# Field Theory

Jason Sass

July 2, 2023

## Fields

**Proposition 1.** ***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.*

*Proof.* Let $(F, +, \cdot)$ be a field.

Then addition and multiplication are binary operations defined on $F$ and addition is associative and commutative and there is a right additive identity and each element of $F$ has a right additive inverse and multiplication is associative and multiplication is left distributive over addition.

To prove $F$ is a ring, we need only prove there is a multiplicative identity in $F$ and multiplication is right distributive over addition.

We prove there is a multiplicative identity in $F$.

Since $F$ is a field, then there is a right multiplicative identity.

Let 1 be a right multiplicative identity in $F$.

Then $1 \in F$ and $a1 = a$ for all $a \in F$.

Let $a \in F$.

Then $a1 = a$.

Since $F$ is a field, then multiplication is commutative, so $a1 = 1a$.

Thus, $a = a1 = 1a$.

Therefore, 1 is a multiplicative identity in $F$, so there is a multiplicative identity in $F$.

We prove multiplication is right distributive over addition.

Let $a, b, c \in F$.

Then

$$\begin{aligned}(b+c)a &= a(b+c) \\ &= ab + ac \\ &= ba + ca.\end{aligned}$$

Hence, multiplication is right distributive over addition.

Therefore, $(F, +, \cdot)$ is a ring.

Since multiplication is commutative, then $(F, +, \cdot)$ is a commutative ring.

We prove $1 \neq 0$.

Since $(F, +, \cdot)$ is a ring, then $(F, +)$ is an abelian group.

Therefore, 0 is the additive identity of $F$.

Since $F$ is a field, then $1 \neq 0$.

We prove every nonzero element has a multiplicative inverse.

Since $F$ is a field, then each nonzero element of $F$ has a right multiplicative inverse in $F$.

Let $a$ be a nonzero element of $F$.

Then $a$ has a right multiplicative inverse in $F$.

Therefore, there exists $b \in F$ such that $ab = 1$.

Since multiplication is commutative in $F$, then $ab = ba$.

Thus, $1 = ab = ba$, so $b$ is a multiplicative inverse of $a$.

Hence, every nonzero element of $F$ has a multiplicative inverse in $F$.

Therefore, $(F, +, \cdot)$ is a commutative ring with multiplicative identity $1 \neq 0$ such that every nonzero element of $F$ has a multiplicative inverse.

Let $(F, +, \cdot)$ be a commutative ring with multiplicative identity $1 \neq 0$ such that every nonzero element has a multiplicative inverse.

We prove $(F, +, \cdot)$ is a field.

Since $(F, +, \cdot)$ is a commutative ring, then $+$ is a binary operation on $F$ and addition is associative and commutative and there is a right additive identity $0 \in F$ and each element has a right additive inverse in $F$ and $\cdot$ is a binary operation on $F$ and multiplication is associative and commutative and there is a multiplicative identity $1 \in F$ and multiplication is left distributive over addition.

Since 1 is a multiplicative identity, then $1a = a1 = a$ for all $a \in F$.

Hence, $a1 = a$ for all $a \in F$, so 1 is a right multiplicative identity.

By hypothesis, $1 \neq 0$.

Let $a$ be a nonzero element of $F$.

Then $a$ has a multiplicative inverse.

Hence, there exists $b \in F$ such that $ab = ba = 1$.

Thus, there exists $b \in F$ such that $ab = 1$, so $a$ has a right multiplicative inverse in $F$.

Therefore, every nonzero element of $F$ has a right multiplicative inverse in $F$.

Therefore, $F$ is a field. □

**Theorem 2.** ***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 )*

*Proof.* Let $a, b, c \in F$.

We prove if $ac = bc$ and $c \neq 0$, then $a = b$.

Suppose $ac = bc$ and $c \neq 0$.

Since $c \neq 0$, then the multiplicative inverse $c^{-1}$ exists in $F$.

Observe that

$$\begin{aligned} a &= a \cdot 1 \\ &= a(c \cdot c^{-1}) \\ &= (ac) \cdot c^{-1} \\ &= (bc) \cdot c^{-1} \\ &= b(c \cdot c^{-1}) \\ &= b \cdot 1 \\ &= b. \end{aligned}$$

Therefore, $a = b$, as desired.

We prove if $ca = cb$ and $c \neq 0$, then $a = b$.

Suppose $ca = cb$ and $c \neq 0$.

Since $ac = ca = cb = bc$, then $ac = bc$.

Therefore, $ac = bc$ and $c \neq 0$, so by the previously proved result, we have $a = b$, as desired. □

**Proposition 3.** ***multiplication and division are inverse operations***
*Let $F$ be a field.*
*Then $(\forall a, b \in F, a \neq 0)(\exists! x \in F)(ax = b)$.*

*Proof.* Let $a, b \in F$ with $a \neq 0$.

We prove a solution to the equation $ax = b$ is unique.

