Math 55a: Honors Abstract Algebra

Homework Assignment #3 (15 September 2017):
Linear Algebra III

> The expression δ_{ij} is called the Kronecker delta (after the mathematician Leopold Kronecker [1823–1891], who made more substantial contributions to mathematics than this).[1]
> — Corwin and Szczarba, *Calculus in Vector Spaces*, p.124

A bit more about the structure of infinite-dimensional vector spaces:

1. i) Prove that a vector space with a countable[2] spanning set over a countable field is countable.
   ii) Prove that a vector space with a countable spanning set over any field does not have an uncountable linearly independent set.
   iii) Prove that if a vector space V has a countable spanning set S then some subset of S is a basis for V.

2. Suppose V is a vector space and U a subspace with basis B_0. Suppose that for some (finite) n we can extend B_0 by n vectors to obtain a basis for V. Prove that if B is any basis for U, and B' any basis for V that contains B, then $\{v \in B' : v \notin B\}$ has cardinality n. U, and thus also V, is finite dimensional), once we've shown that the dimension is well-defined when finite; but the point is that the result still holds without that assumption.]

Some basics about linear transformations and their matrices:

3.–4. Solve Exercises B-11 (page 68) and D-9, 10, 16 (page 89) from Chapter 3 of the textbook. For B-11, if $S_1 \cdots S_n$ is injective, what if anything can be said of $S_1, S_2, \ldots, S_n$? For the other three exercises, note that "$\mathcal{L}(V)$" is Axler's abbreviation for "$\mathcal{L}(V, V)$" (it is also known as $\mathrm{End}(V) = \mathrm{Hom}(V, V)$).

5. Let $\mathcal{P}_n$ be the ($\mathbf{R}$- or $\mathbf{C}$-)vector space of polynomials of degree at most n, and $L : \mathcal{P}_n \to \mathcal{P}_n$ be the linear transformation taking any polynomial $P(x)$ to the polynomial
$$(L(P))(x) = (x - 3)P''(x)$$
(here P'' is the second derivative d^2P/dx^2). Exhibit a matrix for L relative to a suitable basis for $\mathcal{P}_n$, and determine the kernel, image, and rank of L.

---

[1] It is the (i, j) entry of an identity matrix, that is, $\delta_{ij} = 1$ if $i = j$ and 0 otherwise; also $\delta_{ij} = \varphi_j(v_i)$ where $(v_i)_{i=1}^n$ is a basis for a finite-dimensional vector space, and $(\varphi_j)_{j=1}^n$ its dual basis, see 3.96 on page 102.

[2] For us "countable" means "finite or countably infinite".

6. Let V, W be arbitrary vector spaces over the same field. Show that, for any vector v in V, the evaluation map $E_v : \mathcal{L}(V, W) \to W$ defined by $E_v(L) = L(v)$ for all $L \in \mathcal{L}(V, W)$ is a linear transformation. If V, W are finite dimensional, what is the dimension of $\ker E_v$?

7. Let V, W be vector spaces <u>over the rational field</u> $\mathbf{Q}$. Prove that a map $T : V \to W$ is linear if and only if $T(v + v') = Tv + Tv'$ for all $v, v' \in V$. (Cf. the italicized note to Exercise 9 on p.58 of the textbook.)

More about duality:

8. We saw that, for any vector spaces V, W, the dual of $V \oplus W$ is naturally identified with $V^* \oplus W^*$. What is the dual of $\oplus_{i \in I} V_i$? Use this to construct a vector space V over some field F such that V is <u>not</u> isomorphic with V^*.

9. Let $x_0, \ldots, x_m$ be distinct elements of F. Recall that the $m + 1$ vectors $v_i := (x_0^i, x_1^i, \ldots, x_m^i)$ $(0 \leq i \leq m)$ constitute a basis of F^{m+1}. Describe the dual basis.

10. Finally, suppose F is a finite field of q elements, and let e be a positive integer such that $2e < q$. Then we can regard $\mathcal{P}_{q-2e}$ as a subspace of F^F by evaluation at the elements of F. Call this subspace U. Show that for any $v \in V$ there is at most one $u \in U$ that differs from v in fewer than e coordinates; that is, there is at most one polynomial $P \in \mathcal{P}_{q-2e}$ such that $P(x) \neq v_x$ holds for fewer than e elements $x \in F$. Suppose such P exists and is nonzero, and let $d < e$ be the number of $x \in F$ such that $P(x) \neq v_x$. Prove that d is also the smallest integer n such that the intersection of $\mathcal{P}_{q-2e+d}$ with the vector space

$$\mathcal{P}_d \, v := \{Pv : P \in \mathcal{P}_d\}$$

contains some vector $w \neq 0$. Explain how this can be used to recover u in fewer than q calculations of such w.

(The point of this is that each such calculation can be done "in polynomial time" [i.e. there exist C and k such that the calculation requires at most Cq^k field operations in F, regardless of what q, e, v might be — one way to do this is "Gaussian elimination"]; while trying all e-element subsets of F certainly cannot be done in polynomial time. Of course the exceptional case $u = P = 0$ *can* be detected in polynomial time.)

Problem set is due Friday, Sep. 22 in class.