Assignment 2A: Linear Spaces
Due Thursday September 17, 2026

John McCuan

In the following problems a **linear space** W over a field F is an Abelian group under addition for which there exists a scaling $\sigma : F \times W \to W$, with $\sigma(\mu, v)$ denoted μv for $\mu \in F$ and $v \in W$, and for which the following conditions hold:

(LS1) $(\mu_1\mu_2)v = \mu_1(\mu_2 v)$ for all $\mu_1, \mu_2 \in F$ and $v \in W$.

(LS2) $1v = v$ for every $v \in W$ where 1 is the multiplicative identity in F.

(LS3) $(\mu_1 + \mu_2)v = \mu_1 v + \mu_2 v$ for all $\mu_1, \mu_2 \in F$ and $v \in W$.

(LS4) $\mu(v_1 + v_2) = \mu v_1 + \mu v_2$ for all $\mu \in F$ and $v_1, v_2 \in W$.

Problem 1 Prove that in a linear space W over a field F there holds

$$0v = \mathbf{0}$$

where $0 \in F$ is the additive identity in the field, $v \in W$ is any element, and $\mathbf{0} \in W$ is the zero element in the linear space.

Problem 2 Consider the field $\mathbb{F}_2 = \{0, 1\}$ with two elements.

(a) Write down the addition and multiplication tables for $\mathbb{F}_2$. Hint $1 + 1 = 0$.

(b) Find the multiplicative group of invertible elements.

(c) Find $\mathbb{F}_2\backslash\{0\}$.

Problem 3 (cardinality) The empty set ϕ has no elements. The set $\{\phi\}$ has one element. The number of elements in a set S is called the **cardinality** of S and is denoted $\#(S)$.

(a) Find

$$\#\left(\quad \left\{\phi, \{\phi\}\right\} \quad \right).$$

(b) The quantity in part **(a)** may also be denoted more "compactly" by

$$\#\left\{\phi, \{\phi\}\right\}$$

where the round parentheses have been omitted. This is also the same thing as $\#\{\phi, \{\phi\}\}$. Find $\#\{\phi, \{\phi\}, \{\phi, \{\phi\}\}\}$.

Consider the following "standard" sets:

$$\begin{aligned}
S_1 &= \{\phi\} \\
S_2 &= \{\phi, S_1\} \\
S_3 &= \{\phi, S_1, S_2\} \\
&\vdots \\
S_n &= \{\phi\} \cup \{S_j : j = 1, 2, \ldots, n-1\} \\
&\vdots
\end{aligned}$$

These particular sets are also called **ordinal sets**,[1] and they provide a standard for determining the number of elements in certain sets. A set S is said to have **finite cardinality** and one writes $\#(S) < \infty$ if for some $n \in \mathbb{N} = \{1, 2, 3, \ldots\}$ there exists a bijection $\beta : S \to S_n$.

One also writes in this case $\#(S) = n$ and says the cardinality of S is n.

(c) Determine an appropriate natural number n and find a bijection $\beta : S \to S_n$ for the following sets S of finite cardinality:

(i) $S = \{m \in \mathbb{Z} : -500 < m < 1001\}$ (Remember $\mathbb{Z} = \{0, \pm1, \pm2, \pm3, \ldots\}$ denotes the integers.)

[1] ...or ordinal numbers. These are not all the standard ordinal **numbers**, but they are helpful for counting. If you want to count other quantities (i.e., determine other cardinalities) perhaps it will be helpful for you to learn additional ordinals.

(ii) $S = \{(m_1, m_2) \in \mathbb{Z}^2 : m_1^2 + m_2^2 < 5\}$. Remember $\mathbb{Z}^2 = \{(m_1, m_2) : m_1, m_z \in \mathbb{Z}\}$ denotes the set of ordered pairs of integers.

(iii) $S = \{(m_1, m_2, m_3) \in \mathbb{Z}^3 : m_1^2 + m_2^2 + m_3^2 < 5\}$.

Problem 4 A nonempty set S is said to have **infinite cardinality** if $\#(S)$ is not finite. A set S is said to be **countable** if there is a bijection $\beta : \mathbb{N} \to S$.

(a) Show $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$ is countable. That is, find a bijection $\beta : \mathbb{N}_0 \to \mathbb{N}$.

(b) Show $\mathbb{Z}$ is countable.

