^\ell} = z$ for some constant $z \in \mathbb{F}$. Therefore, $a_m t^m - z a_\ell t^\ell = 0$ ($t$ satisfies a non-zero polynomial over $\mathbb{F}$). Thus we have $t$ is algebraic over $\mathbb{F}$ (again, a contradiction). Therefore, at most one coefficient is non-zero (i.e. $f(t)$ is a monomial). □

We can now give Liouville's theorem which characterizes which "functions" in $\mathbb{F}$ can be "integrated" in terms of elementary functions.

**Theorem 4.12** (Liouville)**.** *Let $\mathbb{F}$ be a differential field of characteristic 0. Let $\alpha \in \mathbb{F}$. If $y' = \alpha$ has a solution $y$ in an elementary extension of $\mathbb{F}$ (with the same constants), then there exists constants $c_1, \ldots, c_n$ and elements $u_1, \ldots, u_n, v \in \mathbb{F}$ such that*

$$\alpha = v' + c_1 \frac{u_1'}{u_1} + c_2 \frac{u_2'}{u_2} + \cdots + c_n \frac{u_n'}{u_n}\,.$$

*Proof.* Suppose that $y = \int \alpha$, a solution of $y' = \alpha$ is elementary over $\mathbb{F}$. This implies that there exists a tower of differential fields:

$$\mathbb{F} \subseteq \mathbb{F}(t_1) \subseteq \mathbb{F}(t_1, t_2) \subseteq \cdots \mathbb{F}(t_1, t_2, \ldots, t_N)$$

such that all of these fields have the same constants, $y \in \mathbb{F}(t_1, \ldots, t_N)$, and each $t_i$ is either algebraic, logarithmic, or exponential over $\mathbb{F}(t_1, \ldots, t_{i-1})$.

Use proof by induction. If $N = 0$, $y \in \mathbb{F}$ and thus $\alpha = y' \in \mathbb{F}$ so we're done. Suppose the result is true for any tower of height $N-1$. Notice that the tower with $\mathbb{F}$ deleted is $N-1$ steps tall. Therefore, by induction, there exists constants $c_1, \ldots, c_n$ and elements $u_1, \ldots, u_n, v \in \mathbb{F}(t_1)$ such that $\alpha = v' + \sum_{i=1}^{n} c_i \frac{u_i'}{u_i}$. We need to get elements in $\mathbb{F}$ (not $\mathbb{F}(t_1)$). To do this we consider several cases: $t_1$ is algebraic or transcendental (then when $t_1$ is transcendental it must be either logarithmic, or exponential).

Case 1: Suppose $t_1 = t$ is algebraic over $\mathbb{F}$. There exists some non-zero polynomials in $\mathbb{F}[t]$ such that $u_i = U_i(t)$ and $v = V(t)$. Consider the distinct conjugates of $t$ in some algebraic closure of $\mathbb{F}(t)$ [or some splitting field over $\mathbb{F}(t)$] say $t = \tau_1, \tau_2, \ldots, \tau_s$. Now $\mathbb{E} = \mathbb{F}(\tau_1, \ldots, \tau_s)$ is an algebraic extension of $\mathbb{F}$ so it extends uniquely as a differential field. There is an automorphism of $\mathbb{E}$ fixing $\mathbb{F}$ such that $t = \tau_1$ maps to $\tau_j$ (this is the very definition of a "conjugate"), call this map $\sigma_j$, then we have $\alpha = \sigma_j(\alpha) = \sigma_j\left(V(t)' + \sum_{i=1}^{n} c_i \frac{U_i'(t)}{U_i(t)}\right) = V(\tau_j)' + \sum_{i=1}^{n} c_i \frac{U_i'(\tau_j)}{U_i(\tau_j)}$ (because $\alpha$ and all of the coefficients in the polynomials $U_i$ and $V$ lie in $\mathbb{F}$ and so are fixed by $\sigma$).

Now we "symmetrize". Add up all of these conjugate expressions and divide by $s$ (note that $s^{-1}$ exists because we are working in characteristic 0). First, note that by "logarithmic differentiation" we have:

$$\frac{(A_1 \cdots A_s)'}{A_1 \cdots A_s} = \frac{A_1'(A_2 \cdots A_s) + (A_1)A_2'(A_3 \cdots A_s) + \cdots + (A_1 \cdots A_{s-1})A_s'}{A_1 \cdots A_s} = \frac{A_1'}{A_1} + \cdots + \frac{A_s'}{A_s}\,.$$

Therefore, symmetrizing yields:

$$\alpha = \frac{1}{s}\sum_{j=1}^{s} \alpha = \frac{1}{s}\sum_{j=1}^{s} \sigma_j(\alpha) = \frac{1}{s}\sum_{j=1}^{s}\left(V(\tau_j)' + \sum_{i=1}^{n} c_i \frac{U_i'(\tau_j)}{U_i(\tau_j)}\right) = \frac{1}{s}\sum_{j=1}^{s} V(\tau_j)' + \sum_{i=1}^{n} \frac{c_i}{s} \frac{(U_i(\tau_1)\cdots U_i(\tau_s))'}{U_i(\tau_1)\cdots U_i(\tau_s)}\,.$$

Notice that $\frac{1}{s}(V(\tau_1)' + \cdots + V(\tau_s)')$ is fixed by all automorphisms because it's symmetric. Likewise, all automorphisms fix each $\frac{(U_i(\tau_1)\cdots U_i(\tau_s))'}{U_i(\tau_1)\cdots U_i(\tau_s)}$ because they are symmetric. Hence, each of these lies in the ground field $\mathbb{F}$. Letting $v = \frac{1}{s}(V(\tau_1) + \cdots + V(\tau_s))$ and $u_i = U_i(\tau_1)\cdots U_i(\tau_s)$ we're done.

