Math 1554 Extra Problems

Jad Salem

`README:` These problems are designed to go along with Math 1554. While much of the content presented here supplements the curriculum, these problems do not constitute official course material, and should not be used to study for tests.

Extra Problems are intended to be interesting, thought-provoking, and contextualizing, and will highlight the ubiquity of linear algebra across seemingly unrelated fields of math. The problems are often challenging and sometimes open-ended, so students are encouraged to discuss the problems with each other and their instructors. It may be difficult for a student to benefit from these problems without discussing them with an instructor.

Extra Problem Set #0

Definition. Let A and B be sets. The *Cartesian product* of A and B, denoted[1] $A \times B$, is the set of ordered pairs of elements from A and B. Formally,

$$A \times B = \{(a, b) : a \in A, b \in B\} \ .$$

For example, if $A = \{0\}$ and $B = \{1, 2\}$, then $A \times B = \{(0, 1), (0, 2)\}$.

E1. Let $|X|$ denote the number of elements in the set X. For finite sets A, B, what is the relationship between $|A \times B|$, $|A|$, and $|B|$?

Vague Definition. Let A, B be sets. A *function* $f : A \to B$ is an assignment of elements of B to elements of A. In other words, each $a \in A$ gets assigned an element $f(a) \in B$.

E2. Give a more formal definition of *function* using the Cartesian product.

E3. Suppose $|A| = m$ and $|B| = n$. How many functions $f : A \to B$ are there?

Definition A function $f : A \to B$ is *injective*, or *one-to-one*, if $f(a_1) = f(a_2) \implies a_1 = a_2$. The function f is *surjective*, or *onto*, if for all $b \in B$, there is some $a \in A$ with $f(a) = b$.

E4. Give examples of functions which are injective and surjective, injective and not surjective, not injective and surjective, and not injective and not surjective.

[1] We typically denote $A \times A$ by A^2.

E5. Let A, B be finite sets of the same size. Can you find a function $f : A \to B$ which is injective but not surjective? Prove your assertion.

E6. Answer the previous question for infinite sets. What are some settings under which injectivity implies surjectivity?

E7. Is it true that a function $f : A \to B$ has a left-inverse if and only if it is injective?

E8. If a function has a left-inverse, does it have a right-inverse?

Extra Problem Set #1

Definition. Let $A, B \subset \mathbb{R}$. Then the *set-sum* of A and B is $A \oplus B = \{a + b : a \in A, b \in B\}$.

For example, $\{1, 2\} \oplus \{3\} = \{4, 5\}$.

E1. Since $+$ is a binary operation, $|A \oplus B| \leqslant |A \times B| = |A| \cdot |B|$. Can you find nonempty finite sets A,B for which equality is met? Note that this would imply that elements of $A \oplus B$ are uniquely representable as $a + b$, with $a \in A$ and $b \in B$.

E2. Given finite sets A and B, find the best possible lower bound for $|A \oplus B|$. Prove your assertion.

E3. Can you find an infinite set A for which elements of $A \oplus A$ are uniquely expressible as $a_1 + a_2$, for some $a_1, a_2 \in A$? How about a dense set A?

Extra Problem Set #2

These questions concern the problem of fitting a polynomial to a set of points in $\mathbb{R}^2$. In particular, given $b_1, \ldots, b_n \in \mathbb{R}$, can we find a polynomial $p(x)$ satisfying $p(i) = b_i$ for $i = 1, \ldots, n$?

E1. (a) Suppose we had polynomials $E_1, \ldots, E_n$ such that

$$E_i(j) = \begin{cases} 1 & \text{if } j = i \\ 0 & \text{if } j \in \{1, \ldots, n\} \text{ and } j \neq i \end{cases}$$

Using these polynomials, can you find a feasible p?

(b) Can you find such $E_1, \ldots, E_n$?

E2. Assume p has degree $n-1$. Write out the coefficient matrix resulting from the system of equations $p(i) = b_i$, for $n = 2$ and $n = 3$. Find the RREF of these matrices. How does this relate to E1?

