Math 309 – Intermediate Linear Algebra Homework 4 Xida Ren

(Due Friday, February 23)

Each problem will be graded out of 10 points.

1. Find a degree 3 polynomial f with coefficients in $\mathbb{Q}$ such that $f(0) = 1$, $f(1) = 3$, $f(2) = 2$, and $f(3) = 15$.

Proof. We're looking for a vector b such that

$$Mb = v$$

where

$$v = \begin{bmatrix} 1 \\ 3 \\ 2 \\ 15 \end{bmatrix}$$

and

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 \\ 1 & 3 & 9 & 27 \end{bmatrix}$$

Sympy tells us that

$$b = \begin{bmatrix} 1 \\ 55/6 \\ -10 \\ 17/6 \end{bmatrix}$$

So the polynomial is $1 + \frac{55}{6}x - 10x^2 + \frac{17}{6}x^3$. □

2. Let $\mathbb{F}$ be a finite field and $n + 1 \leqslant |\mathbb{F}|$. If $c_0, c_1, \ldots, c_n$ are distinct elements in $\mathbb{F}$, given $b_0, b_1, \ldots, b_n \in \mathbb{F}$ (not necessarily distinct), must there exist a unique polynomial f in $\mathbb{F}[x]$ of degree at most n (i.e., in $P_n(\mathbb{F})$) such that $f(c_i) = b_i$ for each i? Either prove it or provide a counterexample.

Proof. Existance is guaranteed by Larange interpolation: simply use the resulting polynomial. Because $0 * x = 0$ in any finite field, $f_i(c_j) = 0$ for $j \neq i$. Because a field has multiplicative inverses for nonzero elements and no zero divisors, $f_i(c_i) = \Pi_{j \neq i} \frac{x - c_j}{c_i - c_j} = 1$.
Uniqueness is guaranteed by the fact that the Larange Polynomials span $P_n\mathbb{F}$.
First, we observe that $Q \in P_n(\mathbb{F})$. Next, see that $Q(c_i) = 0$ for each c_i. But since the Larange polynomials are a basis of P_n, we know that Q is a linear combination of the

Larange polynomials. Furthermore, each Larange polynomial f_i is 0 at all c_j except when $j = i$. But this means that in the linear combination $Q = a_0 f_0 + \ldots + a_n f_n$ each a_i has to be 0 or else $Q(c_i) = a_i$ would not be 0. Thus $Q(x) = 0$ and is the zero polynomial.
So $P_1(x) = P_2(x)$ □

3. Prove that a vector space is infinite-dimensional if and only if it contains an infinite linearly independent set.

Proof. Suppose a vector space contains an infinitely large independant set. Suppose that the vector space is also finite-dimensional. Then by the replacement theorem the size of the basis is greater than or equal to the size of the independent set, which is impossible because the cardinality of an infinite set cannot be smaller than that of a finite set.
Suppose a vector space V is infinite-dimensional. This means that no finite set can span it. Now we construct a linearly independent set that contains as many vectors as there are natural numbers.
Let S_0 be the empty set.
For
Take an empty set. Call it S_0. Take one vector from $V \setminus \text{span}(S)$ and add it to S_0 to get S_1; repeat until S has more than n vectors. Because V is infinite-dimensional, it can never be spanned by S, so we can keep adding vectors from outside the span of S. Keep adding vectors for every natural number to arrive at S_∞ which has a one-to-one correspondance to the natural numbers, which is infinite. □

4. Let W_1 and W_2 be subspaces of a vector space V. If B_1 is a basis for W_1 and B_2 is a basis for W_2, prove that $V = W_1 \oplus W_2$ if and only if $B_1 \cap B_2 = \varnothing$ and $B_1 \cup B_2$ is a basis for V.