Case 2: Suppose that $t_1 = t$ is transcendental $\mathbb{F}$. Again we have $v, u_1, \ldots, u_n \in \mathbb{F}(t_1) = \mathbb{F}(t)$. But now, since $t$ is transcendental, we need to consider rational polynomials in $t$ with coefficients in $\mathbb{F}$. Such polynomials can be

factored and for any $w = u_i$ we can get $w = a_1(t)^{k_1} \cdots a_\ell(t)^{k_\ell} \cdot b$ where $a_i(t) \in \mathbb{F}[t]$ is monic and irreducible, $k_j \in \mathbb{Z}_{\neq 0}$ (positive and negative powers), and $b \in \mathbb{F}^\times$. Again, using logarithmic differentiation we have

$$\frac{w'}{w} = \frac{(ba_1(t)^{k_1} \cdots a_\ell(t)^{k_\ell})'}{ba_1(t)^{k_1} \cdots a_\ell(t)^{k_\ell}} = \frac{b'}{b} + k_1 \frac{a_1'(t)}{a_1(t)} + \cdots + k_\ell \frac{a_\ell'(t)}{a_\ell(t)}\,.$$

So without loss of generality we can assume each $u_i$ is either a monic irreducible $a(t) \in \mathbb{F}[t]$ or an element of $\mathbb{F}$. As for $v$, decompose it into its partial fraction decomposition. After possibly a polynomial term, each term in the fractional part of this decomposition is of the form $\dfrac{g(t)}{f(t)^r}$ for some monic irreducible $f(t) \in \mathbb{F}[t]$ and some $g(t) \in \mathbb{F}[t]$ where $\deg(g(t)) < \deg(f(t))$.

Case 2A: Suppose that (in addition to being transcendental) $t$ is logarithmic over $\mathbb{F}$. This means that there exists some $a \in \mathbb{F}^\times$ such that $t' = \dfrac{a'}{a}$. Thus $t' = a'/a \in \mathbb{F}$. By Lemma 4.11, if $f(t) \in \mathbb{F}[t]$, then $(f(t))' \in \mathbb{F}[t]$ and $(f(t))'$ has degree 1 less than that of $f(t)$. Since $f(t)$ is irreducible (and the $\mathbb{F}$ is separable since it has characteristic 0), $(f(t))'$ and $f(t)$ must be relatively prime. Notice that

$$\left(\frac{g(t)}{f(t)^r}\right)' = \frac{(g(t))'(f(t))^r - g(t)r(f(t))^{r-1}(f(t))'}{(f(t))^{2r}} = \frac{(g(t))'}{(f(t))^r} - \frac{rg(t)(f(t))'}{(f(t))^{r+1}}\,.$$

Now $\deg(g(t))$ and $\deg((f(t))')$ are both less than $\deg(f(t))$. This along with the fact that $f(t)$ is irreducible implies that $f(t)$ does not divide $g(t)$ or $(f(t))'$. Therefore, the partial fraction decomposition of $v'$ involves a term with the denominator $(f(t))^{r+1}$. Thus this appears in $\alpha$'s partial fraction decomposition. But $\alpha \in \mathbb{F}$ so it has no fractional part to its decomposition (it's already its own decomposition). Thus such terms cannot appear in $v$'s decomposition. Likewise, they cannot appear in the $u_i$'s either. Therefore, $u_1, \ldots, u_n \in \mathbb{F}$ and $v = V(t) \in \mathbb{F}[t]$ (a polynomial in $t$ – that is – $v$ has no fractional part).

At this point we have, $\alpha = (V(t))' - \sum_{i=1}^{n} c_i \dfrac{u_i'}{u_i}$ where $c_i$, $u_i$, $u_i'$, and $\alpha$ all lie in $\mathbb{F}$. Therefore, $(V(t))' \in \mathbb{F}$. Hence $v = V(t) = ct + d$ for some $c, d \in \mathbb{F}$. But $v'$ has degree 0, so $c$ must be a constant. Therefore, $(V(t))' = c\dfrac{a'}{a} + d'$ where $a, d \in \mathbb{F}$ and $c$ is a constant. We then have

$$\alpha = d' + c\frac{a'}{a} + \sum_{i=1}^{n} c_i \frac{u_i'}{u_i}\,,$$

just as we wanted.

