MAT205 **Supplementary Notes**
Section 4.1 Reading

At this point of the semester we take a moment to reflect. One of the most important lessons in linear algebra (and in fact a lot of math) is: *we can often use the same techniques to solve very different types of problems (after perhaps rephrasing the question in new ways).* For example, just knowing how many pivots a matrix has can tell us about existence of solutions, uniqueness of solutions, invertibility of the matrix, and more. Posing this mantra in a different way: *we can sometimes take what seem like very abstract or unrelated questions, and solve them using familiar techniques.* This leads us to ask:

When faced with very different looking questions, how do we know whether we can apply linear algebra techniques to solve them?

Example 1. *For example, in a recent Lab you did linear algebra "modulo 29." All of the numbers were always reduced modulo 29, and fractions could even be transformed back into integers. Amazingly, all of the techniques from linear algebra (like matrix multiplication and inverses) still worked! That should be surprising! To make it even more mysterious: if we tried to re-do the lab but "modulo 30," then the techniques of linear algebra would no longer work!*

To understand when linear algebra techniques are appropriate, we can think about patterns and properties we have seen so far that have appeared in different contexts. For example, for vectors $\mathbf{x}$ and $\mathbf{y}$ we know

$$\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x}.$$

Also, for integers modulo 29, we can check that

$$x + y \mod 29$$

is the same as

$$y + x \mod 29.$$

So, in both instances we were working with addition which was commutative!

Example 2. *We remember that for functions $f(t)$ and $g(t)$ we also have*

$$f(t) + g(t) = g(t) + f(t).$$

So function addition is also commutative. This may make us wonder if linear algebra techniques could be used to study functions. (Spoiler: YES!)

Example 3. *Computer scientists often work in binary so that everything is represented as a vector of* 0*s and* 1*s. This sometimes comes with special rules for addition: for example it can be useful to define* $0+1=1$ *and* $1+1=0$*. One can then check that if* $\mathbf{a}$ *and* $\mathbf{b}$ *are two vectors in binary, say* $\mathbf{a}=(1,0,1)$ *and* $\mathbf{b}=(0,1,1)$ *then still*

$$\mathbf{a}+\mathbf{b}=(1,1,0)=\mathbf{b}+\mathbf{a}.$$

So this binary addition is also commutative. This may make us wonder if linear algebra techniques could be used for computer science in binary (Spoiler: Still YES!)

In all of the examples above, one could try to sit down and think about all of the properties that are similar between vectors, integers modulo 29, and functions, or all of the properties that are different. For example, we can take derivatives of functions, but not of integers or vectors. We can multiply 2 integers, and we can multiply 2 functions, but not vectors.

There are so many things we could compare, that we are faced with the challenge of identifying which properties *need* to be the same in order for use of linear algebra techniques... it turns out that **vector spaces** are the answer. **Vector spaces have all of the necessary properties to allow for the use of linear algebra techniques**.

Definition: A **vector space** is a nonempty set V of elements, called **vectors**, with two operations: *vector addition* and *scalar multiplication*. The vectors and scalars (real numbers) satisfy the following axioms: for all $\mathbf{u},\mathbf{v},\mathbf{w}\in V$, and for all scalars $c,d\in\mathbb{R}$,

i. The sum $\mathbf{u}+\mathbf{v}\in V$ (closure under addition, in other words adding vectors doesn't result in an object that is no longer a vector)

ii. For each $\mathbf{u}\in V$ and scalar c, $c\mathbf{u}\in V$ (closure under scalar mult.)

iii. $(\mathbf{u}+\mathbf{v})+\mathbf{w}=\mathbf{u}+(\mathbf{v}+\mathbf{w})$ (associativity)

iv. There is a zero vector in V: $\mathbf{0}+\mathbf{u}=\mathbf{u}$. (additive identity)

v. For each $\mathbf{u}\in V$ there exists $\mathbf{v}\in V$ so that $\mathbf{u}+\mathbf{v}=\mathbf{0}$ (additive inverses, we often write $\mathbf{v}=-\mathbf{u}$.)

