Field Theory Notes

Jason Sass

July 6, 2023

Fields

A field is an algebraic structure upon which the arithmetic operations (addition, subtraction, multiplication, division) are defined.

Definition 1. Field

A **field** $(F, +, \cdot)$ is a set F with two binary operations $+$ and $\cdot$ defined on F such that the following axioms hold:

A1. Addition is associative.
$(a + b) + c = a + (b + c)$ for all $a, b, c \in F$.
A2. Addition is commutative.
$a + b = b + a$ for all $a, b \in F$.
A3. There is a right additive identity.
$(\exists 0 \in F)(\forall a \in F)(a + 0 = a)$.
A4. Each element has a right additive inverse.
$(\forall a \in F)(\exists b \in F)(a + b = 0)$.
M1. Multiplication is associative.
$(ab)c = a(bc)$ for all $a, b, c \in F$.
M2. Multiplication is commutative.
$ab = ba$ for all $a, b \in F$.
M3. There is a right multiplicative identity.
$(\exists 1 \in F)(\forall a \in F)(a1 = a)$.
M4. Each nonzero element has a right multiplicative inverse.
$(\forall a \in F^*)(\exists b \in F)(ab = 1)$.
D1. Multiplication is left distributive over addition.
$a(b + c) = ab + ac$ for all $a, b, c \in F$.
F1. Multiplicative identity is distinct from additive identity.
$1 \neq 0$.

Since $1 \neq 0$ in F, then any field must contain at least two elements.

Example 2. smallest field $(\mathbb{Z}_2, +, \cdot)$

$(\frac{\mathbb{Z}}{2\mathbb{Z}}, +, \cdot)$ is a field.

Proposition 3. ***alternate definition of a field***

A field is a commutative ring with multiplicative identity $1 \neq 0$ *such that every nonzero element has a multiplicative inverse.*

Let $(F, +, \cdot)$ be a field.
Since $+$ is a binary operation on F, then F is closed under addition.
Since $\cdot$ is a binary operation on F, then F is closed under multiplication.
Since F is a ring, then $(F, +)$ is an abelian group and 0 is the additive identity of F and the additive inverse of $a \in F$ is denoted by $-a$.
Since F is a ring, then 1 is the multiplicative identity of F.
Let F^* be the set of all nonzero elements of F.
Then $F^* = \{a \in F : a \neq 0\}$.
Therefore, F satisfies the following axioms:
A1. $a + b \in F$ for all $a, b \in F$.
A2. $(a + b) + c = a + (b + c)$ for all $a, b, c \in F$.
A3. $a + b = b + a$ for all $a, b \in F$.
A4. $(\exists 0 \in F)(\forall a \in F)(0 + a = a + 0 = a)$.
A5. $(\forall a \in F)(\exists b \in F)(a + b = b + a = 0)$.
M1. $ab \in F$ for all $a, b \in F$.
M2. $(ab)c = a(bc)$ for all $a, b, c \in F$.
M3. $ab = ba$ for all $a, b \in F$.
M4. $(\exists 1 \in F)(\forall a \in F)(1 \cdot a = a \cdot 1 = a)$.
M5. $(\forall a \in F^*)(\exists b \in F)(ab = ba = 1)$.
D1. $a(b + c) = ab + ac$ for all $a, b, c \in F$.
D2. $(b + c)a = ba + ca$ for all $a, b, c \in F$.
F1. $1 \neq 0$.
Since F is a commutative ring with identity $1 \neq 0$ such that every nonzero element has a multiplicative inverse, then F is a commutative division ring.
Therefore, a field is a commutative division ring.
Since F is a division ring, then $(F^*, \cdot)$ is the group of units of F.
Since multiplication is commutative, then $(F^*, \cdot)$ is an abelian group.

Example 4. field of rational numbers $(\mathbb{Q}, +, \cdot)$
$(\mathbb{Q}, +, \cdot)$ is a field.
Additive identity is $0 = \frac{0}{1}$.
Additive inverse of $\frac{a}{b}$ is $-\frac{a}{b}$.
Multiplicative identity is $1 = \frac{1}{1}$.
Multiplicative inverse of $\frac{a}{b} \in \mathbb{Q}^*$ is $\frac{b}{a} \in \mathbb{Q}^*$.

