01: Fields

Mike Bernard

2021-01-19

Contents

1 Fields

A Field is loosely defined as a number system that models the usual conventions for addition, multiplication, subtraction, and division.

Example 1. *Common Fields:*

- $\mathbb{Q}$*: Rational numbers; equivalence classes of pairs* (m, n) *of integers, with* $n \neq 0$*, such that* $\frac{m}{n} = \frac{p}{q}$ *iff* $mq = np$*.*
- $\mathbb{R}$*: Real numbers; decimal expansions.*
- $\mathbb{C}$*: Complex numbers.*

Definition 1. *A* Field F *is a set of elements with:*

- *an additive identity element, denoted* 0 *or* 0_F *to avoid confusion*
- *a multiplicative identity element, denoted* 1 *or* 1_F *to avoid confusion*
- *an additive operation* $+ : F \times F \to F$
- *a multiplicative operation* $\cdot : F \times F \to F$ *(oftened shortened from* $x \cdot y$ *to* xy*)*

with the properties that:

1. $x + y = y + x \forall x, y \in F$ *(additive commutativity)*
2. $(x + y) + z = x + (y + z) \forall x, y, z \in F$ *(additive associativity)*
3. $x + 0 = 0 + x = x \forall x \in F$ *(additive identity)*
4. $\forall x \in F, \exists - x \in F$ *s.t.* $x + (-x) = 0$ *(additive inverse)*
5. $x \cdot y = y \cdot x \forall x, y \in F$ *(multiplicative commutativity)*
6. $(xy)z = x(yz) \forall x, y, z \in F$ *(multiplicative associativity)*
7. $x \cdot 1 = 1 \cdot x = x \forall x \in F$ *(multiplicative identity)*

8. $1 \neq 0$ *and* $\forall x \in F$ *where* $x \neq 0$, $\exists x^{-1} \in F$ *s.t.* $xx^{-1} = 1$ *(multiplicative inverse)*

9. $x(y+z) = xy + xz \forall x, y, z \in F$ *(distributivity)*

Remark 1. *The set of integers* $\mathbb{Z}$ *is not a field; it violates property 8 under Definition 1 (e.g. 2 does not have an integer multiplicative inverse).*

Remark 2. *0 and 1 are always unique in a field.*

Example 2. $\mathbb{Z}_m$ *is the set of equivalence classes of integers modulo* m, $m \geq 2$.

Note that $\mathbb{Z}_2 = \{0, 1\}$ *meets the properties listed in Definition 1, and is therefore a field. In contrast,* $\mathbb{Z}_4$ *is not a field, since* $2 \in \mathbb{Z}_4$ *does not have a multiplicative inverse.*

2 Characteristics

Definition 2. *The* characteristic *of a field is defined as the number of times the multiplicative identity element must be added with itself to yield the additive identity element.*

For example, in $\mathbb{Z}_2$, $1 + 1 = 0$, *so* $\text{char } \mathbb{Z}_2 = 2$.

If the sum never yields the additive identity, we denote the characteristic as 0 by convention. Exemplar fields include $\mathbb{Q}$, $\mathbb{R}$, *and* $\mathbb{C}$.

Note: Nonzero characteristics are always prime.

Note: Arithmetic geometry studies fields with positive characteristics.

Theorem 1. $\mathbb{Z}_m$ *is a field iff* m *is prime.*

Remark 3. *Using field axioms, we can obtain all the usual rules of arithmetic, for example,*

- $0 \cdot x = 0$
- *associativity holds for any finite number of elements (not easily written out)*
- *subtraction can be defined as* $x - y := x + (-y)$

3 Vector Spaces

Definition 3. *A set* V *is a* vector space *over a field* F *if it has:*

- $\exists \vec{0} \in V$ *(zero vector)*
- $+ : V \times V \to V$ *(vector addition)*
- $\cdot : F \times V \to V$ *(scalar multiplication)*

with the properties:

1. $\vec{x} + \vec{y} = \vec{y} + \vec{x} \ \forall \vec{x}, \vec{y} \in V$ *(additive commutativity)*
2. $(x+y) + z = x + (y+z) \ \forall x, y, z \in V$ *(additive associativity)*
3. $x + \vec{0} = x \ \forall x \in V$ *(additive identity)*
4. $\forall x \in V$, $\exists x^{-1} \in V$ *s.t.* $x + (-x) = \vec{0}$ *(additive inverse)*
5. $\alpha(\beta x) = (\alpha\beta)x \ \forall \alpha, \beta \in F, \forall x \in V$ *(scalar multiplication)*
6. $1_F \cdot x = x \ \forall x \in V$ *(multiplicative identity)*
7. $\alpha(x+y) = \alpha x + \alpha y \ \forall \alpha \in F$, $\forall x, y \in V$ *(scalar distributivity)*
8. $(\alpha + \beta)x = \alpha x + \beta x \ \forall \alpha, \beta \in F$, $\forall x \in V$ *(vector distributivity)*

Remarks on Vector Spaces

- F is called the "scalar field"
- The definition of a vector space V includes by necessity some scalar field F
- In introductory linear algebra, F= $\mathbb{R}$
- Best examples to keep in mind are $\mathbb{R}^2$ and $\mathbb{R}^3$
- We won't write arrows for vectors to save time as long as it can be understood that the element is in a vector space
- $\mathbb{R}^1 \cong \mathbb{R}$ is a vector space over $\mathbb{R}$ (i.e. the set of real numbers is a vector space over itself)
- A vector space over $\mathbb{R}$ is called a "real" vector space
- A vector space over $\mathbb{C}$ is called a "complex" vector space
- $\mathbb{R}^1$ and $\mathbb{C}^1$ are too simple examples to say anything interesting
- $\mathbb{C}[x] = P$, the set of polynomials in variable x with complex coefficients is an infinite-dimensional vector space
- In general, F^n is an n-dimensional vector space over the field F
- $\mathbb{C}^n$ is not just a complex vector space, but also a *real* vector space