Case 2B: Suppose that (in addition to being transcendental) $t$ is exponential over $\mathbb{F}$. This means $\dfrac{t'}{t} = b'$ for some $b \in \mathbb{F}$. Recall that Lemma 4.11 says, $\deg(f(t)) = \deg((f(t))')$ and $f(t)$ divides $(f(t))'$ only if $f(t)$ is a monomial. So if $f(t)$ is monic irreducible and $f(t) \neq t$, then $f(t)$ is not a monomial and so $f(t)$ does not divide $(f(t))'$. As before, if $f(t) \neq t$, then $\dfrac{(f(t))'}{f(t)}$ can be written as a polynomial in $t$ plus a proper fraction with denominator $f(t)$. We are led to the same contradiction since if $\dfrac{g(t)}{(f(t))^r}$ appears in the partial fraction decomposition of $v$, then $v'$ will have a term in it's decomposition with denominator $(f(t))^{r+1}$, so this appears in the decomposition of $\alpha \in \mathbb{F}$ (which has no fractional part). The same applies to the $u_i$'s. Therefore, the only fractional parts that can appear must have denominators $f(t)^m = t^m$. This implies that $v = V(t) = \sum a_j t^j$ for some $a_j \in \mathbb{F}$ where the sum ranges over a finite set of integers (some powers can be negative). Likewise, all $u_i \in \mathbb{F}$ with a possible exception of some $u_i = t$, without loss of generality, say $u_1 = t$. Then $\sum_{i=1}^{n} c_i \dfrac{u_i'}{u_i} = c_1 \dfrac{t'}{t} + \sum_{i=2}^{n} c_i \dfrac{u_i'}{u_i}$. But $\dfrac{t'}{t} = b' \in \mathbb{F}$. Therefore, again $(V(t))' = \alpha - c_1 b' - \sum_{i=2}^{n} c_i \dfrac{u_i'}{u_i} \in \mathbb{F}$. Recall that $(at^n)' = ht^n$ for some $h \in \mathbb{F}^\times$. But $(V(t))'$ has no $t$ terms (it belongs to $\mathbb{F}$), thus $V(t) = at^0 = a \in \mathbb{F}^\times$. Therefore, $\alpha = c_1 \dfrac{t'}{t} + \sum_{i=2}^{n} c_i \dfrac{u_i'}{u_i} + v' = (c_1 b + v)' + \sum_{i=2}^{n} c_i \dfrac{u_i'}{u_i}$ as desired. □

Now with Liouville's theorem in hand, we can show that various functions are not elementary functions. This means that we "cannot integrate" them (well, we can't integrate them and get a formula for the antiderivative written in terms of elementary functions).

**Corollary 4.13.** *Let $f(x), g(x) \in \mathbb{C}(x)$ be nonzero and suppose that $g(x)$ is also non-constant. Then $\int f(x)e^{g(x)}\,dx$ is elementary if and only if $f(x) = a'(x) + a(x)g'(x)$ for some $a(x) \in \mathbb{C}(x)$.*

*Proof.* We will suppress the variable $x$ and write $f = f(x)$, $g = g(x)$, etc. Let $\mathbb{F} = \mathbb{C}(x)$ and $t = e^g$ so that we have $t'/t = g'$ (i.e. $\mathbb{F}(t)$ is an exponential extension). Also, since $g$ is non-constant, $\mathbb{F}(t)$ is a pure transcendental extension of $\mathbb{F}$. Suppose that $\int fe^g\,dx = \int ft\,dx$ is elementary, by Liouville's Theorem 4.12 we can write $ft = v' + \sum_{i=1}^{n} c_i \frac{u_i'}{u_i}$ for some $v, u_1, \ldots, u_n \in \mathbb{F}(t)$ and $c_1, \ldots, c_n \in \mathbb{C}$.

As in the proof of Liouville's theorem, we can factor each $u_i \notin \mathbb{F}$ into a power product of irreducible elements of $\mathbb{F}[t]$ and then using logarithmic differentiation, we can guarantee (at the expense of a possibly longer summation) that each of $u_i \notin \mathbb{F}$ is distinct, monic, and irreducible.

Now imagine that $v$ has been expanded in its partial fraction decomposition (with respect to the ring $\mathbb{F}[t]$). If this decomposition of $v$ had some (nonzero) term $\frac{a}{b^k}$ (necessarily with $\deg(a) < \deg(b)$ and $k \in \mathbb{Z}_{>0}$ as this is part of what it takes to be a term in a partial fraction decomposition), then when computing $v'$ we would have a term $\frac{a'b^k - akb^{k-1}b'}{b^{2k}} = \frac{a'}{b^k} - k\frac{ab'}{b^{k+1}}$. Notice that $v' = ft - \sum c_i u_i'/u_i$ where the $u_i$'s of degree $> 0$ are distinct, monic, and irreducible and only appear in denominators raised to the first power. This means that either $a'b^k - akb^{k-1}b' = 0$ (i.e. $(a/b)' = 0$) or $k = 1$ (i.e. only the first power of $b$ can possibly appear in the denominator).

Now if $k = 1$, we have $\frac{a'}{b} - \frac{ab'}{b^2}$ and thus the second term cannot be unreduced (after reducing we can only have the first power of $b$ appearing) so $b$ must divide $-ab'$ (in $\mathbb{F}[t]$). Now $b$ is irreducible so $b$ either divides $-a$ or $b'$. But $\deg(a) < \deg(b)$, so $b$ must divide $b'$. However, by Lemma 4.11, part 2, $\deg(b) = \deg(b')$, this means that $b' = cb$ for some $c \in \mathbb{F}$. Again by Lemma 4.11, $b$ must be a monomial. It's irreducible, monic, and monomial so $b = t$.

On the other hand, $a'b^k - akb^{k-1}b' = 0$ and so $a'b = kab'$. Thus $b$ divides $kab'$ so as in the paragraph above we will be led to conclude that $b = t$. Therefore, the only fractional terms in the partial fraction decomposition of $v$ have denominators $b^k = t^k$. Thus $v = \sum p_j t^j$ for some $p_j \in \mathbb{F}$ (the sum ranging over a finite set of integers).

Now turning back to the $u_i$'s. Notice that $\sum_{i=1}^{n} c_i u_i'/u_i = ft - v' = ft - \sum p_j t^j$ and $u_j$ is either in $\mathbb{F}$ or monic irreducible. Thus the only possible $u_i \notin \mathbb{F}$ would be $u_i = t$. In this case, $u_i'/u_i = t'/t \in \mathbb{F}$. Thus $\sum_{i=1}^{n} c_i u_i'/u_i \in \mathbb{F}$.

