Lecture 4: Fields

Last time: Geometry of linear systems, linear combinations, span

So far: studied linear equations over the reals

Essential for solving equations using Gaussian elimination:

addition (subtraction) and multiplication (division)

→ algebraic structure of a field

Def Fields

A field $(\mathbb{F}, 0, 1, +, \cdot)$ is a set $\mathbb{F}$ with two distinguished elements $0 \in \mathbb{F}$ and $1 \in \mathbb{F}$ $(0 \neq 1)$, and two binary relations $+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ and $\cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ satisfying:

(see next page for list of axioms)

(A1) Associativity of $+$: for $a,b,c \in \mathbb{F}$, $a+(b+c) = (a+b)+c$

(A2) Neutral element for $+$: for all $a \in \mathbb{F}$, $a+0 = a$

(A3) Inverse for $+$: for all $a \in \mathbb{F}$, there exists $b \in \mathbb{F}$ with $a+b = 0$.

(A4) Commutativity of $+$: for all $a,b \in \mathbb{F}$, $a+b = b+a$.

(M1) Associativity of $\cdot$: for all $a,b,c \in \mathbb{F}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(M2) Neutral element for $\cdot$: for all $a \in \mathbb{F}$, $a \cdot 1 = a$

(M3) Inverse for $\cdot$: for all $a \in \mathbb{F} \setminus \{0\}$, there exists $b \in \mathbb{F}$ with $a \cdot b = 1$

(M4) Commutativity of $\cdot$: for all $a,b \in \mathbb{F}$, $a \cdot b = b \cdot a$

(D) Distributive law: for all $a,b,c \in \mathbb{F}$, $a \cdot (b+c) = ab + ac$

Remarks: ·) (A1)–(A4) say that $(\mathbb{F}, +)$ is an Abelian (viz. commutative) group.

·) (M1)–(M4) say that $(\mathbb{F}^*, \cdot)$ (where $\mathbb{F}^* := \mathbb{F} \setminus \{0\}$) is an Abelian group.

·) (D) says that addition and multiplication are compatible.

·) The inverse in (A3) is unique, and usually denoted $-a$.

·) The inverse in (M3) is unique, and usually denoted a^{-1} (or $\frac{1}{a}$).

Examples of fields

1) Rational numbers $\mathbb{Q} := \left\{ \frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\} \right\}$

additive inverse of $\frac{a}{b}$ is $-\frac{a}{b} \equiv \frac{-a}{b}$

multiplicative inverse of $\frac{a}{b}$ $(a \neq 0)$ is $\frac{b}{a}$

$\left(\frac{0}{b} \equiv 0\right)$

2) Real numbers $\mathbb{R} = \overline{\mathbb{Q}}$, the completion of the rational numbers

$\overline{\mathbb{F}}$: every Cauchy sequence in $\mathbb{F}$ converges to a point in $\mathbb{F}$.

$\mathbb{R} \setminus \mathbb{Q}$ include $\sqrt{2}$, π, e, ...

3) Complex numbers $\mathbb{C} = \{ a + bi : a, b \in \mathbb{R} \}$, where "$i$" is the imaginary unit satisfying $i^2 = -1$. ($\hat{=}$ i is a root of $X^2 + 1$)

additive inverse of $a + bi$: $-a - bi$

$a \neq 0$ or $b \neq 0$: $(a+bi)^{-1} = \frac{a - bi}{a^2 + b^2}$

$(a+bi)(c+di) = (ac - bd) + (bc + ad)i$

Alternatively, $\mathbb{C} = \{ (a, b) : a, b \in \mathbb{R} \}$

$(a, b) + (c, d) := (a + c, b + d)$

$(a, b) \cdot (c, d) := (ac - bd, bc + ad)$

Properties of the complex numbers:

·) $\mathbb{C}$ is not an ordered field: there is no total order on $\mathbb{C}$ compatible with field operations

(Compatibility: if $a \leq b$, then $a+c \leq b+c$

and if $0 \leq a$ and $0 \leq b$, then $0 \leq a \cdot b$)

→ Homework

·) $\mathbb{C}$ is algebraically closed: Every non-constant polynomial with coefficients in $\mathbb{C}$ has a root in $\mathbb{C}$.

(Fundamental thm of Algebra)

Other examples of fields:

·) Field with two elements $\mathbb{F}_2 = \{0, 1\}$

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

·) Finite fields $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for p prime

$+$ and $\cdot$ are taken mod p (modular arithmetic)

·) For every prime power $q = p^k$ there exists a finite field $\mathbb{F}_q$ with q elements.

We will develop much of the theory of vector spaces over arbitrary fields $\mathbb{F}$. However, in many applications the choices $\mathbb{F} = \mathbb{R}, \mathbb{C}, \mathbb{F}_2$ are particularly important

$\mathbb{R}$: data science, geometry, "real-world" linear equations

$\mathbb{C}$: Quantum mechanics, Lie theory

$\mathbb{F}_2$: Coding theory, cryptography, information theory