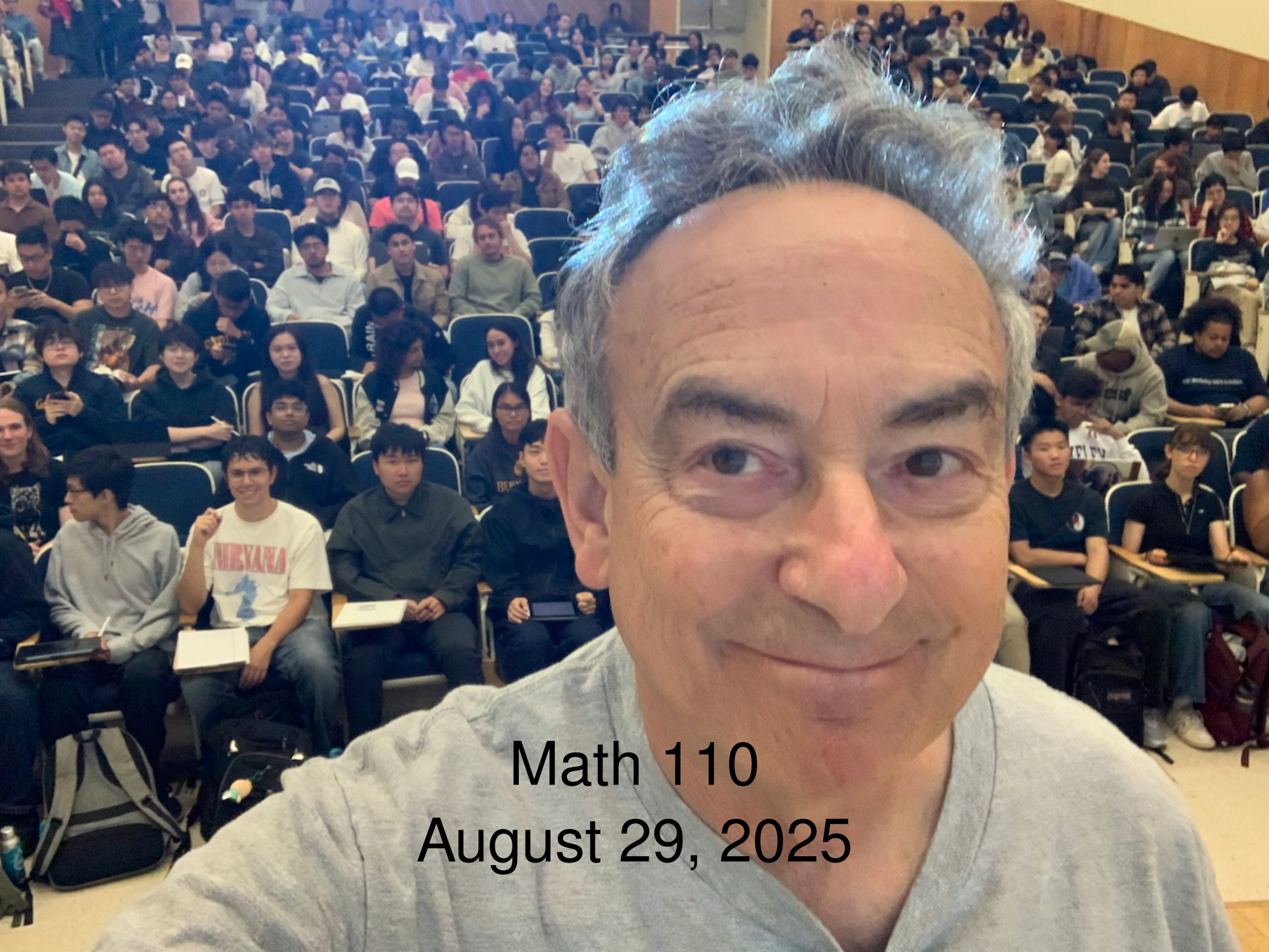
Math 110
August 29, 2025

Fields

A field (as studied in Math 113) is a commutative system where you can add, subtract, multiply and divide (except by 0).

On Wednesday, I mentioned that the set of integers mod a prime form a field under the usual operations of addition and multiplication.

For example, the integers mod 11 are 0, 1, 2,. . . , 10. When you add or multiply, take the remainder on division by 11. For example $9 \cdot 8 = 72 = 6$ because 72 is 6 plus a multiple of 11. To find the inverse of 9 mod 11, one quick way is to note that the inverse of 2 is 6 because $2 \cdot 6 = 12 \equiv 1 \pmod{11}$. Since 9 is -2, the inverse of 9 is -6, which is 5. Note that $9 \cdot 5 = 45 \equiv 1 \pmod{11}$.