Example 5. field of real numbers $(\mathbb{R}, +, \cdot)$
$(\mathbb{R}, +, \cdot)$ is a field.
Additive identity is 0.
Additive inverse of a is $-a$.
Multiplicative identity is 1.
Multiplicative inverse of $a \in \mathbb{R}^*$ is $\frac{1}{a} \in \mathbb{R}^*$.

Example 6. field of complex numbers $(\mathbb{C}, +, \cdot)$
$(\mathbb{C}, +, \cdot)$ is a field.
Additive identity is $0 = 0 + 0i$.
Let $a, b \in \mathbb{R}$.
Additive inverse of $z = a + bi$ is $-z = -a - bi$.

Multiplicative identity is $1 = 1 + 0i$.
Let $z \in \mathbb{C}^*$.
Multiplicative inverse of $z = |z|\text{cis } \theta$ is $z^{-1} = \frac{1}{z} = \frac{1}{|z|}\text{cis } (-\theta)$

Example 7. $\mathbb{Z}_p$ **is a field when** p **is prime**
Let $p \in \mathbb{Z}^+$.
If p is prime, then $(\mathbb{Z}_p, +, \cdot)$ is a field.

Example 8. Gaussian integers
Let $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.
Then $(\mathbb{Z}[i], +)$ is an abelian group under complex addition.
$(\mathbb{Z}[i], +, \cdot)$ is a subring of $(\mathbb{C}, +, \cdot)$ known as the **Gaussian integers**.

Example 9. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a field under addition and multiplication of $\mathbb{R}$.

Theorem 10. ***left and right multiplicative cancellation laws hold in a field***
Let $(F, +, \cdot)$ be a field.
If $ac = bc$ and $c \neq 0$, then $a = b$. (right multiplicative cancellation law)
If $ca = cb$ and $c \neq 0$, then $a = b$. (left multiplicative cancellation law)

Proposition 11. ***multiplication and division are inverse operations***
Let F be a field.
Then $(\forall a, b \in F, a \neq 0)(\exists! x \in F)(ax = b)$.

Therefore, $ax = b$ means $x = \frac{b}{a}$.

Theorem 12. *Every field is an integral domain.*

Let $(F, +, \cdot)$ be a field.
Then $ab = 0$ iff $a = 0$ or $b = 0$ for all $a, b \in F$.
Equivalently, $ab \neq 0$ iff $a \neq 0$ and $b \neq 0$ for all $a, b \in F$.

Therefore, the product of any two nonzero elements of a field is nonzero.

Since F is an integral domain and every integral domain satisfies the multiplicative cancellation laws, then F satisfies the multiplicative cancellation laws, as stated previously.

Example 13. Since $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are fields, then $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are integral domains.

Example 14. Not every integral domain is a field.
The ring of integers $\mathbb{Z}$ is an integral domain, but $\mathbb{Z}$ is not a field.

Proposition 15. *Let $(F, +, \cdot)$ be a field.*
If $a \neq 0$ and $b \neq 0$, then $(ab)^{-1} = a^{-1}b^{-1}$.

Corollary 16. *Let $(F, +, \cdot)$ be a field.*
Let $a, b, c \in F$ such that $b \neq 0$ and $c \neq 0$.
Then $\frac{ac}{bc} = \frac{a}{b}$.

Theorem 17. ***arithmetic operations on quotients***
Let $(F, +, \cdot)$ be a field.
Let $a, b, c, d \in F$ such that $b \neq 0$ and $d \neq 0$. Then
1. $\frac{a}{b} = \frac{c}{d}$ iff $ad = bc$. (equality of quotients)
2. $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$. (multiply quotients)
3. if $c \neq 0$, then $\frac{a}{b} / \frac{c}{d} = \frac{ad}{bc}$. (divide quotients)
4. $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$. (add quotients)
5. $\frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd}$. (subtract quotients)

Theorem 18. *For every prime p, $\mathbb{Z}_p$ is a field of characteristic p.*
In fact, $\mathbb{Z}_p$ is a field iff p is prime.

Polynomial Rings

Let $\mathbb{R}[x]$ be the set of all polynomials in a single variable x having real coefficients.
Define polynomial addition and multiplication on $\mathbb{R}[x]$.
Then $(\mathbb{R}[x], +, \cdot)$ is not a field, but it is a ring.
It is not a field because not every polynomial has a multiplicative inverse.