(c) Show $\mathbb{Z}^2$ is countable.

Problem 5 Given a field F, the **polynomial** ring $F[X]$ is defined by

$$F[X] = \left\{ \sum_{n=0}^{\infty} a_n X^n : F \ni a_0, a_1, a_2, a_3, \ldots \text{ and } \#\{n : a_n \neq 0\} < \infty \right\}.$$

A polynomial

$$\sum_{n=0}^{\infty} a_n X^n$$

in $F[X]$ is uniquely determined by the coefficients, that is, if

$$\sum_{n=0}^{\infty} a_n X^n \qquad \text{and} \qquad \sum_{n=0}^{\infty} b_n X^n$$

are polynomials in $F[X]$, then the **definition of equality** is

$$a_n = b_n \qquad \text{for} \qquad n = 0, 1, 2, 3, \ldots.$$

The **operation of addition** on $F[X]$ is defined by

$$\sum_{n=0}^{\infty} a_n X^n \quad + \quad \sum_{n=0}^{\infty} b_n X^n \quad = \quad \sum_{n=0}^{\infty} (a_n + b_n) X^n.$$

The **operation of multiplication** on $F[X]$ is defined by

$$\left(\sum_{n=0}^{\infty} a_n X^n \right) \left(\sum_{n=0}^{\infty} b_n X^n \right) \quad = \quad \sum_{n=0}^{\infty} \left(\sum_{\ell=0}^{n} a_\ell b_{n-\ell} \right) X^n.$$

The **scaling** of a polynomial by a scalar $\mu \in F$ is defined by

$$\mu \sum_{n=0}^{\infty} a_n X^n \quad = \quad \sum_{n=0}^{\infty} \mu a_n X^n.$$

The **scalars** $a_0, a_1, a_2, a_3, \ldots$ in F for a given polynomial

$$\sum_{n=0}^{\infty} a_n X^n$$

are called the **coefficients** of the polynomial. A polynomial

$$0X^0 + 0X^1 + \cdots + aX^k + 0X^{k+1} + 0X^{k+2} + \cdots$$

with only one nonzero coefficient a is called a **monomial** and may be written simply as

$$aX^k.$$

More generally a monomial $a_n X^n$ appearing in a polynomial

$$\sum_{n=0}^{\infty} a_n X^n$$

is called a **term** in the polynomial.

The following is a somewhat subtle point: The "formal symbol" X used in the definition of the polynomial ring $F[X]$ does not denote an element of F, so the term aX^n does not denote an operation combining a and X^n nor does the formal symbol X^n denote any operation(s) involving X. More properly, there are countably many formal symbols X^0, X^1, X^2, X^3,... involved in the definition of $F[X]$, but no algebraic operations are defined on the formal symbols independent of those defined on the polynomial ring $F[X]$ as described above. Nevertheless the following formal conventions in writing polynomials are usually employed:

(i) The formal symbol X^0 is often omitted. Technically, this does not mean $X^0 = 1$, though the coefficient of the term $1X^0$ is $1 \in F$, and the term may be written as 1 using only the coefficient.

(ii) If the coefficient in a term $a_n X^n$ is $0 \in F$, that is the coefficient $a_n = 0$ is the additive identity in F, then the entire term is often omitted.

(iii) The formal symbol X^1 is often denoted by X.

(iv) If $n > 0$ and the coefficient in a term $a_n X^n$ is $1 \in F$, that is the coefficient is the multiplicative identity in F, then the coefficient is omitted.

Using these conventions, the polynomials

$$1X^0 + 1X^1 + 0X^2 + 1X^3 + 0X^4 + 0X^5 + \cdots$$

and

$$1X^0 + 0X^1 + 0X^2 + 0X^3 + 0X^4 + 1X^5 + 0X^6 + 0X^7 + \cdots$$

may be expressed simply as

$$1 + X + X^3 \qquad \text{and} \qquad 1 + X^5.$$

Similarly, the zero polynomial is just written as 0 and for any other polynomial P in $F[X]\backslash\{0\}$ there is some k for which that polynomial can be written

$$P = \sum_{n=0}^{k} a_n X^n$$

with $a_k \neq 0$. For such a nonzero polynomial P, the **degree** is defined to be the number $k \in \mathbb{N}_0$ (for which $a_k \neq 0$ and $a_{k+1} = a_{k+2} = a_{k+3} = \cdots = 0$. Note I have not written $P(X)$ here using function notation, A (formal) polynomial in $F[X]$ is not a function.

