Lior Silberman’s Math 223: Problem Set 2 (due 26/1/2022)

Practice problems (recommended, but do not submit)

• Study the method of solving linear equations introduced in section 1.4 and use it to solve problem 2 of section 1.4.
• Section 1.4, problems 1-5 (ignore matrices), 8, 12-13, 17-19.
• Section 1.5, problems 1, 2 (ignore matrices), 4, 9, 10

M1. For each vector in the set \( S = \{ (0, 0, 0, 0), (0, 0, 3, 0), (1, 1, 0, 1), (2, 2, 0, 0), (0, 0, 0, -1) \} \subseteq \mathbb{R}^4 \) decide whether that vector is dependent or independent of the other vectors in \( S \).

M2. In the space of 2x2 matrices, is the matrix \( \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \) linearly dependent on the set \( \{ \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 5 & 3 \\ 7 & 6 \end{pmatrix}, \begin{pmatrix} -1 & -2 \\ -2 & -4 \end{pmatrix} \} \)? If it is, express it as a linear combination.

Linear dependence and independence

1. Let \( u = \begin{pmatrix} a \\ b \end{pmatrix}, v = \begin{pmatrix} c \\ d \end{pmatrix} \in \mathbb{R}^2 \) and suppose that \( u \neq 0 \). Show that \( v \) depends linearly on \( u \) iff \( ad - bc = 0 \).

2. In each of the following problems either exhibit the given vector as a linear combination of elements of the set or show that this is impossible (cf. PS1 problem M1).
   
   (a) \( V = \mathbb{R}^3, S = \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}, v = \begin{pmatrix} -4 \\ -2 \\ 0 \end{pmatrix} \) (b) Same \( V, S \) but \( v = \begin{pmatrix} -4 \\ -2 \\ -2 \end{pmatrix} \).
   
   (c) \( V = \mathbb{R}^2, S = \left\{ \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix} \right\} \) such that \( ad - bc \neq 0 \), \( v = \begin{pmatrix} e \\ f \end{pmatrix} \).

*3. The support of a function \( f \in \mathbb{R}^X \) is the set \( \text{supp } f = \{ x \in X \mid f(x) \neq 0 \} \) (note that we are doing algebra here; in analysis the set \( X \) would have some kind of topology and the support would be defined as the closure of the subset we consider). Let \( S \subseteq \mathbb{R}^X \) be a set of non-zero functions of disjoint supports, in that \( \text{supp } f \cap \text{supp } g = \emptyset \) if \( f, g \in S \) are distinct. Show that \( S \) is linearly independent.
   
   Hint: suppose linear combination of functions from \( S \) is zero and evaluate this combination carefully chosen points \( x \in X \).

   
   (a) Let \( W = \text{Span}(S) \) where \( S \) is as in 2(a). Identify \( W \subseteq \mathbb{R}^3 \) as the set of triples which satisfy a single equation in three variables.
   
   (b) Let \( T = \{ x^{k+1} - x^k \}_{k=0}^{\infty} \subseteq \mathbb{R}[x] \). Show that \( \text{Span}(T) \subseteq \{ p \in \mathbb{R}[x] \mid p(1) = 0 \} \).
   
   (*c) Show equality in (b).
   
   (b) Let \( R = \{ 2 + x^k \}_{k=1}^{\infty} \subseteq \mathbb{R}[x] \) (that is, \( R \) is the set of polynomials \( 2 + x, 2 + x^2, 2 + x^3, \cdots \)). Show that this set is linearly independent.
   
   (*e) Give (with proof)! a simple criterion, similar to the one in part (b), for whether a polynomial is in \( \text{Span}(R) \).

