Math 55a Homework 3

Due Wednesday September 23, 2020.

- You are encouraged to discuss the homework problems with other students. However, what you hand in should reflect your own understanding of the material. You are NOT allowed to copy solutions from other students or other sources. Also, please list at the end of the problem set the sources you consulted and people you worked with on this assignment.
- Questions marked * may be on the harder side.

Material covered: Fields, vector spaces, bases and dimension, direct sums, linear maps. (Artin chapter 3 and 4.1-4.2 / Axler chapters 1, 2, 3.A-3.D).

0. Sometime over the weekend of September 19-20, please complete the week 3 feedback survey (in Canvas). This is important to help us assess how well the course structure, pacing, and our efforts at getting students to know each other are working. (There will be more surveys).

1. Let $V \subset \mathbb{R}[x]$ be the vector space of polynomials of degree at most 4 with coefficients in $\mathbb{R}$, $V = \{f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 \,|\, a_i \in \mathbb{R}\}$. Find bases for the following subspaces of V:

(a) $W_1 = \{f \in V \,|\, f(1) = f(2) = 0\}$,

(b) $W_2 = \{f \in V \,|\, f(1) = f(2)\}$,

(c) $W_3 = \{f \in V \,|\, \int_0^1 f(x)\,dx = 0\}$.

2. Let k be any field of characteristic $\mathrm{char}(k) \neq 2$, and let $T : k^n \to k^n$ be the linear map

$$(x_1, x_2, \ldots, x_n) \mapsto (x_1 + x_n, x_2 + x_{n-1}, \ldots, x_n + x_1).$$

What are the dimensions of the kernel and image of T? What changes if $\mathrm{char}(k) = 2$?

3. Let k be a field, and let M be the vector space of $n \times n$ matrices with entries in k. Let $S \subset M$ be the subspace of *symmetric* matrices, that is, matrices $A = (a_{i,j})$ such that $a_{i,j} = a_{j,i}\ \forall i, j$, and let $Q \subset M$ be the subspace of *skew-symmetric* matrices, that is, matrices $A = (a_{i,j})$ such that $a_{i,j} = -a_{j,i}\ \forall i, j$.

(a) Find the dimensions of S and Q.

(b) Show that if $\mathrm{char}(k) \neq 2$ then $M = S \oplus Q$.

(c) Show that this is false if $\mathrm{char}(k) = 2$.

4. (a) Find a field $\mathbb{F}_4$ with 4 elements! Namely, denote the elements by $\{0, 1, \alpha, \beta\}$ and write out the tables for addition and multiplication in $\mathbb{F}_4$.

(b) If we forget the multiplicative structure of $\mathbb{F}_4$ and just think of it as an abelian group, is it isomorphic to $\mathbb{Z}/4$ or $\mathbb{Z}/2 \times \mathbb{Z}/2$?

(c) Show that this is the unique field with 4 elements up to isomorphism.

5. Let V and W be vector spaces of dimensions m and n over a field k, and let $U \subset V$ and $T \subset W$ be subspaces of dimensions a and b, and let $S = \{\phi \in \mathrm{Hom}(V, W) \,|\, \phi(U) \subset T\}$.

(a) Show that S is a subspace of $\mathrm{Hom}(V, W)$.

(b) What is the dimension of S?

6. Let $\mathbb{R}^\infty = \{(a_0, a_1, a_2, \dots) \,|\, a_i \in \mathbb{R}\}$. Let $e_i = (0, \dots, 0, 1, 0, \dots) \in \mathbb{R}^\infty$ be the sequence with a 1 in the i-th place and all other terms zero, and let $w = (1, 1, \dots) \in \mathbb{R}^\infty$ be the sequence consisting entirely of 1's. Describe the span of the set $\{w, e_0, e_1, \dots\} \subset \mathbb{R}^\infty$.

7.* With $\mathbb{R}^\infty$ as above, and for $p \in \{1, 2, \dots\}$, let $\ell^p = \left\{(a_0, a_1, a_2, \dots) \in \mathbb{R}^\infty \;\middle|\; \sum_{i=0}^{\infty} |a_i|^p < \infty\right\}$.

(a) Show that ℓ^p is a subspace of $\mathbb{R}^\infty$.

(b) Show that ℓ^p is a proper subspace of ℓ^{p+1}.