Proof. We first prove the if-direction.
Suppose B_1 and B_2 are independent sets with $B_1 \cap B_2 = \varnothing$ and $B_1 \cup B_2$ being a basis of V. By definition of $\oplus$, to prove $W_1 \oplus W_2 = V$ we have to prove that $W_1 \cap W_2 = \{0\}$ and $W_1 + W_2 = V$.
Consider any vector $v \in \text{span}(B_1 \cap B_2)$. v is in the spans of both B_1 and B_2, which means that if v is nonzero, then the multiset $B_1 \cup B_2$ is not linearly independent. If after removing duplicate elements $B_1 \cup B_2$ becomes linearly independent, $B_1 \cap B_2$ musn't be the empty set. Otherwise, the set $B_1 \cup B_2$ is not linearly independant and cannot be a basis of V.
Now we prove that $W_1 + W_2 = V$. Because $B_1 \cup B_2$ is a basis of V, any $v \in V$ can be represented as a linear combination of vectors in $B_1 \cup B_2$ like this: for $b_1, \ldots b_k \in B_1$ and $b_{k+1}, \ldots b_n$ where n is the total number of vectors in $B_1 \cup B_2$, $v = \sum_i c_i b_i$ for some coefficients $\{c_i\}$. Consider $v_1 = \sum_{i=0}^{k} c_i b_i$ and $v_2 = \sum_{i=k+1}^{n} c_i b_i$. $v_1 \in \text{span}(B_1)$ and $v_2 \in \text{span}(B_2)$. They add to v, so $v \in V$ implies $V \in W_1 + W_2$.
We now prove the only-if direction.
If $W_1 \cap W_2 = \{0\}$, W_1 and W_2 musn't share any nonzero vectors, or else any shared vector would appear in $W_1 \cap W_2$. Since the basis is always a subset of the span, $B_1 \cap B_2 \subseteq \{0\}$. No linearly independent set of vectors can contain 0 because it creates the linear combination $a \cdot 0 = 0$ for any a, so $B_1 \cap B_2 = \varnothing$.

$B_1 \cup B_2$ spans V because any vector in V can be written as the sum of two vectors in W_1 and W_2, and because the sum of two linear combinations of elements in $B_1 \cup B_2$ is a linear combination of elements in $B_1 \cup B_2$, any vector in V is in the span of $B_1 \cup B_2$.
$B_1 \cup B_2$ is linearly independant: if not, let $v_1 \dots v_k \in B_1 \cup B_2$. There exists a set of coefficients $a_1 \dots a_k$, some of which are nonzero, such that $\sum_{i=1}^{k} a_i v_i = 0$. Now, separate the terms to get a linear combination of B_1's terms on the left and a linear combination of B_2's terms on the right.
If both sides are all zero, then we started with all-zero coefficients, which is impossible given linearly dependent $B_1 \cup B_2$. If only one side has zero coefficients, that means that B_1 or B_2 is linearly dependant, violating our assumption that they are bases for W_1 and W_2.
If both sides have nonzero coefficients, then that means that the sum of each side is in $W_1 \cap W_2$, which is impossible because $W_1 \oplus W_2 = v$ implies that $W_1 \cap W_2 = \{0\}$. □

5. Let V be the set $\mathbb{R}$ of real numbers regarded as a vector space over $\mathbb{Q}$. Prove that V is infinite-dimensional.
HINT: You may assume that there are transcendental numbers, such as π, that are not a zero of any polynomial with rational coefficients.

Proof. Consider the set containing all nonnegative integer powers of π.
If it is linearly dependant, there must be a minimal n such that $\sum_{i=0}^{n} a_i \pi^i = 0$ where the coefficients $a_i \in \mathbb{Q}$ and the coefficient $a_n \neq 0$. But this means that π is a zero of a polynomial, giving contradiction.
So our set is a linearly independant subset of V. Because the set is as large as the natural nmubers, V is infinite-dimensional. □

6. Prove the following generalization of the Replacement Theorem: Let B be a basis for a vector space V, and let L be a linearly independent subset of V. Prove that there exists a subset B' of B such that $L \cup B'$ is a basis for V.

Proof. We prove this by Zorn's lemma, which states that each containment-ordered chain of sets in a family of sets has a maximal element if the family has an upper bound.
Consider the family of sets $F = \{S : S \subseteq B, S \cup L \text{is linearly independent}\}$.
Any containment chain in this family is bounded above by B, so there is at least one maximal element in this family. Take any one of these and call it M.
Now consider span$(M \cup L)$. It has to be a basis of V, or else M couldn't have been the maximal element of F.
If all elements of the basis B can be found in span$(M \cup L)$, we're done, because all $v \in V$ can be written as a linear combination of the basis and hence a linear combination of span$(M \cup L)$.
Otherwise, if there is an element $b \in B$ that is not in span$(M \cup L)$, we create a contradiction by adding it to M to create $M' = M \cup \{b\} \subseteq S$.
This undermines the maximality of M in F: First, $M' \cup L$ is necessarily an independent set, because we started out assuming that b is not in the span span$(M \cup L)$. Second, because $b \in B$ and $M \subseteq B$, $\{b\} \cup M \subseteq B$.

So $M' \in F$, and $M \subsetneq M'$ is a contradiction to the fact that M is the maximal element. Hence no $v \in V$ is outsite $\operatorname{span}(M \cup L)$, and there exists a set $M \subseteq B$ such that $M \cup L$ is a basis of V. □