(a) Show $F[X]$ is a linear space[2] over F.

A subset S of a linear space W over a field F is a **subspace** of W if the operations on W restricted to S, and the scaling of elements of W by elements of F restricted to S make S a linear space over F.

To see a subset S of a linear space W is a subspace of W requires the nominal verification of many conditions. One must show, first of all, the operation of addition on W restricted to S is an operation on S.

[2]In fact, $F[X]$ is isomorphic, i.e., linear isomorphic if one knows what that means, to the linear space $F_0^{\mathbb{N}}$ consisting of sequences $(a_1, a_2, a_3, \ldots)$ with $a_1, a_2, a_3, \ldots \in F$ with $\#\{n \in \mathbb{N} : a_n \neq 0\} < \infty$ and componentwise addition and scaling. The linear space $F_0^{\mathbb{N}}$ is a subspace of the linear space $F^{\mathbb{N}}$ of all sequences with entries in F. Note the familiar finite dimensional spaces like $\mathbb{R}^n$ and $\mathbb{C}^n$ are subspaces of $\mathbb{R}^{\mathbb{N}}$ and $\mathbb{C}^{\mathbb{N}}$.

(b) **(i)** Show for each $k \in \mathbb{N}$ the operation of multiplication on $F[X]$, when restricted to the subset

$$\left\{ \sum_{n=0}^{\infty} a_n X^n \in F[X] : a_{k+1} = a_{k+2} = a_{k+3} = \cdots = 0 \right\} \tag{1}$$

is **not** an operation on this subset. What about when $k = 0$?

Hint: If you have trouble with this part **(i)**, go on to part **(ii)** and come back to this part.

(ii) Show the operation of addition when restricted to

$$\left\{ \sum_{n=0}^{\infty} a_n X^n \in F[X] : a_{k+1} = a_{k+2} = a_{k+3} = \cdots = 0 \right\}$$

is an operation on the subset.

Polynomials in the subset of $F[X]$ appearing in (1) are called **polynomials of order no more than** k, and the set is denoted by

$$F_k[X] = \left\{ \sum_{n=0}^{\infty} a_n X^n \in F[X] : a_{k+1} = a_{k+2} = a_{k+3} = \cdots = 0 \right\}.$$

Note $F_k[X] \times F_k[X]$ is a subset of $F[X] \times F[X]$, so it makes sense to restrict the addition of polynomials to $F_k[X]$:

$$+ : F_k[X] \times F_k[X] \to F[X].$$

The question you must ask yourself here is the following: When two polynomials P_1 and P_2 in $F_k[X]$ are added using the addition in $F[X]$, one knows from part **(a)** above that the sum $P_1 + P_2$ is in $F[X]$, but is it true that $P_1 + P_2 \in F_k[X]$ so that the codomain of the addition may also be made smaller

$$+ : F_k[X] \times F_k[X] \to F_k[X] \qquad ?$$

(Note the answer was "no" in part **(i)** just above for multiplication.)

Part **(ii)** just above is the verifiction that the operation of addition is **closed** on $F_k[X]$. One also says simply that the subset $F_k[X]$ is **closed** under addition.

(iii) Verify the addition $+ : F_k[X] \times F_k[X] \to F_k[X]$ makes $F_k[X]$ an Abelian group. Hint: The field F is an Abelian group.

The next step in the verification that $F_k[X]$ is a subspace of $F[X]$ is showing the scaling on $F[X]$ when restricted to $F_k[X]$ gives a scaling by elements of the field F on $F_k[X]$, that is $F_k[X]$ is **closed under scaling**. When that is done, one still needs to verify conditions **(LS1)**, **(LS2)**, **(LS3)**, **(LS4)** in the definition of a linear space given above.

(iv) Show that in general if a subset S of a linear space W is nonempty, closed under addition and closed under scaling, then S is a subspace of W.

(c) Is $F_k[X]$ a ring?

Problem 6 (finite and infinite dimension) From Problem 5 above, you should be familiar with (or at least know about) the linear space $F[X]$ of polynomials with coefficients in a field F and the subsepace $F_k[X]$ for $k \in \mathbb{N}$.

