Problem Set 1

The following exercises are open-ended and sometimes intentionally under-specified. You should always feel free to ask for help from the mentors (as well as from your fellow students). **Read all the exercises before beginning to work.**

In the first series of exercises, we will investigate how much you can simplify matrices using various kinds of row and column operations. Everything we will do this summer is built on these foundations. Assume that all matrices have entries in a fixed, arbitrary field F (if it helps, feel free to think about $\mathbb{R}$ or $\mathbb{C}$).

1. **Elementary, my dear Jordan.** (Do this first!) Prove that two matrices X, Y are related by a series of row operations if and only if there exists an invertible matrix A such that $AX = Y$. (The same is true for column operations and multiplying on the right).

2. **What does canonical mean, anyways?** Consider $k \times n$ matrices, with $k \leq n$ (k rows, n columns).

   (a) How much can you simplify such a matrix A using row operations? Can you put such a matrix in a best-possible "canonical form" up to these operations? Write down an explicit list of conditions specifying when a matrix is in canonical form.

   (b) Can you put any matrix into one of your canonical forms? Does any matrix have multiple canonical forms? Make some statements and prove them.

   (c) Now allow yourself to use both row and column operations. How much can you simplify your matrices now? Describe a canonical form for matrices up to these actions.

3. **Canon in B.** Let B denote the set of upper-triangular, invertible matrices in GL_2.

   (a) How much can you simplify an invertible 2x2 matrix using only left multiplication by elements of B? Can you describe a criterion for detecting when two matrices are related by such a left-multiplication?

   (b) Now allow yourself the ability to multiply on the left AND right by elements of B. Describe a canonical form for matrices up to this action. What about when $k = n$?

   (c) Can you generalize the result of part (b) to GL_3? GL_n? Make a precise conjecture and try to prove it.

4. **Field Observations.** "Recall" that there is a unique finite field $\mathbb{F}_q$ consisting of $q = p^e$ elements for some prime p and some $e \geq 1$. When $q = p$, $\mathbb{F}_p = \mathbb{Z}/p$. Otherwise, the finite fields can be constructed as the quotient of a polynomial ring:

$$\mathbb{F}_q = \mathbb{F}_p[x]/(f(x)),$$

   where $f \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree e.[1]

   (a) Give an example of a degree 3 irreducible polynomial over $\mathbb{F}_2$. Write out the multiplication table in $\mathbb{F}_8$.

[1] Remind me, why does this construction give a field?

(b) Give an example of a matrix with $\mathbb{F}_2$-coefficients whose characteristic polynomial is the polynomial you constructed in the previous part. Can you generalize? What can you say about eigenvalues and diagonalizability of this matrix?

5. **How do I span thee? Let me count the ways.** Let V be an n-dimensional vector space over the finite field $\mathbb{F}_q$, where $q = p^e$. How many subspaces of dimension k does V have? (Hint: first count how many bases a k-dimensional space has).

6. **I value you, despite your uncountably many holes.** Let F be an arbitrary field and consider the following function on single variable polynomials $p(x) = \sum_i a_i x^i \in F[x]$:

$$v(p) := \min\{i : a_i \neq 0\} \in \mathbb{N}.$$

So for example $v(1 + x^3) = 0$, $v(x^3 - 7x^4) = 3$, and $v(0) = \infty$.

(a) How does the function v behave under multiplication in the ring $F[x]$? How about under addition? Make precise claims and prove them.

(b) Define $|p(x)| = e^{-v(p)}$. Can you use this to define a distance function on $F[x]$? Does it deserve to be called a distance function? What properties does it have/not have that you would expect "distance" to have?

(c) Recall that a metric space (set with a distance function) is called *complete* if every Cauchy sequence converges. Is $F[x]$ complete with respect to the distance function you found above? If not, can you describe what kinds of Cauchy sequences don't have limits?

(d) Can you describe the *completion* of $F[x]$ with respect to this distance function? That is, can you find a ring B containing $F[x]$ as a subring, such that B has a distance function extending $|\cdot|$ and B is complete?