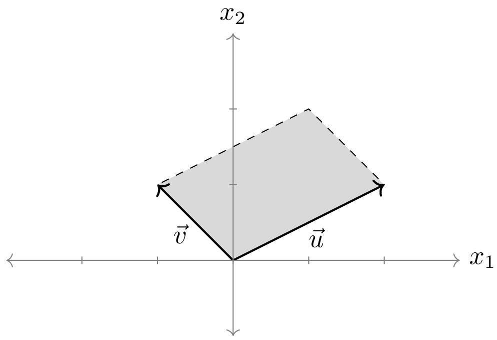
E3. Show that the columns of this matrix are linearly independent, for any $n \geqslant 2$.

Extra Problem Set #3

Given two linearly independent vectors $\vec{u} = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}$, $\vec{v} = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \in \mathbb{R}^2$, we define the *fundamental parallelogram* of $\vec{u}, \vec{v}$, denoted $\mathcal{P}(\vec{u}, \vec{v})$, by

$$\mathcal{P}(\vec{u}, \vec{v}) = \{c_1\vec{u} + c_2\vec{v} : 0 \leqslant c_1, c_2 < 1\} .$$

For example, if $\vec{u} = \binom{2}{1}$ and $\vec{v} = \binom{-1}{1}$, then $\mathcal{P}(\vec{u}, \vec{v})$ is



which has area 3.

E1. Let $A = (\vec{w}_1\ \vec{w}_2) \in \mathbb{R}^{2\times 2}$ be the matrix associated with rotation by π radians. Find $\mathcal{P}(\vec{w}_1, \vec{w}_2)$.

E2. Let $\vec{u} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\vec{v} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$. Find the area of $\mathcal{P}(\vec{u}, \vec{v})$.

E3. Let $\vec{x} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$ and $\vec{y} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$. Find the area of $\mathcal{P}(\vec{x}, \vec{y})$.

E4. Let $A = (\vec{u}\ \vec{v})$ and $B = (\vec{x}\ \vec{y}) \in \mathbb{R}^{2\times 2}$ (using $\vec{u}, \vec{v}, \vec{x}, \vec{y}$ from the previous problems). Find the product $AB = (\vec{z}_1\ \vec{z}_2)$. What is the area of $\mathcal{P}(\vec{z}_1, \vec{z}_2)$? How does this relate to the areas in E2 and E3?

E5. Make a conjecture and try to prove it.

Extra Problem Set #4

We have seen that if $A \in \mathbb{R}^{n\times n}$ is a square matrix which can be reduced to a (upper-,lower-)diagonal form with nonzero entries along the diagonal, then we can find some $\vec{x} \in \mathbb{R}^n$ satisfying $A\vec{x} = \vec{b}$. Here we will explore how well this theory extends to systems of equations over other number systems. In particular, we will look at systems of equations over $\mathbb{Q}$ (the set of rationals) and $\mathbb{Z}$ (the set of integers).

E1. Let $A = \begin{bmatrix} 2 & 0 & \frac{1}{2} \\ 1 & 1 & 1 \\ 0 & 1 & \frac{1}{4} \end{bmatrix}$ and $\vec{b} = \begin{bmatrix} 1 \\ 2 \\ \frac{1}{2} \end{bmatrix}$. Suppose we want to solve the system $A\vec{x} = \vec{b}$, but require that $\vec{x} \in \mathbb{Q}^3$. Solve this system using row reduction, if a solution exists.

[Note: to ensure your solution is rational, you can only scale rows by rational numbers!]

E2. Now suppose we want our solution to be integral (i.e., we want to find a solution $\vec{x}$ whose entries are integers). Solve the system

$$\begin{cases} 2x_1 + 2x_2 = 2 \\ 6x_1 + 2x_2 = 12 \end{cases}$$

[Note that we can only scale rows by integers.]

E3. You should have had different experiences with these two examples. What about the structure of $\mathbb{Q}$ and $\mathbb{Z}$ accounts for these differences?

Extra Problem Set #5

E1. Consider the functions $L, R : \mathbb{R}^2 \to \mathbb{R}^2$ defined by

$$L\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} x-y \\ y \end{bmatrix} \quad \text{and} \quad R\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} x \\ y-x \end{bmatrix}.$$

(a) Are these linear transformations? If so, find the standard matrices for L^k and R^k, for any natural number k.