In our course, a field is either **R** or **C**. It's called **F**.

As seen on Wednesday

The real numbers are the familiar decimal numbers, positive, negative or 0.

Some real numbers that come to mind are 110, 155, π, $\sqrt{2}$, -10^{10}, etc.

The field of complex numbers

A complex number is a sum $a + bi$, where a and b are real numbers and i satisfies $i^2 = -1$. Thanks to 0, every real number is also a complex number; for instance $110 = 110 + 0 \cdot i$.

Axler, page 2: a complex number is a pair (a, b) with $a, b \in \mathbf{R}$. This pair is written $a + bi$. Note that a real number a is $(a, 0)$ and i is $(0, 1)$.

You should practice finding inverses of nonzero complex numbers if you're not sure that you can do that without breaking a sweat.

NAME: **STUDENT ID:**

g. (3 pts) The complex number $\frac{7+i}{1-i}$ can be written as $a + bi$ for some real numbers a and b.

What is a?

What is b?

What is $|a + bi|$?

We all can do this problem from a 2022 Math 1B final. Multiply $7 + i$ by the inverse that we just found.

Vectors

Vector spaces are abstractions of the spaces $\mathbf{R}^n$ (and $\mathbf{C}^n$) that we saw in Math 54.

When we start the subject, vectors are arrows in n-space (having magnitude and direction, as one says), but we slide them so they come out of the origin $(0, \ldots, 0)$. Then what matters is where they end up, which is some point $(a_1, \ldots, a_n)$. The vectors in $\mathbf{F}^n$ are n-tuples of elements of $\mathbf{F}$. Said otherwise, the vector space $\mathbf{F}^n$ is the set of n-tuples of elements of $\mathbf{F}$.

If $n = 0$, there's only the empty n-tuple, $(\quad)$.

For $n \geq 0$, the n-tuple whose only entries are 0 is called 0.

Thus $\mathbf{F}^0$ consists of a single element: 0.

Operations on vectors

As you may remember from Math 54, $\mathbf{F}^n$ has two salient structures: vector addition and scalar multiplication.

Addition:

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (c_1, \ldots, c_n),$$

where $c_j = a_j + b_j$ for each j.

Scalar multiplication:

$$\lambda \cdot (a_1, \ldots, a_n) = (\lambda a_1, \ldots, \lambda a_n).$$

Here, λ is an element of $\mathbf{F}$ (a "scalar").

> *A vector space over* $\mathbf{F}$ *is a set with an addition and a scalar multiplication. These operations are constrained to satisfy a pile of axioms that are familiar for* $\mathbf{F}^n$.

Axioms for addition

A vector space is a set V with an addition $v, w \longmapsto v + w$ that's commutative

$$v + w = w + v$$

and associative

$$v + (w + z) = (v + w) + z.$$

There's a vector $0 \in V$ such that $v + 0 = v$ for all $v \in V$. For each $v \in V$, there's a vector $-v$ such that $v + (-v) = 0$.

For fans of Math 113, these axioms state that V with its addition is an abelian group.

A first exercise is to prove that 0 is unique and that $-v$ is unique for each v. (I used the **p** word.)

Axioms for multiplication

The set V also has a scalar multiplication

$$\lambda \in F, v \in V \longmapsto \lambda \cdot v \in V.$$

The remaining axioms:

- $1 \cdot v = v$;
- $(\mu\lambda) \cdot v = \mu(\lambda \cdot v)$;
- $(\mu + \lambda)v = \mu \cdot v + \lambda \cdot v$;
- $\lambda(v + w) = \lambda v + \lambda w$.

Comments:

The "dot" in scalar multiplication is optional and tends to disappear.

My bad: I didn't mention the "for all. . . " quantification in each axioms.

Executive session

Here's how I think of the axioms for a vector space V over $\mathbf{F}$:

The addition axioms state that V is an abelian group.

For each $\lambda \in \mathbf{F}$, scalar multiplication by λ is a function $m_\lambda : V \to V$, $v \mapsto \lambda v$. The distributive law $\lambda(v + w) = \lambda v + \lambda w$ states that m_λ is a *homomorphism* of abelian groups. (I'm just introducing a vocabulary word here.)

The next axioms state:

$$m_{\lambda+\mu} = m_\lambda + m_\mu$$
$$m_{\lambda\mu} = m_\lambda \circ m_\mu.$$

The first of these two equations is a second distributive law; the second is an associative law.

Examples of vector spaces

First off, $\mathbf{F}^n$ for all $n \geq 0$.