vi. $\mathbf{u}+\mathbf{v}=\mathbf{v}+\mathbf{u}$ (commutativity)

vii. $c(\mathbf{u}+\mathbf{v})=c\mathbf{u}+c\mathbf{v}$ (scalar distribution)

viii. $(c+d)\mathbf{u}=c\mathbf{u}+d\mathbf{u}$ (vector distribution)

ix. $c(d\mathbf{u}) = (cd)\mathbf{u}$ (compatibility of multiplication)

x. $1\mathbf{u} = \mathbf{u}$ (multiplicative identity)

Important: The word "vector" is a very loaded word here. It sometimes means vector in the way we have seen all semester: an ordered list of numbers from $\mathbb{R}^n$. However, mathematicians use the word vector to mean any element from a vector space. In the Lab, a vector was an ordered list of numbers between $0, \ldots, 28$. Functions can be called vectors, or polynomials can be called vectors, or binary sequences can be called vectors. It all depends on context.

Also important: Vector spaces range from very familiar sets with "normal" operations, to very surprising and bizarre objects. It is very important to remember that "vector addition" and "scalar multiplication" have to be defined as part of the vector space. One could define "addition" of vectors $\mathbf{u} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$ and $\mathbf{v} = \begin{pmatrix} 5 \\ 6 \end{pmatrix}$ by

$$\mathbf{u} + \mathbf{v} = \begin{pmatrix} 2 \\ 3 \\ 5 \\ 6 \end{pmatrix}.$$

Then it would be our job to go over each axiom of vector spaces to see if each rule still holds. If they do, then this is a different type of vector space than the usual $\mathbb{R}^n$. If the rules do not hold, then it is not a vector space. (Do you think the addition proposed here could be allowed in a vector space?)

Example 4. *The spaces of column vectors $\mathbb{R}^n$, $n \geq 1$ with our regular vector addition and scalar multiplication are the classic examples of vector spaces. Everything we've done so far this semester has been done using these vector spaces.*

Example 5. *Let $\mathbb{P}_n$ denote the set of polynomials of degree $\leqslant n$:*

$$\mathbb{P}_n = \{\mathbf{p}(t) \colon \mathbf{p}(t) = a_0 + a_1 t + \cdots + a_n t^n\}.$$

Define addition by

$$\mathbf{p}(t) + \mathbf{q}(t) = (a_0 + a_1 t + \cdots + a_n t^n) + (b_0 + b_1 t + \cdots + b_n t^n) = (a_0 + b_0) + (a_1 + b_1)t + \cdots + (a_n + b_n)t^n.$$

Notice that any or all coefficients are allowed to be zero here! Define scalar multiplication by

$$c\mathbf{p}(t) = ca_0 + ca_1 t + \cdots + ca_n t^n.$$

Then, the set $\mathbb{P}_n$ is a vector space! Each polynomial is a single vector. To be sure this is a vector space, we should check every single part of the definition. Let's check just a few:

- *(iv) The zero vector is a special element of the vector space that doesn't affect any other vectors when added. So, which polynomial do we need? After you think about it, can you convince yourself that the right polynomial is*

$$\mathbf{0} = 0 + 0t + \cdots + 0t^n?$$

It is slightly silly to write it this way, but I want to emphasize that it is not $\mathbf{0} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ *or* $\mathbf{0} = 0$ *(a single number). The zero vector here is the polynomial whose values are zero for all t. I want to check that $\mathbf{0} + \mathbf{p} = \mathbf{p}$ always.*

To rigorously check: let $\mathbf{p} \in \mathbb{P}_n$, so that $\mathbf{p}(t) = a_0 + \cdots + a_n t^n$. Then

$$\mathbf{0} + \mathbf{p} = (0 + a_0) + \cdots + (0 + a_n)t^n = a_0 + \cdots + a_n t^n = \mathbf{p}.$$

- *(v) Let $\mathbf{p} \in \mathbb{P}_n$. Then $\mathbf{p}(t) = a_0 + \cdots + a_n t^n$. We expect that the additive inverse should be the polynomial whose coefficients are all opposite sign of $\mathbf{p}$. To check let $\mathbf{v} = -a_0 + \cdots + (-a_n)t^n$. Then*

$$\mathbf{p} + \mathbf{v} = (a_0 - a_0) + \cdots + (a_n - a_n)t^n = 0 + \cdots + 0t^n = \mathbf{0}.$$

Feel free to check the other parts of the definition for yourself!