(b) Notice that $R^2L^2R\left(\begin{bmatrix} 10 \\ 14 \end{bmatrix}\right) = \begin{bmatrix} 2 \\ 0 \end{bmatrix}$. Suppose a and b are positive integers. Can we always arrive at $\begin{bmatrix} d \\ 0 \end{bmatrix}$, for some positive integer d, by applying a sequence of Rs and Ls to $\begin{bmatrix} a \\ b \end{bmatrix}$?

(c) Going off part (b), suppose we do arrive at some $\begin{bmatrix} d \\ 0 \end{bmatrix}$. Is d uniquely determined by a and b? Is the sequence of Ls and Rs uniquely determined?

Extra Problem Set #6

Consider Pascal's triangle

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
\iddots & & & & & & & & & & \ddots
\end{array}
$$

where each entry is the sum of its two "parents" in the previous row.

E1. On the back of this page, write out as many rows of Pascal's triangle as you can, with the following modification: if an entry is even, replace it with 0; if an entry is odd, replace it with 1.

E2. Ask some good questions. Answer them?

E3. For each row in your modified Pascal's triangle, add up the entries. Any conjectures?

Extra Problem Set #7

E1. Find a polynomial $p(x)$ with *nonnegative integer coefficients* satisfying $p(1) = 9$ and $p(10) = 1233$. How many such p are there?

E2. Let $p_0, p_1, p_2, \ldots$ be a sequence of primes. You have shown (if you did Extra Problem Set #2) that for any nonnegative integer N, we can find a polynomial $f_N(x)$ satisfying

$$f_N(i) = p_i \quad \text{for } i = 0, 1, \ldots, N.$$

Can you find a polynomial $f(x)$ satisfying $f(i) = p_i$ for all nonnegative integers i?

Extra Problem Set #8

Consider the set $\mathbb{Z}_2 := \{0, 1\}$ with the following operations:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

and let $\mathrm{GL}_2(\mathbb{Z}_2)$ denote the set of invertible 2×2 matrices with entries in $\mathbb{Z}_2$.

E1. How many elements are in $\mathrm{GL}_2(\mathbb{Z}_2)$?

E2. Let $A \in \mathrm{GL}_2(\mathbb{Z}_2)$. Is it true that $A^{-1} = A^k$ for some natural number k? Justify your answer.

E3. Do matrices in $\mathrm{GL}_2(\mathbb{Z}_2)$ commute? If $A, B \in \mathrm{GL}_2(\mathbb{Z}_2)$, is it true that $A + B \in \mathrm{GL}_2(\mathbb{Z}_2)$?

E4. Let $A, B, C \in \mathrm{GL}_2(\mathbb{Z}_2)$, and suppose $AB = AC$. Is it true that $B = C$?

E5. Let S be a subset of $\mathrm{GL}_2(\mathbb{Z}_2)$ which is closed under multiplication, and let $A \in \mathrm{GL}_2(\mathbb{Z}_2)$. How many matrices are in the set $AS = \{AB : B \in S\}$?

Extra Problem Set #9

Definition. A function $f : \{1, \dots, n\} \to \{1, \dots, n\}$ is a *permutation* if it is one-to-one and onto. We define S_n to be the set of permutations of $\{1, \dots, n\}$.

For any permutation $\sigma \in S_n$, we can write σ as a composition of transpositions (swaps). Define the *sign* of σ, denoted $\operatorname{sgn}(\sigma)$, to be $(-1)^M$, where M is the number of transpositions in the decomposition of σ.
(Is this well-defined?)

Define a function $\delta : \mathbb{R}^{n\times n} \to \mathbb{R}$ by

$$\delta(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}$$

E1. Give an algorithm for computing $\delta(A)$. Brute force is okay. What is the asymptotic running time?

E2. Find $\delta(A)$ for an arbitrary matrix $A \in \mathbb{R}^{2\times 2}$. Any conjectures?

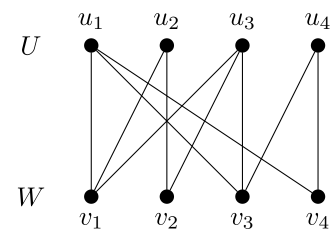
E3. How does δ interact with row operations? Can you prove your conjecture from E2?

E4. Can you use E3 to give a faster algorithm for computing $\delta(A)$?