Secondly, the set of all "infinite vectors" $(a_1, a_2, a_3, \ldots)$ with entries in $\mathbf{F}$. Axler calls this $\mathbf{F}^\infty$. Note that $\mathbf{F}^\infty$ is the set of all functions

$$\{1, 2, 3, \ldots\} \longrightarrow F.$$

More generally, if S is a set, the set of functions

$$S \longrightarrow \mathbf{F}$$

is a vector space $\mathbf{F}^S$. We add functions in the natural way ("pointwise") and we multiply functions by scalars in the way that you'd guess.

Function space examples

The set of all functions $\mathbf{R} \longrightarrow \mathbf{R}$ is a vector space over $\mathbf{R}$. (We know how to add two functions or to multiply a function by 42.)

So is the set of all continuous functions $\mathbf{R} \to \mathbf{R}$. And so is the set of all differentiable functions $\mathbf{R} \to \mathbf{R}$.

Finally, so is the set of all twice differentiable functions $f : \mathbf{R} \to \mathbf{R}$ satisfying the differential equation

$$y'' - 3y' + 2y = 0.$$

Two such functions are e^x and e^{2x} (if I'm not mistaken).

Polynomials

For $m \geq 0$, a polynomial of *degree m* is an expression

$$a_0 + a_1 z + \cdots + a_m z^m$$

with the a_j in **F** and a_m nonzero. A polynomial of degree $\leq m$ is an expression $a_0 + a_1 z + \cdots + a_m z^m$ with the a_j in **F** and a_m possibly 0.

Digression

First of all, polynomials are defined relatively late in the book: you have to scroll down all the way to page 30.

Secondly, there is some nuance about polynomials as "formal expressions" and polynomials as functions $\mathbf{F} \to \mathbf{F}$. Because $\mathbf{F}$ has infinitely many elements, the two points of view are the same. Namely, you may remember from high school or math 55 that a nonzero polynomial has no more roots than its degree allows. A quintic polynomial can have no more than five roots, for example.

If $p(z)$ and $q(z)$ are expressions as above that yield the same function, then the polynomial $p(z) - q(z)$ is identically 0 and thus has infinitely many roots. As a result, it can't be a nonzero polynomial.

More words about degrees

A polynomial $a_0 + a_1 z + \cdots + a_m z^m$ has degree m if a_m is nonzero. A polynomial of degree 0 is a nonzero constant. A polynomial of degree 1 is an expression $az + b$ with a nonzero. A polynomial of degree 2 is a quadratic $az^2 + bz + c$ with a again nonzero.

The degree of the polynomial 0 is usually deemed to be $-\infty$ (whatever that means). If you don't like that, just say it's undefined.

The set of polynomials of degree $\leq m$ is denoted $\mathcal{P}_m(\mathbf{F})$. This set is a vector space under the natural addition and scalar multiplication that I'll describe.

Note that

$$\mathcal{P}_m(\mathbf{F}) \longleftrightarrow \mathbf{F}^{m+1}, \qquad a_0 + a_1 z + \cdots + a_m z^m \longleftrightarrow (a_0, a_1, \ldots, a_m).$$

The union $\mathcal{P}(\mathbf{F}) := \bigcup_{m \geq 0} P_m(\mathbf{F})$ is the set of polynomials over $\mathbf{F}$ of all degrees. It's again a vector space over $\mathbf{F}$.

We can view $\mathcal{P}(\mathbf{F})$ as the set of sequences

$$(a_0, a_1, a_2, \ldots,)$$

of elements of $\mathbf{F}$ with the property that there's an $m \geq 0$ such that $a_j = 0$ for $j > m$. These are the sequences with only a finite number of nonzero entries. These are the sequences that are "eventually 0."

Comparing $\mathcal{P}(\mathbf{F})$ with $\mathbf{F}^\infty$

The space $\mathcal{P}(\mathbf{F})$ is the set of sequences that are eventually 0. It doesn't matter whether we call the first entry a_0 or a_1. Every element of $\mathcal{P}(\mathbf{F})$ is also an element of $\mathbf{F}^\infty$:

$$\mathcal{P}(\mathbf{F}) \hookrightarrow \mathbf{F}^\infty.$$

For example, the polynomial $1 - x + x^3$ can be regarded as the sequence $(1, -1, 0, 1, 0, 0, \ldots, 0, \ldots)$, which is an element of $\mathbf{F}^\infty$.

After we define the notion of a *subspace*, you will agree that $\mathcal{P}(\mathbf{F})$ is a subspace of $\mathbf{F}^\infty$. (I hope you will, anyway.)

Another example: null spaces of matrices

Suppose that A is an $m \times n$ matrix of elements of $\mathbf{F}$. Let

$$V = \{\, x \in \mathbf{F}^n \mid Ax = 0 \,\}.$$

Thus V is the set of solutions of m homogeneous equations in n unknowns, and we have

$$V \hookrightarrow \mathbf{F}^n.$$

After we define the notion of a *subspace*, you will agree that V is a subspace of $\mathbf{F}^n$. (I hope you will, anyway.)