*5. Let \( V \) be a vector space, \( S \subseteq V \) a non-empty subset, and let \( w \in V \). Show that the following are equivalent: (1) \( w \in \text{Span}(S) \); (2) \( \text{Span}(S + w) \subset \text{Span}(S) \). Here \( S + w = \{ v + w \mid v \in S \} \) is the translation of \( S \) by \( w \).
**Challenge: The “minimal dependent subset” trick**

The following result (C1(d)) is a uniqueness result, very handy in proving linear independence.

C1. Let $V$ be a vector space, and let $S \subset V$ be linearly dependent.

(a) Show that $S$ contains a finite subset which is linearly dependent (this is a test of understanding the definitions)

Now let $S' \subset S$ be a linearly dependent subset of the smallest possible size, and enumerate its elements as $S' = \{v_i\}_{i=1}^n$ (so $n$ is the size of $S'$ and the $v_i$ are distinct).

(b) By definition of linear dependence there are scalars $\{a_i\}_{i=1}^n \subset \mathbb{R}$ not all zero so that $\sum_{i=1}^n a_i v_i = 0$. Show that all the $a_i$ are non-zero.

(c) Conclude from (b) that every vector of $S'$ depends on the other vectors.

(d) Suppose that there existed other scalars $b_i$ so that also $\sum_{i=1}^n b_i v_i = 0$. Show that there is a single scalar $t$ such that $b_i = ta_i$ for all $1 \leq i \leq n$.

C2. (hint: differentiation might help here!)

(a) Show that the set of functions $\{x^a\}_{a \in \mathbb{R}}$ is independent in $\mathbb{R}^{(0,\infty)}$.

(b) Fix $a < b$ and consider the infinite set $\{\cos(rx), \sin(rx)\}_{r>0} \cup \{1\}$ of functions on $[a, b]$ (you can treat 1 as the function $\cos(0x)$). Show that this set is linearly independent.

**Challenge: Independence in direct sums**

C3 Before thinking more about direct sums, meditate on the following: by breaking every vector in $\mathbb{R}^{n+m}$ into its first $n$ and last $m$ coordinates, you can identify $\mathbb{R}^{n+m}$ with $\mathbb{R}^n \oplus \mathbb{R}^m$. Now do the same problem twice:

(a) Let $n, m \geq 1$ and let $S_1, S_2 \subset \mathbb{R}^{n+m}$ be two linearly independent subsets. Suppose that every vector in $S_1$ is supported in the first $n$ coordinates, and that every vector in $S_2$ is supported in the last $m$ coordinates. Show that $S_1 \cup S_2$ is also linearly independent. If $n = 2, m = 1$ this means that vectors from $S_1$ look like $\begin{pmatrix} \ast \\ \ast \\ 0 \end{pmatrix}$ and vectors in $S_2$ look like $\begin{pmatrix} 0 \\ 0 \\ \ast \end{pmatrix}$.

(b) Let $V, W$ be two vector spaces. Let $S_1 \subset V$ and $S_2 \subset W$ be linearly independent. Show that $\{(y, 0) \mid y \in S_1\} \cup \{(0, w) \mid w \in S_2\}$ is linearly independent in $V \oplus W$.

RMK To understand every problem about direct sums consider it first in setting of part (a). Then try the general case.
Supplementary problem: another construction

A. (Quotient vector spaces) Let \( V \) be a vector space, \( W \) a subspace.

(a) Define a relation \( \cdot \equiv \cdot (W) \) (read “congruent mod \( W \)”) on \( V \) by \( \overline{v} \equiv \overline{v'} (W) \iff (v - v') \in W \). Show that this relation is an equivalence relation, that is that it is reflexive, symmetric and transitive.

(b) For a vector \( v \in V \) let \( v + W \) denote the set of sums \( \{v + w \mid w \in W\} \). Show that \( v + W = v' + W \iff v - v' \in W \). In particular show that if \( v' \in v + W \) then \( v' + W = v + W \). These subsets are the equivalent classes of the relation from part (a) and are called cosets mod \( W \) or affine subspaces.