(a) Find $k+1$ polynomials $P_0, P_1, P_2, \dots, P_k$ in $F_k[X]$ for which every polynomial $P \in F_k[X]$ may be expressed as

$$P = \sum_{\ell=0}^{k} b_\ell P_\ell. \tag{2}$$

(b) Are the polynomials you found in part **(a)** above unique? That is, are they the only polynomials you might have found?

An expression like that contained in (2) is called a **linear combination** of the polynomials $P_0, P_1, P_2, \dots, P_k$. Like a polynomial itself the linear combination has **coefficients** $b_0, b_1, b_2, \dots, b_k$.

(c) Show the collection

$$\left\{ \sum_{\ell=1}^{m} b_\ell v_\ell : m \in \mathbb{N},\ b_1, b_2, \dots, b_m \in F \text{ and } v_1, v_2, \dots, v_m \in S \right\} \tag{3}$$

is a subspace of a linear space W (over a field F) whenever S is any subset of W. Hint: Use part **(b)(iv)** of Problem 5 above.

The subspace appearing in (3) is called the **span** of the set S and is denoted

$$\operatorname{span}(S) = \left\{ \sum_{\ell=1}^{m} b_\ell v_\ell : m \in \mathbb{N},\ b_1, b_2, \dots, b_m \in F \text{ and } v_1, v_2, \dots, v_m \in S \right\}$$

If there is a subset S of linear space W with $\#(S) < \infty$ and

$$\operatorname{span}(S) = W,$$

then W is said to be **finitely generated** or **finite dimensional**.

(d) Is $F[X]$ finite dimensional?

A linear space which is not finite dimensional is said to be **infinite dimensional**.

Problem 7 (spanning sets, Boas 3.8.2) A subset S of a linear space W is said to be a **spanning set** if $\text{span}(S) = W$. One of the most important facts about finite dimensional linear spaces is that all spanning sets S fall into two categories:

(A) There exists a proper subset R of S for which $\text{span}(R) = W$. By **proper** one means $R \subset S$ but $R \neq S$.

(B) If one excludes a single element v of S, then $R = S \backslash \{v\}$ is no longer a spanning set: $\text{span}(S \backslash \{v\})$ is a proper subset (and a proper subspace) of W.

Recall that

$$\mathbb{Q} = \left\{ \frac{p}{q} : q \in \mathbb{N}, p \in \mathbb{Z} \right\}$$

is the field of rational numbers. Consider the linear space

$$W = \text{span}\{1 - 2X + 3X^2, 1 + X + X^2, -2 + X - 4X^2, 3 + 5X^2\} \subset \mathbb{Q}[X].$$

(a) Determine if each of the following sets is a spanning set for W.

- **(i)** $\{1 + X + X^2, -2 + X - 4X^2, 3 + 5X^2\}$
- **(ii)** $\{1 - 2X + 3X^2, -2 + X - 4X^2, 3 + 5X^2\}$
- **(iii)** $\{1 - 2X + 3X^2, 1 + X + X^2, 3 + 5X^2\}$
- **(iv)** $\{1 - 2X + 3X^2, 1 + X + X^2, -2 + X - 4X^2\}$
- **(v)** $\{-2 + X - 4X^2, 3 + 5X^2\}$
- **(vi)** $\{1 + X + X^2, 3 + 5X^2\}$
- **(vii)** $\{1 + X + X^2, -2 + X - 4X^2\}$
- **(viii)** $\{1 - 2X + 3X^2, 3 + 5X^2\}$
- **(ix)** $\{1 - 2X + 3X^2, -2 + X - 4X^2\}$
- **(x)** $\{1 - 2X + 3X^2, 1 + X + X^2\}$
- **(xi)** $\{3 + 5X^2\}$
- **(xii)** $\{-2 + X - 4X^2\}$
- **(xiii)** $\{1 + X + X^2\}$
- **(xiv)** $\{1 - 2X + 3X^2\}$

(b) For each spanning set for W you found in part **(b)** determine if that set is a category **(A)** spanning set or a category **(B)** spanning set.

Problem 8 (spanning sets, Boas 3.8.2)

(a) Find the cardinality of each category **(A)** spanning set you found in part **(b)** of Problem 7.

(b) Find the cardinality of each category **(B)** spanning set you found in part **(b)** of Problem 7.

(c) True or False: Every category **(A)** spanning set has the same number of elements.

