Math 223: Problem Set 2 (due 25/1/2021)

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

Linear dependence and independence

1. Let $\underline{u} = \begin{pmatrix} a \\ b \end{pmatrix}, \underline{v} = \begin{pmatrix} c \\ d \end{pmatrix} \in \mathbb{R}^2$ and suppose that $\underline{u} \neq \underline{0}$. Show that $\underline{v}$ is not dependent on $\underline{u}$ iff $ad - bc \neq 0$.

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 2).
   (a) $V = \mathbb{R}^3$, $S = \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \right\}$, $\underline{v} = \begin{pmatrix} -4 \\ -2 \\ 0 \end{pmatrix}$ (b) Same V, S but $\underline{v} = \begin{pmatrix} -4 \\ -2 \\ -2 \end{pmatrix}$.
   (c) $V = \mathbb{R}^2$, $S = \left\{ \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix} \right\}$ such that $ad - bc \neq 0$, $\underline{v} = \begin{pmatrix} e \\ f \end{pmatrix}$.

3. More on spans.
   (a) Let $W = \mathrm{Span}(S)$ where S is as in 2(a). Identify W as the set of triples which solve a single equation in three variables.
   (b) Let $T = \left\{ x^{k+1} - x^k \right\}_{k=0}^{\infty} \subset \mathbb{R}[x]$. Show that $\mathrm{Span}(T) \subset \{ p \in \mathbb{R}[x] \mid p(1) = 0 \}$.
   (*c) Show equality in (b).
   (d) Let $R = \left\{ 1 + x^k \right\}_{k=1}^{\infty} \subset \mathbb{R}[x]$ (that is, R is the set of polynomials $1+x, 1+x^2, 1+x^3, \cdots$). 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 $\mathrm{Span}(S)$.

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

*5. Let $S \subset \mathbb{R}[x]$ be a set of non-zero polynomials, no two of which have the same degree. Show that S is linearly independent.

The "minimal dependent subset" trick

The following result (6(d)) is a *uniqueness* result, very handy in proving linear independence.

6. Let V be a vector space, and let $S \subset V$ be linearly dependent. Let $S' \subset S$ be a linearly dependent subset of the smallest possible size, and enumerate its elements as $S' = \{\underline{v}_i\}_{i=1}^{n}$ (so n is the size of S' and the $\underline{v}_i$ are distinct, in particular $n \geq 1$).
   (a) Show that S contains a finite subset which is linearly dependent (this is a test of understanding the definitions)
   RMK Part (a) justifies the existence of S'.
   (b) By definition of linear dependence there are scalars $\{a_i\}_{i=1}^{n} \subset \mathbb{R}$ not all zero so that $\sum_{i=1}^{n} a_i \underline{v}_i = \underline{0}$. 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 $\sum_{i=1}^{n} b_i \underline{v}_i = \underline{0}$. Show that there is a single scalar t such that $b_i = t a_i$ for all $1 \leq i \leq n$.

**7. (Linear independence of functions) Some differential calculus will be used here.
   (a) Let $r_1, \ldots, r_n$ be distinct real numbers. Show that the set of functions $\{e^{r_i x}\}_{i=1}^{n}$ is independent in $\mathbb{R}^{\mathbb{R}}$.
   (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.

Supplementary problem: Independence in direct sums

A 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 $\begin{pmatrix} * \\ * \\ 0 \end{pmatrix}$ and vectors in S_2 look like $\begin{pmatrix} 0 \\ 0 \\ * \end{pmatrix}$.
   (b) Let V, W be two vector spaces. Let $S_1 \subset V$ and $S_2 \subset W$ be linearly independent. Show that $\{(\underline{v}, 0) \mid \underline{v} \in S_1\} \cup \{(0, \underline{w}) \mid \underline{w} \in S_2\}$ 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.

Hint for 5: (1) In a linear combination of polynomials from S, consider the polynomial of highest degree appearing with a non-zero coefficient. (2) Try to see what happens if $S = \left\{1+1, 1+x, 1+x^2\right\}$.

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 $\underline{v} \equiv \underline{v}'\,(W) \iff (\underline{v}-\underline{v}') \in W$. Show that this relation is an *equivalence relation*, that is that it is reflexive, symmetric and transitive.
   (b) For a vector $\underline{v} \in V$ let $\underline{v}+W$ denote the set of sums $\{\underline{v}+\underline{w} \mid \underline{w} \in W\}$. Show that $\underline{v}+W = \underline{v}'+W$ iff $\underline{v}+W \cap \underline{v}'+W \neq \emptyset$ iff $\underline{v}-\underline{v}' \in W$. In particular show that if $\underline{v}' \in \underline{v}+W$ then $\underline{v}'+W = \underline{v}+W$. These subsets are the equivalence classes of the relation from part (a) and are called *cosets* mod W or *affine subspaces.*
   (c) Show that if $\underline{v} \equiv \underline{v}'\,(W)$ and $\underline{u} \equiv \underline{u}'\,(W)$ and $a, b \in \mathbb{R}$ then $a\underline{v}+b\underline{u} \equiv a\underline{v}'+b\underline{u}'\,(W)$.
   DEF Let $V/W = \{\underline{v}+W \mid \underline{v} \in V\}$ be the set of cosets mod W. Define addition and scalar multiplication on V/W by $(\underline{v}+W)+(\underline{u}+W) \stackrel{\text{def}}{=} (\underline{v}+\underline{u})+W$ and $a\,(\underline{v}+W) \stackrel{\text{def}}{=} (a\underline{v})+W$.
   (d) Use (c) to show that the operation is *well-defined* – that if $\underline{v}+W = \underline{v}'+W$ and $\underline{u}+W = \underline{u}'+W$ then $(\underline{v}+\underline{u})+W = (\underline{v}'+\underline{u}')+W$ 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 $\{0, 1, \cdots, p-1\}$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.

B. (Elementary calculations)
   (a) Show that these operations are associative and commutative, that 0 is neutral for addition, that 1 is netural 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.
   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 $1 \le a \le p-1$ then $p | a^{p-1} - 1$.
   Hint: If $p|xy$ but $p \nmid x$ then $p|y$.
   (f) Show that for every integer a, $1 \le a \le p-1$, $a^{p-1} = 1$ if we exponentiation means repeated $\cdot_p$ rather than repeated $\cdot$.
   (g) Conclude that every $1 \le a \le p-1$ has a multiplicative inverse.

DEFINITION. The field defined in problem B is called "the field with p elements" or "F p" and denoted $\mathbb{F}_p$.

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