**Existence:**

Since $a \neq 0$, then the multiplicative inverse $a^{-1}$ exists in $F$. Since $F$ is closed under multiplication, then $ba^{-1} \in F$.

Let $x = \frac{b}{a}$.

Then

$$\begin{aligned} ax &= a(\frac{b}{a}) \\ &= a(ba^{-1}) \\ &= a(a^{-1}b) \\ &= (aa^{-1})b \\ &= 1 \cdot b \\ &= b. \end{aligned}$$

Hence, $ax = b$. Therefore, at least one solution exists.

**Uniqueness:**

Suppose $x_1, x_2 \in F$ are solutions to $ax = b$.

Then $ax_1 = b$ and $ax_2 = b$. Thus $ax_1 = ax_2$. Since $ax_1 = ax_2$ and $a \neq 0$, then $x_1 = x_2$, by the left multiplicative cancellation law for fields. Therefore, at most one solution exists.

Since at least one solution exists and at most one solution exists, then exactly one solution exists.

Therefore, a solution to $ax = b$ is unique. □

**Theorem 4.** *Every field is an integral domain.*

*Proof.* Let $(F, +, \cdot)$ be a field. To prove $F$ is an integral domain, we must prove $F$ is a commutative ring with nonzero unity and $F$ has no zero divisors. By definition of field, $F$ is a commutative ring with nonzero unity.

To prove $F$ has no zero divisors, we prove if $ab = 0$, then either $a = 0$ or $b = 0$ for all $a, b \in F$. Let $a, b \in F$.

To prove $ab = 0$ implies $a = 0$ or $b = 0$, we assume $ab = 0$ and $a \neq 0$. We must prove $b = 0$.

Since $a \neq 0$, then $a^{-1} \in F$ exists.

Observe that

$$\begin{aligned} b &= 1 \cdot b \\ &= (a^{-1} \cdot a)b \\ &= a^{-1}(ab) \\ &= a^{-1} \cdot 0 \\ &= 0. \end{aligned}$$

Therefore, $b = 0$, as desired. □

**Proposition 5.** *Let $(F, +, \cdot)$ be a field. If $a \neq 0$ and $b \neq 0$, then $(ab)^{-1} = a^{-1}b^{-1}$.*

*Proof.* Suppose $a \neq 0$ and $b \neq 0$.

Since $F$ is a field, then every nonzero element of $F$ has a multiplicative inverse in $F$. Therefore, $a^{-1} \in F$ and $b^{-1} \in F$. Since $F$ is closed under multiplication, then $a^{-1}b^{-1} \in F$. Since $F$ is a field, then $F$ is an integral domain, so the product of nonzero elements of $F$ is nonzero. Therefore, $ab \neq 0$, so $(ab)^{-1} \in F$.

Observe that

$$\begin{aligned} (ab)(a^{-1}b^{-1}) &= a(ba^{-1})b^{-1} \\ &= a(a^{-1}b)b^{-1} \\ &= (aa^{-1})(bb^{-1}) \\ &= 1 \cdot 1 \\ &= 1. \end{aligned}$$

and

$$\begin{aligned}
(a^{-1}b^{-1})(ab) &= a^{-1}(b^{-1}a)b \\
&= a^{-1}(ab^{-1})b \\
&= (a^{-1}a)(b^{-1}b) \\
&= 1 \cdot 1 \\
&= 1.
\end{aligned}$$

Hence, $(ab)(a^{-1}b^{-1}) = 1 = (a^{-1}b^{-1})(ab)$. Therefore, $(ab)^{-1} = a^{-1}b^{-1}$. □

*Proof.* Suppose $a \neq 0$ and $b \neq 0$.

Since $F$ is a division ring, then $(F^*, \cdot)$ is the group of units of $F$. Since $a \neq 0$, then $a \in F^*$. Hence, $a$ is a unit, so $a^{-1}$ exists. Since $b \neq 0$, then $b \in F^*$. Hence, $b$ is a unit, so $b^{-1}$ exists. Since $(F^*, \cdot)$ is a group, then $(F^*, \cdot)$ is closed under $\cdot$. Since $a \in F^*$ and $b \in F^*$, then $ab \in F^*$. Hence, $ab$ is a unit, so $(ab)^{-1}$ exists. Thus, $(ab)^{-1} = b^{-1}a^{-1}$. Since $\cdot$ is commutative, then $b^{-1}a^{-1} = a^{-1}b^{-1}$. Therefore, $(ab)^{-1} = a^{-1}b^{-1}$. □

**Corollary 6.** *Let $(F, +, \cdot)$ be a field. Let $a, b, c \in F$ such that $b \neq 0$ and $c \neq 0$. Then $\frac{ac}{bc} = \frac{a}{b}$.*

*Proof.* Since $b \neq 0$ and $c \neq 0$, then $(bc)^{-1} = b^{-1}c^{-1}$. Therefore,

$$\begin{aligned}
\frac{ac}{bc} &= (ac)(bc)^{-1} \\
&= (ac)(b^{-1}c^{-1}) \\
&= a(cb^{-1})c^{-1} \\
&= a(b^{-1}c)c^{-1} \\
&= (ab^{-1})(cc^{-1}) \\
&= (ab^{-1}) \cdot 1 \\
&= ab^{-1} \\
&= \frac{a}{b}.
\end{aligned}$$

□

**Theorem 7.** ***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)*

*Proof.* We prove 1.