Definition 19. polynomial
Let R be a ring.
Let X be a variable (formal symbol that is not an element of R).
Let $\tilde{N} = \{0, 1, 2, ...\} = \{n \in \mathbb{Z} : n \geq 0\}$.
Let $n \in \tilde{N}$.
Let $a_0, a_1, ..., a_n \in R$.
A **polynomial** f **in variable** X **over** R is a map $f : \tilde{N} \mapsto R$ defined by

$$f_k = \begin{cases} a_k & \text{if } k \leq n \\ 0 & \text{if } k > n \end{cases}$$

such that $f = \sum p_k X^k$ for all $k \in \tilde{N}$.

Let p be a polynomial in variable X over a ring R.
Then there exists $n \in \mathbb{Z}, n \geq 0$ such that $a_0, a_1, ..., a_n \in R$ and for all $k > n, p_k = 0$ and $p_k = a_k$ iff $k \leq n$ and $p = \sum p_k X^k$.

Therefore,

$$\begin{aligned}
p &= \sum p_k X^k \\
&= p_0 + p_1 X + p_2 X^2 + ... + p_n X^n + 0 + 0 + ... \\
&= a_0 + a_1 X + a_2 X^2 + ... + a_n X^n + 0 + 0 + ... \\
&= a_0 + a_1 X + a_2 X^2 + ... + a_n X^n \\
&= a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0 \\
&= \sum_{k=0}^{n} a_k X^k.
\end{aligned}$$

Each $a_k X^k$ is called a **monomial**.
a_k is the **coefficient of** X.
The **degree of a monomial** $a_k X^k$ is the exponent k of the variable X.
Each monomial is a **term** of the polynomial.
Therefore, a polynomial is a finite sum of monomials.
$(a_0, a_1, ..., a_n)$ is a sequence of coefficients of the polynomial p.
$0X^n = 0$ for each $n \in \tilde{N}$.
$(\forall m, n \in \tilde{N})(X^m X^n = X^{m+n})$.
$X^0 = 1$
$X^1 = X$
A polynomial is a linear combination of powers of X with coefficients in R.

Definition 20. constant polynomial
Let p be a polynomial in variable X over a ring R such that $n = 0$.
Then $a_0 \in R$ and $p = \sum_{k=0}^{0} a_k X^0 = a_0 X^0 = a_0$.
Thus p is called a **constant polynomial** and a_0 is called a **constant**.
Hence, $(a_0, 0, ..., 0)$ is the sequence of coefficients of p.

Let $a \neq 0 \in R$.
Since $a = aX^0$, then the degree of a is 0.
Therefore, the degree of a nonzero constant polynomial is zero.

Definition 21. zero polynomial
Let $\tilde{N} = \{0, 1, 2, ...\} = \{n \in \mathbb{Z} : n \geq 0\}$.
Let p be a polynomial in variable X over a ring R such that $p_n = 0$ for all $n \in \tilde{N}$.
Then p is the **zero polynomial**.
Thus, $(0, 0, ..., 0)$ is the sequence of coefficients of p.
The zero polynomial corresponds to the zero of the ring R.
Therefore, $p = 0$.

The degree of the zero polynomial is defined to be $-\infty$.

The zero polynomial is a constant polynomial.

Definition 22. degree of a polynomial

Let $\tilde{N} = \{0, 1, 2, ...\} = \{n \in \mathbb{Z} : n \geq 0\}$.

Let p be a nonzero polynomial in variable X over a ring R.

Then there exists $n \in \tilde{N}$ such that $a_0, a_1, ..., a_n \in R$ and $p_k = 0$ for all $k > n$ and $p_k = a_k$ iff $k \leq n$ and $p = \sum_{k=0}^{n} a_k X^k$ and $p \neq 0$.

The degree of p is $\max(k \in \tilde{N} : p_k \neq 0)$.

Therefore, the degree of a nonzero polynomial is the largest degree of the nonzero terms of the polynomial.

Since $aX = aX^1$, then the degree of aX is one.