At this point we have $ft = v' + \sum_{i=1}^{n} c_i \frac{u_i'}{u_i} = \sum p_j' t^j + \sum p_j j t^{j-1} t' + q$ where $q = \sum_i u_i'/u_i \in \mathbb{F}$. Recall that $t'/t = g' \in \mathbb{F}$ so $ft = \sum p_j' t^j + \sum j p_j g' t^j + q$. Comparing coefficients of $t^1$, we get $f = p_1' + 1p_1 g'$. Letting $a = p_1$ ($\in \mathbb{F}$), we have $f = a' + ag'$ as desired.

Conversely, suppose that $f = a' + ag'$ for some $a \in \mathbb{F}$. Then $\int fe^g = \int (a' + ag')e^g = ae^g$. □

**Example 4.14.** $\int e^{x^2}\,dx$ is not elementary. In Corollary 4.13, this goes with $f(x) = 1$ and $g(x) = x^2$. So if it were elementary, we would have a solution $a(x) \in \mathbb{C}(x)$ for $1 = a'(x) + 2xa(x)$. Consider $a(x) = p(x)/q(x)$ for some $p(x), q(x) \in \mathbb{C}[x]$ and $q(x) \neq 0$. Without loss of generality, assume $p(x)$ and $q(x)$ are relatively prime. Then $1 = \frac{p'(x)q(x) - p(x)q'(x)}{q(x)^2} + 2x\frac{p(x)}{q(x)}$. Clearing denominators we get $q(x)^2 = p'(x)q(x) - p(x)q'(x) + 2xp(x)q(x)$. In other words, $q(x)(q(x) - 2xp(x) - p'(x)) = -p(x)q'(x)$. Notice that if $q(x)$ has a root, say $r$, then $p(r) \neq 0$ (since $p(x)$ and $q(x)$ are relatively prime). But $q(x)(q(x) - 2xp(x) - p'(x)) = -p(x)q'(x)$ so if $q(x)$ has a factor $(x - r)^k$ then $q'(x)$ must have the same factor! This is impossible ($q'(x)$ must have one less factor). Thus $q(x)$ cannot have any roots (i.e. $q(x) = c$ is constant). But then we have $a(x) = p(x)/c$ so $a(x)$ must be a polynomial. But then looking at degrees we have $0 = \deg(1) = \deg(a'(x) + 2xa(x)) = \deg(a(x)) + 1$ (contradiction). Hence, no such $a(x)$ exists. Thus our integral is not elementary. This means that the error function: $\operatorname{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{t^2}\,dt$ isn't elementary.

**Example 4.15.** $\int \frac{e^x}{x}\,dx$ is not elementary. In Corollary 4.13, this goes with $f(x) = 1/x$ and $g(x) = x$. So if it were elementary, we would have a solution $a(x) \in \mathbb{C}(x)$ for $1/x = a'(x) + 1a(x)$. In other words, $1 = x(a'(x) + a(x))$. If $a(x) = p(x)/q(x)$ is again written in lowest terms, $a'(x) = (p'(x)q(x) - p(x)q'(x))/q(x)^2$ and so after clearing denominators $q(x)^2 = x[p'(x)q(x) - p(x)q'(x) + p(x)q(x)]$. Suppose that $q(x)$ has some root $r \neq 0$ with multiplicity $k$, then $xp(x)q'(x) = q(x)[xp'(x) + p(x) - q(x)]$ and again we reach the same kind of contradiction as in the example above. Thus the only root $q(x)$ can have is 0. Since $q(x)^2 = x[p'(x)q(x) - p(x)q'(x) + p(x)q(x)]$, 0 is a root (and must be repeated). Thus $q(x) = cx^k$ for some $k > 1$. Then, $x^k(ckp(x)) = xp(x)kcx^{k-1} = xp(x)q'(x) = q(x)[xp'(x) + p(x) - q(x)] = cx^k[xp'(x) + p(x) - cx^k]$ and so $kp(x) = xp'(x) + p(x) - cx^k$ and thus $(k-1)p(x) = xp'(x) - cx^k$ so that $p(x)$ has 0 as a root. But then $p(x)$ and $q(x)$ aren't relatively prime (contradiction). Thus our integral is not elementary.

This also implies that the real and imaginary parts of this integral are not elementary. Therefore, the sine integral function $\mathrm{Si}(x) = \int_0^t \frac{\sin(t)}{t}\,dt$ isn't elementary.

**Example 4.16.** $\int \frac{1}{\ln(x)}\,dx$ is not elementary. Let $u = \ln(x)$ (so $e^u = x$) then $du = 1/x\,dx$ so that $\int \frac{1}{\ln(x)}\,dx = \int \frac{x}{x\ln(x)}\,dx = \int \frac{e^u}{u}\,du$. Thus if the integral of $1/\ln(x)$ were elementary, then $\int \frac{e^x}{x}\,dx$ would be too – which it isn't.

The above proof of Liouville's theorem was drawn from the article [Rosenlicht]. Additional examples of non-elementary integrals as well as some more details about our examples can be found in the article [Mead]. The books [Kaplansky] and [Ritt] are classical introductions to differential algebra whereas [Magid] and [Crespo & Hajto] give more modern introductions to the subject.