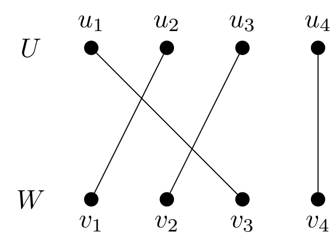
Extra Problem Set #10

Recall that a *permutation* is a one-to-one, onto function, and S_n is the set of permutations of $\{1, \ldots, n\}$. Also recall the formula for determinants from the last extra worksheet: $\det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}$.

Suppose we have a network of $2n$ nodes, where the nodes are split into two groups of size n. Suppose no two vertices in a group are connected by an edge. Here is an example for $n = 4$:



A *perfect matching* is a collection of n disjoint edges. For example, this is a perfect matching of the network above:



A perfect matching can be encoded via a permutation. For example, the matching above can be represented by $\sigma(1) = 3,\ \sigma(2) = 1,\ \sigma(3) = 2,\ \sigma(4) = 4$. If our network has edge weights w_e, then the *weight* of a perfect matching M is $\prod_{e \in M} w_e$.

E1. Find a formula (involving permutations) for the sum of weights of all perfect matchings in a network.

E2. If you did Extra Problem Set #9, you found a polynomial-time algorithm for calculating $\displaystyle\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}$.
Can you give a polynomial-time algorithm for calculating your expression from E1?

Extra Problem Set #11

Definition. Let $\mathbb{Z}_2$ denote the set $\{0, 1\}$, along with the operations "addition and multiplication (mod 2)." In particular, $+$ and $\cdot$ in $\mathbb{Z}_2$ are defined as follows:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

You have seen vector spaces over $\mathbb{R}$ in this course, but there are also vector spaces over $\mathbb{Z}_2$, such as $\mathbb{Z}_2^n$ (vectors of length n with entries in $\mathbb{Z}_2$).

E1. (a) There are 4 lights in a row, all initially off. We have three switches, which control different light. Switch 1 toggles lights 1 and 3; Switch 2 controls lights 2 and 3. Switch 3 controls lights 3 and 4. Find all (if any) sets of switches which would turn all the lights on.

(b) There are 3 lights in a row, all initially off. We have 4 switches this time. Switch 1 toggles lights 1 and 3; Switch 2 toggles lights 2 and 3; Switch 3 toggles light 2; Switch 4 toggles lights 1 and 2. Find all (if any) sets of switches which would turn on only light 3.

The notion of a "subspace" also extends to this finite setting. A subspace of $\mathbb{Z}_2^n$ is called a *linear code.*

E2. How many vectors are in $\mathbb{Z}_2^n$?

E3. List all linear codes contained in $\mathbb{Z}_2^2$.

E4. How many linear codes are there of $\mathbb{Z}_2^n$ of dimension 2?

E5. Define $\mathbb{Z}_3$ analagously. How many one-dimensional subspaces are there of $\mathbb{Z}_3^3$?

Extra Problem Set #12

Recall that $\mathbb{Z}_2$ is the set $\{0,1\}$ along with the operations "addition and multiplication mod 2," and that $\mathbb{Z}_2^n$ is a vector space over $\mathbb{Z}_2$. A subspace of $\mathbb{Z}_2^n$ is called a *linear code*. One central issue in coding theory is how to deal with the presence of noise along a communication channel. Here we will consider the problem of 1-bit alterations. i.e., upon reception of a word (vector), a single bit may have been flipped from 0 to 1, or vice versa.

E1. Consider the linear code $\mathbb{Z}_2^2$ (bit-strings of length 2). Consider the following process for detection of bit flips. First we "encode" each word $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in \mathbb{Z}_2^2$ as $\begin{bmatrix} x_1 \\ x_2 \\ x_1 + x_2 \end{bmatrix} \in \mathbb{Z}_2^3$.

(a) Find the matrix of this linear transformation.

(b) Explain how to recover the original word from this encoding. What property of our linear tranformation (encoding) allows for this recovery?

(c) Explain how to detect if the encoded word was altered in transmission.

E2. The previous problem dealt with detecting if there was a bit-flip. Find an encoding of $\mathbb{Z}_2^4$ which allows you to detect *and* correct bit-flips. What is the smallest n for which one could correct bit-flips using an encoding of $\mathbb{Z}_2^4$ into $\mathbb{Z}_2^n$?