For the moment, let's think about the fact that V is a set with an addition and scalar multiplication and is definitely a vector space over $\mathbf{F}$ on its own steam (i.e., without thinking too much about $\mathbf{F}^n$).

Consequences of the axioms

You can find (in the text, including the exercises) lots of consequences of the axioms. A sample:

- For $\lambda \in F$ and $v \in V$: if $\lambda v = 0$, then either $v = 0$ or $\lambda = 0$ (or both).
- For each $v \in V$, $-(-v) = v$.
- For $v \in V$, $(-1) \cdot v = -v$.

The first statement amounts to the implication

If $\lambda v = 0$ *and* λ *is nonzero, then* $v = 0$*.*

To prove it, assume the hypothesis of the implication, namely that $\lambda v = 0$ and λ is nonzero. Then λ is invertible in **F**. Since $\lambda v = 0$, $0 = \frac{1}{\lambda}(\lambda v)$. By the associativity of multiplication,

$$0 = (\frac{1}{\lambda} \cdot \lambda)v = 1 \cdot v = v.$$

Back to the flow of the book

After defining a vector space, and even before giving lots of example, the book introduces the notion of a *subspace* of a vector space on page 18.
A subspace of a vector space V over $\mathbf{F}$ is a nonempty subset of V that is stable under both addition and scalar multiplication.

If the subset is called U, then the requirements are

$$u + u' \in U \text{ for all } u, u' \in U$$

and

$$\lambda u \in U \text{ for all } u \in U, \lambda \in \mathbf{F}.$$

If U is a subspace of V, then U is an $\mathbf{F}$-vector space: we can use the addition inside V to define an addition on U and similarly use the scalar multiplication on V to define a scalar multiplication on U. The axioms are built exactly for that purpose.

Examples of subspaces

For $m \geq 0$, $\mathcal{P}_m(\mathbf{F})$ is a subspace of $\mathcal{P}(\mathbf{F})$, and $\mathcal{P}(\mathbf{F})$ is a subspace of $\mathbf{F}^\infty$.

The space of continuous functions $\mathbf{R} \to \mathbf{R}$ is a subspace of the space of all functions $\mathbf{R} \to \mathbf{R}$. The space of differentiable functions $\mathbf{R} \to \mathbf{R}$ is a subspace of the space of continuous functions $\mathbf{R} \to \mathbf{R}$.

The null space of an $m \times n$ matrix is a subspace of $\mathbf{F}^n$. (I predicted you'd agree.)

Subspaces of $\mathbf{F}^2$

The full space V is a subspace of V. So is the singleton set $\{0\}$. Thus $\{0\}$ and $\mathbf{F}^2$ are subspaces of $\mathbf{F}^2$. Are there others?

Sure: take a vector $v \in \mathbf{F}^2$ and consider the set of its multiples; this set could be denoted $\mathbf{F} \cdot v$. If v is nonzero, it's a line.

Is that it? Yup, but we don't really know that yet. Informally at least: if $U \subseteq \mathbf{F}^2$ is a subspace, it could be $\{0\}$. If it isnt, it contains a nonzero vector v and thus the line $\mathbf{F} \cdot v$. Is it $\mathbf{F} \cdot v$? Maybe, but if not, it also contains a vector $w \notin \mathbf{F} \cdot v$. It then contains all expressions $\lambda v + \mu w$ with $\lambda, \mu \in \mathbf{F}$. We can convince ourselves using Math 54 or whatever that all elements of $\mathbf{F}^2$ may be written as sums $\lambda, \mu \in \mathbf{F}$. Thus the subspace is all of $\mathbf{F}^2$.

Smallest subspace containing a subset

Suppose that S is a subset of V. Then there is a subspace U of V that contains S with the property that U is contained in all subspaces of V that contain S. Thus U is the *smallest* subspace of V containing S.

The description of U is as follows: it consists of all sums

$$\lambda_1 s_1 + \cdots + \lambda_m s_m$$

with $m \geq 0$, $s_1, \ldots, s_m \in S$ and $\lambda_1, \ldots, \lambda_m \in \mathbf{F}$. The particular case $m = 0$ corresponds to the *empty sum*, which is 0.

Mathematicians like to say that it is "clear" that U is a subspace of V that contains each element of S and that all subspaces of V that contain S also contain U. It'll be on me to explain this to you.

Sums like $\lambda_1 s_1 + \cdots + \lambda_m s_m$ are referred to as *linear combinations* of the vectors s_i.