It turns out that there is a complete algorithm for determining when a function can be integrated in terms of elementary functions. This is the so called "Ricsh Algorithm" developed by Robert Risch in the late 60's. For an excellent, very readable, introduction to this as well as more details about results like Liouville's theorem, I highly recommend [Geddes].

## 4.2 Some Differential Galois Theory

**Definition 4.17.** Let $R$ be a (commutative) differential integral domain with 1. Use the usual abbreviation for our derivation: $\partial(a) = a'$. Let $R\{Y\} = R[Y, Y', Y'', \dots]$ (polynomials in variables $Y, Y', Y'', \dots$ and coefficients in $R$). We adopt the usual derivative notation: $Y^{(0)} = Y, Y^{(1)} = Y', Y^{(2)} = Y''$ etc. Extend the derivation on $R$ to a derivation on $R\{Y\}$ as follows: $\partial(Y^{(i)}) = Y^{(i+1)}$. This makes $R\{Y\}$ into a differential integral domain. This is the ring of polynomials in a *differential indeterminate* $Y$. Likewise, one can define $R\{Y_1, Y_2, \dots\}$ (differential polynomials in several or even infinitely many differential indeterminates).

Since $R$ is an integral domain, then so is any ring of polynomials with coefficients in $R$. Therefore, $R\{Y\}$ is an integral domain. We denote its field of fractions as $R\langle Y\rangle$. As discussed in our other handout, the derivation on a differential ring can be extended to its field of fractions in a unique way (using the quotient rule). Thus $R\langle Y\rangle$ is a differential field called *differential rational functions* in $Y$.

If $\mathbb{E}/\mathbb{K}$ is a differential field extension and $y_1, \dots, y_n \in \mathbb{E}$, we write $\mathbb{K}\{y_1, \dots, y_n\}$ for the differential subalgebra of $\mathbb{E}$ generated by $\mathbb{K}$ and $\{y_1, \dots, y_n\}$. Likewise, $\mathbb{K}\langle y_1, \dots, y_n\rangle$ is the differential subfield generated by $\mathbb{K}$ and $\{y_1, \dots, y_n\}$.

**Definition 4.18.** Let $R$ be a differential ring and $y_1, \dots, y_n \in R$. We define the *Wronskian* of these elements as follows:

$$W(y_1, y_2, \dots, y_n) = \det\left(\begin{bmatrix} y_1 & y_2 & \cdots & y_n \\ y_1' & y_2' & \cdots & y_n' \\ \vdots & \vdots & \ddots & \vdots \\ y_1^{(n-1)} & y_2^{(n-1)} & \cdots & y_n^{(n-1)} \end{bmatrix}\right).$$

Recall that when studying linear differential equations, one uses the Wronskian to determine whether a set of solutions is linearly independent or not.

**Definition 4.19.** Let $\mathbb{E}$ be a differential field extension of a differential field $\mathbb{K}$. We say that $\mathbb{E}/\mathbb{K}$ is a *Picard-Vessiot* (read "Picard Vess-e-o") extension if $\mathbb{E}$ has no new constants (i.e. the constants of $\mathbb{E}$ and $\mathbb{K}$ are the same) and there exists some

$$\mathcal{L}(Y) = Y^{(n)} + a_{n-1}Y^{(n-1)} + \cdots + a_1Y' + a_0Y \in \mathbb{K}\langle Y\rangle$$

and $y_1, \ldots, y_n \in \mathbb{E}$ such that $\mathbb{E} = \mathbb{K}\langle y_1, \ldots, y_n\rangle$, $\mathcal{L}(y_i) = 0$ for $i = 1, \ldots, n$, and $W(y_1, \ldots, y_n) \neq 0$.

This means that $\mathcal{L}(Y) = 0$ is an $n$-th order homogenous linear differential equation. We demand that $y_1, \ldots, y_n$ is a fundamental solution set: $\mathcal{L}(y_i) = 0$ says that $y_i$ is a solution, $W(y_1, \ldots, y_n) \neq 0$ says that these solutions are linearly independent. One can show that the solution set of $\mathcal{L}(Y) = 0$ is an $n$-dimensional (over the constants of $\mathbb{K}$) vector space. This means that if $\mathbb{C}$ is the field of constants of $\mathbb{K}$ (and $\mathbb{E}$) then the solution set of $\mathcal{L}(Y) = 0$ is $\text{span}_{\mathbb{C}}\{y_1, \ldots, y_n\}$. Finally, $\mathbb{E} = \mathbb{K}\langle y_1, \ldots, y_n\rangle$ says that $\mathbb{E}$ is generated by this solution set.

Some analogies: $\mathbb{K}\{Y\}$ is the differential analog of $\mathbb{K}[x]$ (polynomials). $\mathbb{K}\langle Y\rangle$ is the analog of $\mathbb{K}(x)$ (rational functions). Instead of a polynomial $f(x) \in \mathbb{K}[x]$, we have a differential operator $\mathcal{L}(Y)$. Instead of roots of $f(x)$, we have solutions of $\mathcal{L}$. Instead of a splitting field $\mathbb{E}$ being generated by the roots of $f(x)$, we have the Picard-Vessiot extension $\mathbb{E}$ generated by the solutions of $\mathcal{L}(Y) = 0$. Also, recall that $\mathbb{F}[x]/(p(x)) \cong \mathbb{F}[\alpha]$ if $p(x) \in \mathbb{F}[x]$ is irreducible and $p(\alpha) = 0$. Likewise, we can build $\mathbb{E} = \mathbb{K}\{Y\}/I$ where $I$ is the differential ideal generated by $\mathcal{L}(Y)$ and its dervatives. Then $\mathbb{E}$ extends $\mathbb{K}$ and has a solution "$Y + I$" for $\mathcal{L}(Y) = 0$.