(c) Show that if \( \overline{v} \equiv \overline{v'} (W) \) and \( u \equiv u' (W) \) and \( a, b \in \mathbb{R} \) then \( av + bu \equiv av' + bu' (W) \).

DEF Let \( V/W = \{v + W \mid v \in V\} \) be the set of cosets mod \( W \). Define addition and scalar multiplication on \( V/W \) by \( (v + W) + (u + W) = (v + u) + W \) and \( a(v + W) = av + W \).

(d) Use (c) to show that the operation is well-defined – that if \( v + W = v' + W \) and \( u + W = u' + W \) then \( (v + u) + W = (v' + u') + W \) so that the sum of two cosets comes out the same no matter which vector is chosen to represent the coset.

(e) Show that \( V/W \) with these operations is a vector space, known as the quotient vector space \( V/W \).

Supplementary problems: finite fields

Let \( p \) be a prime number. Define addition and multiplication on \( \{0, 1, \ldots, p - 1\} \) as follows: \( a + p b = c \) and \( a \cdot p b = d \) if \( c \) (resp. \( d \)) is the remainder obtained when dividing \( a + b \) (resp. \( ab \)) by \( p \). For example if \( p = 7 \) we have \( 5 + 7 = 4 \) and \( 5 \cdot 7 = 2 \) because \( 11 = 1 \cdot 7 + 4 \) and \( 30 = 4 \cdot 7 + 2 \).

B. (Elementary calculations)

(a) Show that these operations are associative and commutative, that 0 is neutral for addition, that 1 is neutral for multiplication.

(b) Show that if \( 1 < a < p \) then \( a + p (p - a) = 0 \), and conclude that additive inverses exist in this system.

(c) Show that the distributive law holds.

(d) Show that for every integer \( n \), \( n^p - n \) is divisible by \( p \).

\text{Hint:} Induction on \( n \), using the binomial formula and that \( p | \binom{p}{k} \) if \( 0 < k < p \).

(e) Show that for every integer \( a \), if \( 1 \leq a \leq p - 1 \) then \( p | a^{p-1} - 1 \).

\text{Hint:} If \( p | xy \) but \( p \nmid x \) then \( p \nmid y \).

(f) Show that for every integer \( a \), \( 1 \leq a \leq p - 1 \), \( a^{p-1} = 1 \) if we exponentiation means repeated \( \cdot p \) rather than repeated \( \cdot \). 

(g) Conclude that every \( 1 \leq a \leq p - 1 \) has a multiplicative inverse.

\text{DEFINITION.} The field defined in problem B is called “the field with \( p \) elements” or “\( \mathbb{F} p \)” and denoted \( \mathbb{F} p \).

\text{REMARK.} A better version of this problem relies on a construction like problem A. For integers \( a, b \in \mathbb{Z} \) define \( a \equiv b (p) \) if \( a - b \) is divisible by \( p \) (and say “\( a \) is congruent to \( b \) mod \( p \)”), and write \( \mathbb{Z}/p\mathbb{Z} \) for the set of equivalence classes. First one shows that there are \( p \) such classes, with representatives \( \{0, 1, \ldots, p - 1\} \) (this connects this argument to the one used in problem B). Following the same steps as in problem A we can endow \( \mathbb{Z}/p\mathbb{Z} \) with addition and multiplication operations coming from the integers and deduces the laws of arithmetic from those in \( \mathbb{Z} \). So far this makes sense for any integer \( p \), and now problems B(d) through B(g) prove that this is a field.

C. Let \( (V, +) \) be set with an operation, and suppose all the axioms for addition in a vector space hold. Suppose that for every \( v \in V \), \( \sum_{i=1}^{p} v = 0 \) (i.e. if you add \( p \) copies of the same vector you always get zero). Define \( av = \sum_{i=1}^{a} v \) for all \( 0 \leq a < p \) and show that this endows \( V \) with the structure of a vector space over \( \mathbb{F} p \).