Problem 9 (evaluation of polynomials) Given any polynomial

$$\sum_{n=0}^{\infty} a_n X^n$$

in $F[X]$, there exists a unique function $p : F \to F$ with values

$$p(x) = \sum_{n=0}^{\infty} a_n x^n. \tag{4}$$

Note that we have defined (at least) two functions here. For each $P \in F[X]$ we have defined a function $p : F \to F$.

But also (at another level) I have defined a function with domain the polynomials $F[X]$ and codomain the collection of all functions $f : F \to F$ (with domain F and codomain F). Let us call the collection

$$\{f : \ f \text{ is a function from } F \text{ to } F\}$$

of all functions $f : F \to F$

$$\mathrm{Aut}(F) = \{f : \ f \text{ is a function from } F \text{ to } F\}.$$

These functions are also called the **automorphisms** of F, though the term automorphism may also be used in various restricted contexts. For example sometimes the term "automorphism" refers to linear functions with a fixed domain W and also with the codomain W, or "automorphism" might refer to a group homomorphism $\phi : G \to G$ from a group G to itself. The basic meaning is that the domain and codomain are the same.[3] In the present context, the domain and codomain are the same field F.

[3] Strange but true: The collection of automorphisms $f : S \to S$ on a given set S is sometimes denoted by S^S.

Let us denote this second function by $\Phi : F[X] \to \mathrm{Aut}(F)$ with values

$$\Phi\left(\sum_{n=0}^{\infty} a_n X^n\right) = p$$

where $p \in \mathrm{Aut}(F)$ has values given in (4).

(a) Define (natural) addition and scaling on $\mathrm{Aut}(F)$ so that $\mathrm{Aut}(F)$ is a linear space over F.

The range (or image)

$$\Phi(F(X)) = \left\{\Phi\left(\sum_{n=0}^{\infty} a_n X^n\right) \quad : \quad \sum_{n=0}^{\infty} a_n X^n \in F(X)\right\}$$

of Φ is called the collection of **polynomial functions** on F and is denoted $\mathcal{P}(F)$.

Given an element $x \in F$, the **evaluation** of the polynomial

$$\sum_{n=0}^{\infty} a_n X^n$$

in $F[X]$ is the value

$$\sum_{n=0}^{\infty} a_n x^n.$$

That is, the evaluation if the value of

$$\Phi\left(\sum_{n=0}^{\infty} a_n X^n\right)$$

at $x \in F$. Evaluate the following polynomials at $0 \in F$ and $1 \in F$:

(b) $X + 4X^2$ with $F = \mathbb{R}$.

(c) $X + 4X^2$ with $F = \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

Problem 10 (algebraically complete) Given a polynomial

$$\sum_{n=0}^{\infty} a_n X^n$$

in $F[X]$ and an element $x \in F$, we say x is a **root** or **zero** of

$$\sum_{n=0}^{\infty} a_n X^n$$

if the evaluation of

$$\sum_{n=0}^{\infty} a_n X^n$$

at x is $0 \in F$.

(a) Find the roots of the following polynomials:

- **(i)** $X + X^2 \in \mathbb{Q}[X]$.
- **(ii)** $-2 + X^2 \in \mathbb{R}[X]$.
- **(iii)** $X + X^2 \in \mathbb{Z}_2[X]$.

(b) A field F is said to be **algebraically complete** if every polynomial

$$\sum_{n=0}^{\infty} a_n X^n$$

in $F[X]$ has a root in F. Determine if the following fields are algebraically complete:

- **(i)** $\mathbb{Q}$
- **(ii)** $\mathbb{R}$
- **(iii)** $\mathbb{Z}_2$

Things to think about:

1. (Problem 7) Given a finite dimensional linear space W is it possible to find two category **(B)** subsets with different numbers of elements?

2. (Problem 9) Is the collection of polynomial functions $\mathcal{P}(F)$ a subspace of $\mathrm{Aut}(F)$?

3. (Problem 9) Can you give an example of a field F for which $\mathcal{P}(F)$ is infinite dimensional? How do you know your example is infinite dimensional?

4. (Problem 9) Can you give an example of a field for which $\mathcal{P}(F)$ is finite dimensional?

5. (Problem 9) Note that by definition $\Phi : F[X] \to \mathcal{P}(F)$ is surjective. Can you give an example of a field F for which $\Phi : F[X] \to \mathcal{P}(F)$ is not injective?