At this point you might anticipate that the Picard-Vessiot extension of $\mathcal{L}(Y)$ over $\mathbb{K}$ is unique up to a differential isomorphism extending the identity on $\mathbb{K}$ (if we assume that we have an algebraically closed field of constants).

**Definition 4.20.** Let $\mathbb{E}/\mathbb{K}$ be a differential field extension.

$$\text{Gal}(\mathbb{E}/\mathbb{K}) = \{\sigma : \mathbb{E} \to \mathbb{E} \mid \sigma \text{ is a differential field automorphism of } \mathbb{E} \text{ and } \sigma(x) = x \text{ for all } x \in \mathbb{K}\}$$

That is, $\text{Gal}(\mathbb{E}/\mathbb{F})$ is the automorphisms of $\mathbb{E}$ fixing $\mathbb{K}$ pointwise. We call this the *differential Galois group* of the differential field extension $\mathbb{E}/\mathbb{K}$.

Since every differential ring homomorphism is also a plain old ring homomorphism, we get that the differential Galois group is actually a subgroup of the regular Galois group of $\mathbb{E}/\mathbb{K}$ thought of as a plain old field extension.

As with regular Galois theory, if $\mathbb{E}/\mathbb{K}$ is the Picard-Vessiot extension of some linear differential equation $\mathcal{L}(Y) = 0$, we call $\text{Gal}(\mathbb{E}/\mathbb{K})$ the Galois group of $\mathcal{L}(Y)$.

Proposition 6.2.1 in [Crespo & Hajto] proves that for a Picard-Vessiot extension $\mathbb{E} = \mathbb{K}\langle y_1, \ldots, y_n\rangle/\mathbb{K}$ where the constants $\mathbb{C}$ are algebraically closed, there exists a set of polynomials $S \subset \mathbb{C}[x_{11}, \ldots, x_{1n}, x_{21}, \ldots, x_{2n}, \ldots, x_{n1}, \ldots, x_{nn}]$ such that for all $\sigma \in \text{Gal}(\mathbb{E}/\mathbb{K})$ and $\sigma(y_j) = \sum_i c_{ij}y_i$ (where $c_{ij} \in \mathbb{C}$) then $F(c_{11}, \ldots, c_{nn}) = 0$ for all $F \in S$. Also, given $C = (c_{ij}) \in \text{GL}_n(\mathbb{C})$ such that $F(c_{11}, \ldots, c_{nn}) = 0$ for all $F \in S$, then $\sigma$ defined by $\sigma$ is the identity on $\mathbb{K}$ and $\sigma(y_j) = \sum_i c_{ij}y_i$ is always an element of $\text{Gal}(\mathbb{E}/\mathbb{K})$.

This Proposition tells us that the differential Galois group of a Picard-Vessiot extension is a closed subgroup of $\text{GL}_n(\mathbb{C})$. In other words, these are *Linear Algebraic Groups*.

It turns out that $\dim(\text{Gal}(\mathbb{E}/\mathbb{K}))$ equal to the transcendence degree of $\mathbb{E}/\mathbb{K}$.

**Example 4.21.** Notice $\text{GL}_1(\mathbb{C}) = \mathbb{C}^\times$. The closed subgroups of this group are either the whole group itself (i.e. $\mathbb{C}^\times$) or finite (hence cyclic since finite subgroups of a group of units of a field must be cyclic). So the Galois group of any first order $\mathcal{L}(Y) = Y' + aY$, must be a subgroup of $\text{GL}_1(\mathbb{C})$ and so it is either finite and cyclic or $\mathbb{C}^\times$.

Let $\mathbb{K} = \mathbb{C}(x)$. If $a = 0$, then $\mathcal{L}(Y) = Y'$. Here the solutions are just constants (i.e. $\mathbb{C}$). Thus $\mathbb{E} = \mathbb{K}\langle 1\rangle = \mathbb{C}(x)$. Thus $\mathbb{E}/\mathbb{K}$ is trivial and so $\text{Gal}(\mathbb{E}/\mathbb{K})$ is trivial. On the other hand if $a \neq 0$, then $\mathcal{L}(Y) = Y' + aY = 0$ has solution $t = e^{-\int a}$. When $a \neq 0$, $t = e^{-\int a}$ is transcendental over $\mathbb{K} = \mathbb{C}(x)$. So $\mathbb{E} = \mathbb{C}(x, e^{-\int a})$ has transcendence degree 1 (over $\mathbb{K} = \mathbb{C}(x)$) and so the Galois group is 1 dimensional. Therefore, $\text{Gal}(\mathbb{E}/\mathbb{K}) = \mathbb{C}^\times$.

**Theorem 4.22** (The fundamental theorem of differential Galois theory)**.** *Let $\mathbb{E}/\mathbb{K}$ be a Picard-Vessiot extension and $G = \text{Gal}(\mathbb{E}/\mathbb{K})$. Assume that $\mathbb{C}$, the field of constants of $\mathbb{E}$ and $\mathbb{K}$, is algebraically closed. Then $H \mapsto \mathbb{E}^H$ and*

$\mathbb{F} \mapsto \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ *is an inclusion reversing bijection (and its inverse) from the collection of closed subgroups of* $G$ *to the set of intermediate differential fields of* $\mathbb{E}/\mathbb{K}$.