Degrees of polynomials:

zero $-\infty$

nonzero constant 0

linear 1

quadratic 2

cubic 3

quartic 4

quintic 5

sextic 6

septic 7

octic 8

nonic 9

decic 10

hectic 100

Definition 23. equal polynomials

Let p, q be polynomials in variable X over a ring R.

Let $\tilde{N} = \{0, 1, 2, ...\} = \{n \in \mathbb{Z} : n \geq 0\}$.

Then there exist $m, n \in \tilde{N}$ such that $a_0, a_1, ..., a_m \in R$ and $p_k = 0$ for all $k > m$ and $p_k = a_k$ iff $k \leq m$ and $p = \sum_{k=0}^{m} a_k X^k$ and $b_0, b_1, ..., b_n \in R$ and $q_k = 0$ for all $k > n$ and $q_k = b_k$ iff $k \leq n$ and $q = \sum_{k=0}^{n} b_k X^k$.

Thus,

$p = a_0 + a_1 + ... + a_m X^m$

and

$q = b_0 + b_1 + ... + b_n X^n$.

Therefore, $p = q$ iff $(\forall k \in \tilde{N})(p_k = q_k)$.

Two polynomials are equal iff corresponding coefficients for each power of X are equal.

Definition 24. Addition of polynomials

Let $\tilde{N} = \{0, 1, 2, ...\}$.

Let p and q be polynomials in variable X over a ring R.

Then there exist $m, n \in \tilde{N}$ such that $a_0, a_1, ..., a_m \in R$ and $p_k = 0$ for all $k > m$ and $p_k = a_k$ iff $k \leq m$ and $p = \sum_{k=0}^{m} a_k X^k$ and $b_0, b_1, ..., b_n \in R$ and $q_k = 0$ for all $k > n$ and $q_k = b_k$ iff $k \leq n$ and $q = \sum_{k=0}^{n} b_k X^k$.

The sum of polynomials is defined by the rule $p + q = \sum c_k x^k$ where $c_k = p_k + q_k$ for all $k \in \tilde{N}$.

Thus,

$$\begin{aligned} p + q &= \sum a_k x^k + \sum_{k=0}^{n} b_k x^k \\ &= \sum (p_k + q_k) x^k \\ &= \sum_{k=0}^{n} (a_k + b_k) x^k. \end{aligned}$$

Therefore, the sum of two polynomials is the sum of coefficients of corresponding terms.

Let $m = \deg p$ and $n = \deg q$.

Then $\deg(p + q) = \max(m, n)$.

The sum of polynomials, denoted $(p + q)(x)$ is the same as : $(p + q)(x) = p(x) + q(x)$, but this is not the definition of polynomial addition.

Definition 25. Multiplication of polynomials

Let $\tilde{N} = \{0, 1, 2, ...\}$.

Let p and q be polynomials in variable X over a ring R.

Then there exist $m, n \in \tilde{N}$ such that $a_0, a_1, ..., a_m \in R$ and $p_k = 0$ for all $k > m$ and $p = \sum_{k=0}^{m} a_k X^k$ and $b_0, b_1, ..., b_n \in R$ and $q_k = 0$ for all $k > n$ and $q = \sum_{k=0}^{n} b_k X^k$.

The product of polynomials is defined by the rule $pq = \sum_{k=0}^{m+n} c_k x^k$ where $c_k = \sum_{i=0}^{k} a_i b_{k-i}$ for all $k \in \tilde{N}$.

Let $m = \deg p$ and $n = \deg q$.

Then $\deg(pq) = m + n$.

The product of polynomials, denoted $(pq)(x)$ is the same as : $(pq)(x) = p(x)q(x)$, but this is not the definition of polynomial multiplication.

Definition 26. polynomial ring $R[x]$

Let R be a ring.

Let $R[x]$ be the set of all polynomials in variable x over R.

Then $R[x] = \{\sum_{k=0}^{n} a_k x^k : (\exists n \in \mathbb{Z})(n \geq 0)(\forall k = 0, 1, ..., n)(a_k \in R)\}$.

Theorem 27. *Then* $(R[x], +, *)$ *is a ring with unity .*

The zero of $R[x]$ is the zero polynomial 0.

The additive inverse of $\sum_{k=0}^{n} a_k x^k$ is $\sum_{k=0}^{n} (-a_k) x^k$.