8.* Let

$$0 \longrightarrow V_1 \xrightarrow{\phi_1} V_2 \xrightarrow{\phi_2} \cdots \xrightarrow{\phi_{n-2}} V_{n-1} \xrightarrow{\phi_{n-1}} V_n \longrightarrow 0$$

be an exact sequence of linear maps (i.e., $\mathrm{Im}(\phi_{i-1}) = \mathrm{Ker}(\phi_i)$ for all i). Show that if all the V_i are finite-dimensional, then

$$\sum_{i=1}^{n} (-1)^i \dim V_i = 0.$$

9.* (a) Let $k = \mathbb{F}_q$ be a finite field with q elements, and consider the 3-dimensional vector space $V = k^3$. How many one-dimensional subspaces (*lines through the origin*) are there in V? How many two-dimensional subspaces (*planes through the origin*) are there?

(b) How many lines through the origin does each plane contain? How many planes contain a given line through the origin?

(c) The party game "*Spot It!*" (also known as *Dobble* overseas) features 55 cards, each of which has eight symbols printed on it, in such a way that any two cards have exactly one symbol in common. (In the game, each player looks at a pair of cards and tries to find their common symbol.) The "Junior" version of the game has 30 cards with six symbols each. How do you use geometry over finite fields, as in parts (a)(b), to build decks of cards with the required property? (Note: *Spot It* decks don't quite have the optimal number of cards.)

10.* (Optional, extra credit) (Finite geometry and perfect difference sets)[1]

A *perfect difference set* is a subset $S = \{s_0, \dots, s_q\} \subset \mathbb{Z}/N$ such that each non-zero element of $\mathbb{Z}/N$ occurs *exactly once* as the difference $s_i - s_j$ $(i, j \in \{0, \dots, q\},\ i \neq j)$ of two distinct elements of S. (In particular, $N = q^2 + q + 1$.) Example: $S = \{0, 1, 3\} \subset \mathbb{Z}/7$. (Optional: find examples of perfect difference sets in $\mathbb{Z}/13$ and $\mathbb{Z}/21$). This problem describes a systematic construction discovered by J. Singer in 1938.

As in the previous problem, let $k = \mathbb{F}_q$ be a finite field with q elements, and let V be a 3-dimensional vector space over k. The key ingredient in Singer's construction is the following:

[1] Besides being a neat piece of recreational mathematics, perfect difference sets (and the more general notion of cyclic difference sets) have real-world applications to error-correcting codes and to radar technology!

Theorem. *There exists an invertible linear transformation $f : V \to V$ which acts on the set of lines through the origin (one-dimensional subspaces) in V by a cyclic permutation, so all lines occur as the successive images of any given line $L_0 = L \subset V$: denoting by N the number of lines in V, the assignment $j \mapsto L_j = f^j(L)$ defines a bijection from $\mathbb{Z}/N$ to the set of lines in V. Moreover, f acts in the same manner on the set of planes (two-dimensional subspaces) in V, with all planes arising as the successive images $P_j = f^j(P)$ of any given plane $P_0 = P \subset V$ under iterates of f.*

(a) Assuming the theorem holds, show that $S = \{j \in \mathbb{Z}/N \mid L_j \subset P_0\}$ is a perfect difference set.

(b) We now prove the theorem. Let $p(x) = x^3 - ax^2 - bx - c \in k[x]$ be a degree 3 polynomial which has no roots in k, and let $K = k[x]/(p)$, i.e. the 3-dimensional vector space of polynomials of degree ≤ 2 with coefficients in k, with a multiplication operation defined by taking the product of two polynomials and taking the remainder mod $p(x)$ (i.e., replacing x^3 by $ax^2 + bx + c$, and x^4 by $a(ax^2 + bx + c) + bx^2 + cx$).

We will be using, without proof, two classical facts of field theory (take Math 123!):

(1) K is a field (containing k as a subfield);

(2) the multiplicative group of non-zero elements of any finite field is cyclic.

Let α be a generator of the multiplicative group K^* of non-zero elements of K. Show that multiplication by α, viewed as a linear map $f : K \to K$, has the properties of Theorem 1.

(Hint: take the line L_0 to be the subspace of constant polynomials, i.e. $k \subset K$; which powers of α are elements of k? take the plane P_0 to be the subspace of polynomials of degree ≤ 1, i.e. the span of 1 and x).

11. How long did this assignment take you? How hard was it? What resources did you use, and how much help did you need? (Remember to list the students you collaborated with on this assignment.) Did you have any prior experience with this material?