Extra Problem Set #13

Definition. A matrix is called *row stochastic* if each row is a probability vector. Similarly, it is called *column stochastic* if each column is a probability vector. A matrix which is both row stochastic and column stochastic is called *doubly stochastic*.

Let $A \in \mathbb{R}^{n\times n}$, and let $\mathbf{1}$ be the column vector $\begin{bmatrix}1\\1\\\vdots\\1\end{bmatrix}$ of all 1's.

E1. Show that A is row stochastic if and only if $A\mathbf{1} = \mathbf{1}$.

E2. A is doubly stochastic if and only if $A\mathbf{1} = A^T\mathbf{1} = \mathbf{1}$.

E3. If A and B are row stochastic, must AB be as well?

E4. If A is doubly stochastic, must A^{-1} be as well?

E5. Is the set of doubly stochastic matrices convex?

Definition. $\sigma(A) := \{\lambda : \det(A - \lambda I) = 0\}$ is called the *spectrum* of A. The *spectral radius* of A is $\rho(A) := \max_{\lambda \in \sigma(A)} |\lambda|$.

E6. Let A be row stochastic, suppose the eigenvalues of A are real. Show that $\rho(A) = 1$.

Extra Problem Set #14

Definition. Let $G = (V, E)$ be a graph on vertex set V with edge set E. Then the *adjacency matrix* of G, denoted $A(G)$, is the matrix

$$A_{ij} = \begin{cases} 1 & v_i v_j \in E \\ 0 & \text{else} \end{cases}$$

E1. Find an expression (involving $A(G)$) for the number of walks of length k from v_i to v_j.

E2. Let $\lambda_1 \geqslant \cdots \geqslant \lambda_n$ be the eigenvalues of $A(G)$. Show that the number of closed walks (i.e., the starting and ending vertices are the same) of length k is $\sum_{i=1}^{n} \lambda_i^k$.
[Hint: diagonalize A]

E3. Show that if the spectrum of a graph G is symmetric (i.e., $\lambda_i = -\lambda_{n-i}$), then G has no odd cycles.

Extra Problem Set #15

In this class, you have seen that $\mathbb{R}^n$ is a vector space with scalars in $\mathbb{R}$. In this case, a basis of $\mathbb{R}^n$ contains n vectors. In particular, a basis for $\mathbb{R}$ as a vector space over $\mathbb{R}$ contains exactly one vector.

What if we choose a different set of scalars? Here we will consider $\mathbb{R}$ as a vector space over $\mathbb{Q}$, the set of rational numbers.

E1. Describe Span$\{1\}$.
Remember that your linear combination must use rational scalars!

E2. Is $\{1, \sqrt{2}\}$ a linearly independent set? What about $\{\sqrt{2}, \sqrt{3}\}$? What about $\{\sqrt{2}, \sqrt{3}, \sqrt{6}\}$?

E3. Can you find a basis for $\mathbb{R}$ as a vector space over $\mathbb{Q}$? How big is it?

Extra Problem Set #16

We can think of the real numbers $\mathbb{R}$ as a vector space over the rational numbers, $\mathbb{Q}$. In other words, $\mathbb{R}$ is a vector space with rational scalars. For this worksheet, let's assume that this vector space has a basis H (must such a basis exist?). Using this basis, we will prove something bizarre.

E1. Try to partition the positive real numbers $\mathbb{R}^+$ into two nonempty sets, each of which is closed under addition.
[In other words, find two disjoint sets A_1, A_2, whose union is $\mathbb{R}^+$, which satisfies the following property; for $i = 1, 2$ and all $a, b \in A_i$, we have $a + b \in A_i$.]

E2. Follow the steps below to prove the existence of such a decomposition.

(a) Recall that we can define a linear transformation by its action on a basis. So, let $h \in H$ be an element in our basis, and define the fuction $g : H \to \mathbb{Q}$ by

$$g(a) = \begin{cases} 1 & \text{if } a = h \\ 0 & \text{else} \end{cases},$$

and extend g to a linear function $f : \mathbb{R} \to \mathbb{Q}$. Show that $f(\mathbb{R}^+) = \mathbb{Q}$.