*Moreover, if* $H$ *is a closed normal subgroup of* $G$*, then* $\mathbb{E}^H/\mathbb{K}$ *is a Picard-Vessiot extension and* $G/\mathrm{Gal}(\mathbb{E}/\mathbb{E}^H) \cong \mathrm{Gal}(\mathbb{E}^H/\mathbb{K})$*. Also, if* $\mathbb{F}/\mathbb{K}$ *is Picard-Vessiot, then* $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ *is a closed normal subgroup of* $G$.

**Definition 4.23.** Let $\mathbb{E}/\mathbb{K}$ be a differential field extension. We say that $t \in \mathbb{E}$ is *integral* over $\mathbb{K}$ if $t' \in \mathbb{K}$ (i.e. $t = \int a$ for some $a \in \mathbb{K}$). We say that $t \in \mathbb{E}$ is *exponential integral* over $\mathbb{K}$ if $t \neq 0$ and $t'/t \in \mathbb{K}$ (i.e. $t' = at$ for some $a \in \mathbb{K}$ so that $t = \exp(\int a)$).

For example, $\mathbb{C}(x)/\mathbb{C}$ is an extension by an integral since $x = \int 1$. Whereas, $\mathbb{C}(x, e^{\arctan(x)})/\mathbb{C}(x)$ is an extension by an exponential integral since $(e^{\arctan(x)})'/e^{\arctan(x)} = \dfrac{1}{x^2+1} \in \mathbb{C}(x)$ (i.e. $e^{\arctan(x)} = e^{\int 1/(x^2+1)}$).

Adjunction of an integral yields a Galois group isomorphic to $\mathbb{C}$ (under addition). Adjunction of an exponential of an integral yields a Galois group isomorphic to $\mathbb{C}^\times$ (under multiplication). See [Crespo & Hajto] Example 6.1.4.

**Definition 4.24.** Let $\mathbb{K} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_n = \mathbb{E}$ be a tower of differential fields and assume they all share the same algebraically closed field of constants (call this $\mathbb{C}$). Then $\mathbb{E}/\mathbb{K}$ is a *Liouville extension* if for $i = 1, \ldots, n$, $\mathbb{F}_i = \mathbb{F}_{i-1}(t)$ for some $t \in \mathbb{F}_i$ and $t$ is either algebraic, integral, or exponential integral over $\mathbb{F}_{i-1}$.

Let $\mathbb{E}/\mathbb{K}$ be a Picard-Vessiot extension associated with some $\mathcal{L}(Y)$. We say $\mathcal{L}(Y) = 0$ is *solvable* (by a finite number of integrations) if there exists some Liousville extension $\mathbb{L}/\mathbb{K}$ with $\mathbb{E}$ a differential subfield of $\mathbb{L}$.

So $\mathcal{L}(Y) = 0$ is solvable if its solutions can be obtained after a finite number of integrations, exponentiations, and algebraic operations.

*Note.* Liouville extensions can be arranged so that $\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{E}$ where $\mathbb{F}/\mathbb{K}$ is a Galois extension (in the standard Galois theory sense) and $\mathbb{E}/\mathbb{K}$ is the result of adjoining integrals and exponentials of integrals (i.e. you can arrange your tower so that all of the algebraic stuff is attached first). This is why [Crespo & Hajto] don't allow for adjoining algebraic stuff in their Liouville extensions (they assume your base field already includes all that stuff).

Algebraic groups are a good deal more complicated than finite groups. There is a way to define "connectedness" in such groups. It turns out that, given an algebraic group $G$, the connected component at the identity $G_0$ (this is the connected piece of the algebraic group $G$ which contains the identity) is in fact a subgroup of $G$. An algebraic group is called *virtually solvable* if $G_0$ is solvable.

**Theorem 4.25.** *Liouville extensions have virtually solvable differential Galois groups. Moreover,* $\mathcal{L}(Y) = 0$ *is solvable if and only if its differential Galois group is virtually solvable.*

**Example 4.26.** $\mathbb{C}(x)$ is a Picard-Vessiot (and Liouville) extension of $\mathbb{C}$. It is Picard-Vessiot with respect to $\mathcal{L}(Y) = Y''$. Notice that $\{1, x\}$ form a solution set for $Y'' = 0$ also $W(1, x) = \det \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} = 1 \neq 0$. Clearly, $\mathbb{C}(x) = \mathbb{C}(x, 1)$. It is Liouville since $x = \int 1$ is integral over $\mathbb{C}$.

$$\mathrm{Gal}(\mathbb{C}(x)/\mathbb{C}) \cong \mathbb{C} \text{ (under addition) } \cong \left\{ \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} \;\middle|\; c \in \mathbb{C} \right\} \text{ (a closed subgroup of } \mathrm{GL}_2(\mathbb{C})).$$

**Example 4.27.** Let $\mathcal{L}(Y) = Y'' + 2xY' \in \mathbb{C}(x)\{Y\}$. Let $\mathbb{E}/\mathbb{K} = \mathbb{C}(x)$ be the Picard-Vessiot extension for $\mathcal{L}(Y) = 0$. We have that $\mathbb{E} = \mathbb{C}(x)\langle 1, y\rangle$ for some solutions $\{1, y\}$. We must have $W(1, y) = \det \begin{bmatrix} 1 & y \\ 0 & y' \end{bmatrix} = y' \neq 0$. In fact, [Magid] in Example 6.10 shows that $y' \notin \mathbb{C}(x)$. Moreover, he also shows that $y \notin \mathbb{C}(x, y')$. We get the following tower:

$$\mathbb{K} = \mathbb{C}(x) \subsetneq \mathbb{L} = \mathbb{K}(y') \subsetneq \mathbb{E} = \mathbb{K}(y)$$

