Fields

Informally A field is a set F with two binary operations $+, \cdot$ such that

1. $a+b=b+a$, $ab=ba$ $\forall a,b \in F$
2. $\exists\, 0 \neq 1 \in F$ w/ usual properties
3. $\exists -a$ so $a+-a=0$
4. If $a \neq 0$ $\exists\, 1/a$ so $a \cdot 1/a = 1/a \cdot a = 1$
5. Usual distributive, associative laws. Think: add, subtract, multiply & divide

Examples

0. Integers $\mathbb{Z}$, not a field!
1. Rationals $\mathbb{Q} = \{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \}$
2. Reals $\mathbb{R}$
3. Complex #'s $\mathbb{C} = \{ a+bi \mid a,b \in \mathbb{R} \}$

   ↳ usual setting for our book

4. $\mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \ldots, p-1\}$ under $+, \cdot$ mod p

Easy exercise: Check $\mathbb{Z}/n\mathbb{Z}$ is not a field if n is composite.
Harder exercise: Prove $\mathbb{Z}/p\mathbb{Z}$ is a field (hard part is mult inverse)

Def The characteristic of F is the smallest n such that $\underbrace{1+1+\cdots+1}_{n \text{ times}} = 0$

If no such n, say F has characteristic 0.

Exc If char $F \neq 0$ then it is prime.

Def F is algebraically closed if every poly w/ coefs in F has a root in F.

FTOA: $\mathbb{C}$ is algebraically closed

Vector spaces and F-algebras

Ex F a field, $M_{n \times m}(F) = \{n \times m \text{ matrices entries in } F\}$

- can add matrices
- multiply a matrix by a scalar
- "subtract", i.e. $\exists$ 0-matrix $\begin{pmatrix} 0 & \cdots & 0 \\ 0 & \cdots & 0 \end{pmatrix}$, $A + -A = \begin{pmatrix} 0 & \cdots & 0 \\ 0 & \cdots & 0 \end{pmatrix}$

Ex $F^n = \left\{ \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} \middle| \, c_i \in F \right\}$ n-long column vectors.

Ex $F[x] = \{ c_0 + c_1 x + \cdots + c_s x^s \mid c_i \in F \}$ polynomials w/ coefs in F.

Informal Def: A vector space over F (scalars) is a set V (vectors) with operations addition, scalar mult so

1. $V_1 + V_2 = V_2 + V_1$
2. $\exists \vec{0} \in V$, $\vec{v} + \vec{0} = \vec{v}$ $\forall \vec{v}$, $\exists -\vec{v}$ so $v + -\vec{v} = \vec{0}$

   Rmk 0 vector not same as $0 \in F$ Exc $0\vec{v} = \vec{0}$

3. Scalar mult: $c\vec{v} \in \vec{V}$
4. Usual associative, distributive laws $c(\vec{v}_1 + \vec{v}_2) = c\vec{v}_1 + c\vec{v}_2$

   $(cd)\vec{v} = c(d\vec{v}) = d(c\vec{v})$

   etc...

Def A subset $W \subseteq V$ is a subspace if it is a vector space under same operations, i.e. $w_1 + w_2 \in W$, $-w_1 \in W$, $cw_1 \in W$ $\forall w_1, w_2 \in W$, $F \ni c$.

Subspace Examples

1. $V = F^n$, $W = \left\{ \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_{n-1} \\ 0 \end{pmatrix} \right\}$

2. $V = \mathbb{R}^3$, W = plane through origin

3. $V = F[x]$ $W = \{ p(x) \mid \deg p(x) \le n \}$

4. $V = M_{n \times n}(F)$ $W = \{ A \mid \operatorname{trace} A = 0 \}$

5. Intersections of 2 subspaces

Rmk. Note $M_{n\times n}(F)$, $F[x]$ have additional structure of multiplication

Def An F-algebra is a vector space A over F w/ a multiplication $A \times A \to A$ so that

1. $(a+b)c = ac + bc$, $a(b+c) = ab + ac$ $\forall a,b,c \in A$
2. $\lambda(ab) = (\lambda a)b = a(\lambda b)$ $\forall a,b \in A, \lambda \in F$

It is associative if $(ab)c = a(bc)$ $\forall a,b,c \in A$

commutative if $ab = ba$

unital if $\exists\, 1 \in A$ with $1a = a1 = a$ $\forall a$

Ex 1. $M_n(F)$ is associative but not $(n>1)$ commutative

2. $F[x]$ is a commutative algebra

3. W in #3 above is a subspace but not a subalgebra.

Bases and Linear Independence

Def Let $v_1, v_2, ..., v_n \in V$. The span $\langle v_1, ..., v_n \rangle = \{c_1\vec{v}_1 + \cdots + c_n\vec{v}_n \mid c_i \in F\}$.
This is the set of all linear combinations of $v_1, ..., v_n$ and is clearly a subspace.

Rmk If $v_1 \in \langle v_2, ..., v_n \rangle$ then $\langle v_1, ..., v_n \rangle = \langle v_2, ..., v_n \rangle$

Def The set $\{\vec{v}_1, ..., \vec{v}_n\}$ is linearly independent if no $\vec{v}_i$ is a linear combination of the other $\vec{v}_j$'s.

Equivalently: $c_1\vec{v}_1 + c_2\vec{v}_2 + \cdots + c_n\vec{v}_n = 0$ implies $c_1, c_2, ..., c_n$ all $= 0$.

Def $\{\vec{v}_1, \vec{v}_2, ..., \vec{v}_n\}$ is a basis of V if it is linearly independent and spans, i.e. $V = \langle \vec{v}_1, ..., \vec{v}_n \rangle$.

Thm Any vector space has a basis, and the cardinality of the basis is independent of choice, called the dimension.

Ex

1. F^n, std basis $e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \quad e_n = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$

2. $V = \{2\times 2$ matrices with trace zero$\}$

   Basis $\left\{ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$

3. $V = F[x]$, Basis $\{1, x, x^2, x^3, x^4, ...\}$ infinite-dimensional vector space.

Basic Properties

1. Given any lin. ind. set $\{\vec{v}_1, \ldots, \vec{v}_s\} \in V$, it can be extended to a basis $\{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_s, \vec{v}_{s+1}, \ldots, \vec{v}_n\}$ of V.

2. Given any spanning set of V, it contains a basis

3. Every vector space $/F$ of dim n is $\cong$ to F^n, just pick a basis.

Linear Maps

<u>Def</u> $T: V \to W$ is <u>Linear</u> If $T(\vec{v}_1 + \vec{v}_2) = T(\vec{v}_1) + T(\vec{v}_2)$
$T(\lambda \vec{v}_1) = \lambda T(\vec{v}_1) \quad \forall v_i \in V, \lambda \in F$

If T is bijective, say T in an $\cong$

Rank-Nullity Thm

Let $T: V \to W$ be linear.

$$\dim V = \underbrace{\dim T(V)}_{\text{rank}} + \underbrace{\dim \operatorname{Ker} T}_{\text{nullity}}$$