(b) Is $\{x \in \mathbb{R}^+ : f(x) \geqslant 0\}$ closed under addition? Finish the proof. Did you use (a)?

April Fools Problem Set #17

E1. A function $f : \mathbb{R} \to \mathbb{R}$ is *linear* if $f(\alpha x + \beta y) = \alpha f(x) + \beta f(y)$, for any $\alpha, \beta, x, y \in \mathbb{R}$. Find a function $f : \mathbb{R} \to \mathbb{R}$ satisfying $f(x + y) = f(x) + f(y)$ that is not linear.

E2. Let n be a positive integer. Consider the sequence (a_k) defined as follows: we let $a_1 = n$. Then for any $k > 1$, we set

$$a_k = \begin{cases} \frac{a_{k-1}}{2} & \text{if } a_{k-1} \text{ is even} \\ 3a_{k-1} + 1 & \text{if } a_{k-1} \text{ is odd} \end{cases}$$

Show that eventually, this sequence will reach 1.
(This one should be quick).

E3. Show that any map of countries can be colored with 4 colors, such that no two countries sharing a boundary receive the same color.
(This one is slightly computational, you may need to use the back of this worksheet).

Extra Problem Set #18

Definition. Define $\binom{n}{k}$, pronounced "n choose k," to be the number of subsets of $\{1, \ldots, n\}$ of size k.

E1. How many subsets are there of $\{1, \ldots, n\}$?
[If you are stuck, answer the question for $n = 1, 2, 3$ and make a guess!]

E2. Use E1 to evaluate $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n}$.
[This may be relevant in the next question.]

E3. **Ehrenfest Gas Diffusion.** Suppose we have N gas particles in two chambers. There is a small opening through which particles can move from one chamber to the other. At time t, a particle is chosen uniformly at random, and that particle moves to the other chamber. For example, if there are 2 particles in Chamber 1 and $N - 2$ particles in Chamber 2, then with probability $\frac{2}{N}$, a particle moves from Chamber 1 to Chamber 2; and with probability $\frac{N-2}{N}$, a particle moves from Chamber 2 to Chamber 1.

Let state i be the state in which i particles are in Chamber 1. Find a (the?) steady-state vector of this Markov chain.
[You may want to consider small values of N first, and then make a conjecture.]

Extra Problem Set #19

Your classmate wants to send you an encrypted message. The encryption is as follows: first, you agree upon a 3×3 matrix A. We impose several conditions on A, so that if A is corrupted, we might be able to recover the original matrix. In particular, we require:

- A can be obtained from the identity by applying row-swaps and adding multiples of a row to a different row, and scaling rows by ± 1
- $\det A > 0$

Now we start with a message, say `I'm here`. Next, we represent the ith letter of the alphabet by the number i. So, our message is 9,13,8,5,18,5. Next, we put these numbers into vectors of length 3. Our message is then x_1, x_2, where

$$x_1 = \begin{bmatrix} 9 \\ 13 \\ 8 \end{bmatrix}, \; x_2 = \begin{bmatrix} 5 \\ 18 \\ 5 \end{bmatrix}.$$

If the number of letters is not divisible by 3, you can pad your message with 0s. Finally, your friend sends you the encoded message Ax_1, Ax_2. You can then recover the original message using your knowledge of A.

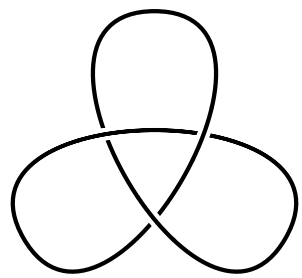
E1. You and your classmate agree upon the matrix $A = \begin{bmatrix} 0 & -1 & -1 \\ 1 & 1 & 0 \\ 0 & 0 & * \end{bmatrix}$. Unfortunately, the information was corrupted and you no longer know what the last entry $*$ is. The message you receive is

$$\begin{bmatrix} -5 \\ 11 \\ 4 \end{bmatrix}, \begin{bmatrix} -39 \\ 28 \\ 20 \end{bmatrix}, \begin{bmatrix} -7 \\ 13 \\ 2 \end{bmatrix}, \begin{bmatrix} -39 \\ 24 \\ 20 \end{bmatrix}, \begin{bmatrix} -6 \\ 21 \\ 5 \end{bmatrix}, \begin{bmatrix} -23 \\ 27 \\ 18 \end{bmatrix}.$$

Determine the original message.