Consider some $\sigma \in \mathrm{Gal}(\mathbb{E}/\mathbb{K})$ then $\sigma(y)$ must be some solution of $\mathcal{L}(Y) = 0$ since $\sigma$ must send solutions to solutions (like old school Galois theory sent roots to roots). Thus $\sigma(y) = c1 + dy$ for some $c, d \in \mathbb{C}$. Notice that $\sigma(y') = \sigma(y)' = (c + dy)' = dy'$. Because $\sigma$ is a bijection, $d \neq 0$. This gives us that

$$\mathrm{Gal}(\mathbb{E}/\mathbb{K}) \cong \left\{ \begin{bmatrix} 1 & c \\ 0 & d \end{bmatrix} \;\middle|\; c, d \in \mathbb{C} \text{ and } d \neq 0 \right\} \text{ (a closed subgroup of } \mathrm{GL}_2(\mathbb{C}))$$

Now that this is done, we'll let the out our secret: $y = \int e^{-x^2}\,dx$ [$y' = e^{-x^2}$ and $y'' = -2xe^{-x^2}$ so that $y'' + 2xy' = 0$.]

**Theorem 4.28.** *Let $\mathbb{C}$ be algebraically closed and $\mathbb{F} = \mathbb{C}(x)$ with $x' = 1$. Let $\mathcal{E}/\mathbb{F}$ be an elementary extension and $\mathbb{E}/\mathbb{F}$ a Picard-Vessiot extension with $\mathbb{E} \subseteq \mathcal{E}$. Then the connected component of the identity of* $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ *is abelian.*

This is Proposition 6.12 in [Magid]. Notice that in the above example, $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ is not an abelian group. This means that $\mathbb{E}/\mathbb{K}$ is not contained in an elementary extension. Thus $y = \int e^{-x^2}\,dx$ is not elementary. On the other hand, $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ is virtually solvable, so $y = \int e^{-x^2}\,dx$ does lie in a Liouville extension (this is kind of a silly observation – $y$ is obviously an integral of an exponential of an integral).

**Example 4.29.** Let $\mathcal{L}(Y) = Y'' - xY$ and let $\mathbb{E}$ be the Picard-Vessiot extension of $\mathbb{C}(x)$ associated with $\mathcal{L}(Y) = 0$. In [Magid] Example 6.21, it is shown that $\mathrm{Gal}(\mathbb{E}/\mathbb{C}(x)) \cong \mathrm{SL}_2(\mathbb{C}) = \{A \in \mathbb{C}^{2\times 2} \mid \det(A) = 1\}$. Now $\mathrm{SL}_2(\mathbb{C})$ is not a virtually solvable group. This means that $\mathbb{E}/\mathbb{C}(x)$ is not embeddable in a Liouville extension. This means that $Y'' - xY = 0$ has a solution $y = f(x)$ such that $f(x)$ is not obtainable from $\mathbb{C}(x)$ by a finite number of steps of algebra, integration, and exponentiation. This makes $f(x)$ way beyond being elementary.

The equation $y'' - xy = 0$ is called the *Airy equation*. One of it solutions (one that you can't get to by integration and algebra) is called the *Airy function*.

My main references for this are [Crespo & Hajto] and [Magid]. Both books are well written and modern. [Crespo & Hajto] is a bit easier to read and includes a careful development of algebraic groups. [Magid] has some interesting examples and results that are lacking in the other text. The books [Ritt] and [Kaplansky] are interesting as well, but a bit dated. The large text [Put & Singer 2003] is much more in depth than these other books, but it is written at level which makes it much less accessible.

We have seen Galois theory (for polynomials) and differential Galois theory (for linear differential equations). It is interesting to note that one can develop a Galois theory for linear difference equations (kind of like a discrete version of differential equations). This is done in [Put & Singer 1997] and it looks a lot like the theories we've explored.

# Bibliography


[Crespo & Hajto] T. Crespo and Z. Hajto, *Algebraic Groups and Differential Galois Theory*, AMS Graduate Studies in Mathematics **Vol. 122** (2011).

[Geddes] K. Geddes, S. Czapor, and G. Labahn, *Algorithms for Computer Algebra*, Kluwer Acad. Pub. (1992).

[Kaplansky] I. Kaplansky, *An Introduction to Differential Algebra*, Publications of De L'Institut De Mathematique De L'Universite De Nancago (1957).
Available free online at: http://mmrc.iss.ac.cn/∼weili/DifferentialAlgebra/References/Kaplansky.pdf

[Magid] A. Magid, *Lectures on Differential Galois Theory*, AMS University Lecture Series **Vol. 7** (1994).

[Mead] D. Mead, *Integration*, Am. Math. Monthly **Vol. 68** No. 2 (Feb. 1961) 152–156.

[Put & Singer 1997] M. van der Put, M. Singer, *Galois Theory of Difference Equations*, Lecture Notes in Mathematics, Spring-Verlag (1997).

[Put & Singer 2003] M. van der Put, M. Singer, *Galois Theory of Linear Differential Equations*, Springer (2003).
Available free online at: https://singer.math.ncsu.edu/papers/dbook.ps

[Ritt] J. Ritt, *Differential Algebra*, Dover Publications (1950).

[Rosenlicht] M. Rosenlicht, *Integration in Finite Terms*, Am. Math. Monthly **Vol. 79** No. 9 (Nov. 1972) 963–972.