Extra Problem Set #20

This worksheet concerns knots. Informally, a knot is a closed path in $\mathbb{R}^3$. Typically, knots are drawn as a projection onto $\mathbb{R}^2$, with crossings indicated by overlay. For example, here is a popular knot called the *trefoil*.



Such a drawing of a knot breaks the knot into strands. There are 3 strands in the knot above. A *3-coloring* of a knot is an assignment of colors to the strands of the knot, using at most 3 colors. A 3-coloring is called *valid* if for each crossing, the three incident strands have all different colors, or have the same color.

E1. Given colors Red, Blue, Green, how many valid 3-colorings does the trefoil have?

Let $\mathbb{Z}_3 = \{0, 1, 2\}$, with operations addition and multiplication modulo 3. I.e., the elements $a+b$ and ab are defined to be their remainders upone division by 3. So, $1+2=0$, and $2 \cdot 2 = 1$. Now let's color the strands of a knot using the colors 0,1,2.

E2. Show that the condition "at each crossing, all colors and the same or they are all different" is equivalent to the condition "at each crossing, the sum of the colors in $\mathbb{Z}_3$ is 0."

E3. A 3-coloring of a knot can be thought of as a vector in $\mathbb{Z}_3^r$, where r is the number of strands in the drawing of the knot. Show that the set of valid 3-colorings of a knot is a subspace of $\mathbb{Z}_3^r$.

E4. What does E3 imply about the number of valid 3-colorings of a knot?

Extra Problem Set #21

In this class, you have dealt entirely with the finite-dimensional vector spaces $\mathbb{R}^n$, for $n \in \mathbb{N}$. A question you should be asking yourselves is: which properties of finite-dimensional vector spaces extend to infinite-dimensional vector spaces?

E1. Let A, B be $n \times n$ matrices satisfying $AB = I$. Show that $BA = I$.
[In other words, right-inverses are left-inverses]

E2. Let $\mathcal{P}$ be the set of polynomials with real coefficients. Show that $\mathcal{P}$ is a real vector space (i.e., a vector space with $\mathbb{R}$ as scalars). Find a basis.

E3. Define functions $\mathcal{D}, \mathcal{I} : \mathcal{P} \to \mathcal{P}$ as follows:

$$\mathcal{D}(a_0 + a_1 x + \cdots a_k x^k) = a_1 + 2a_2 x + \cdots + k a_k x^{k-1}$$

and

$$\mathcal{I}(a_0 + a_1 x + \cdots a_k x^k) = a_0 x + \frac{a_1}{2} x^2 + \cdots + \frac{a_k}{k+1} x^{k+1} .$$

Show that $\mathcal{D}$ and $\mathcal{I}$ are linear transofmations.

E4. Is $\mathcal{D} \circ \mathcal{I}$ is the identity map? Is $\mathcal{I} \circ \mathcal{D}$? Compare with E1.

Extra Problem Set #22

Definition. A *partially ordered set*, or a *poset*, is a set A along with a relation $\preceq$, which satisfies the following conditions:

- For all $a \in A$, we have $a \preceq a$ ("reflexivity")
- If $a \preceq b$ and $b \preceq a$, then $a = b$ ("antisymmetry")
- If $a \preceq b$ and $b \preceq c$, then $a \preceq c$ ("transitivity")

A partially ordered set is called *totally ordered* if for every $a, b \in A$, either $a \preceq b$ or $b \preceq a$ (i.e., any two elements are comparable).

E1. Let U be any set, and let $\mathcal{P}(U)$ be the set of all subsets of U. Show that $\mathcal{P}(U)$ is a poset under the relation $\subseteq$. Is it totally ordered?

The following statement is unprovable using standard Zermelo-Fraenkel set theory axioms. However, it is provable if we also assume the axiom of choice.

Zorn's Lemma. Let P be a poset with relation $\preceq$, and suppose every totally ordered subset is bounded above. Then P has a maximal element.

E2. Prove that every vector space has a basis.

[Hint: use Zorn's Lemma to show the existence of a maximal linearly independent set. What can you say about such a set?]