We prove if $\frac{a}{b} = \frac{c}{d}$, then $ad = bc$.

Suppose $\frac{a}{b} = \frac{c}{d}$.

Then

$$\begin{aligned} ad &= a \cdot 1 \cdot d \\ &= a(b^{-1}b)d \\ &= (ab^{-1})(bd) \\ &= \frac{a}{b}(bd) \\ &= \frac{c}{d}(bd) \\ &= (cd^{-1})(bd) \\ &= (cd^{-1})(db) \\ &= c(d^{-1}d)b \\ &= c \cdot 1 \cdot b \\ &= cb \\ &= bc. \end{aligned}$$

Conversely, we prove if $ad = bc$, then $\frac{a}{b} = \frac{c}{d}$.

Suppose $ad = bc$.

Then

$$\begin{aligned} \frac{a}{b} &= ab^{-1} \\ &= b^{-1}a \\ &= (b^{-1}a)(dd^{-1}) \\ &= b^{-1}(ad)d^{-1} \\ &= b^{-1}(bc)d^{-1} \\ &= (b^{-1}b)(cd^{-1}) \\ &= cd^{-1} \\ &= \frac{c}{d}. \end{aligned}$$

We prove 2.

Since $F$ is a field and $b \neq 0$ and $d \neq 0$, then $(bd)^{-1} = b^{-1}d^{-1}$. Therefore,

$$\begin{aligned} \frac{a}{b} \cdot \frac{c}{d} &= (ab^{-1})(cd^{-1}) \\ &= a(b^{-1}c)d^{-1} \\ &= a(cb^{-1})d^{-1} \\ &= (ac)(b^{-1}d^{-1}) \\ &= (ac)(bd)^{-1} \\ &= \frac{ac}{bd}. \end{aligned}$$

We prove 3.

Suppose $c \neq 0$. Since every nonzero element of $F$ has a multiplicative inverse and $d \neq 0$, then $d^{-1} \in F$. Since $d^{-1}d = 1 = dd^{-1}$, then $d$ is a multiplicative inverse of $d^{-1}$, so $d^{-1}$ is a unit. Since every unit is nonzero, then $d^{-1} \neq 0$. Therefore,

$$\begin{aligned}
\frac{a}{b}/\frac{c}{d} &= \frac{(ab^{-1})}{(cd^{-1})} \\
&= (ab^{-1})(cd^{-1})^{-1} \\
&= (ab^{-1})(c^{-1}(d^{-1})^{-1}) \\
&= (ab^{-1})(c^{-1}d) \\
&= a(b^{-1}c^{-1})d \\
&= (ad)(b^{-1}c^{-1}) \\
&= (ad)(bc)^{-1} \\
&= \frac{ad}{bc}.
\end{aligned}$$

We prove 4.

Since $F$ is an integral domain, then the product of nonzero elements of $F$ is nonzero. Since $b \neq 0$ and $d \neq 0$, then $bd \neq 0$. Therefore,

$$\begin{aligned}
\frac{a}{b} + \frac{c}{d} &= \frac{a}{b} \cdot 1 + \frac{c}{d} \cdot 1 \\
&= \frac{a}{b}(dd^{-1}) + \frac{c}{d}(bb^{-1}) \\
&= \frac{a}{b} \cdot \frac{d}{d} + \frac{c}{d} \cdot \frac{b}{b} \\
&= \frac{ad}{bd} + \frac{cb}{db} \\
&= \frac{ad}{bd} + \frac{bc}{bd} \\
&= \frac{ad+bc}{bd}.
\end{aligned}$$

We prove 5.

Since $F$ is an integral domain, then the product of nonzero elements of $F$ is nonzero. Since $b \neq 0$ and $d \neq 0$, then $bd \neq 0$.

Therefore,

$$\begin{aligned}
\frac{a}{b} - \frac{c}{d} &= \frac{a}{b} \cdot 1 - \frac{c}{d} \cdot 1 \\
&= \frac{a}{b}(dd^{-1}) - \frac{c}{d}(bb^{-1}) \\
&= \frac{a}{b} \cdot \frac{d}{d} - \frac{c}{d} \cdot \frac{b}{b} \\
&= \frac{ad}{bd} - \frac{cb}{db} \\
&= \frac{ad}{bd} - \frac{bc}{bd} \\
&= \frac{ad - bc}{bd}.
\end{aligned}$$

□

**Theorem 8.** *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.*

*Proof.* Let $p$ be a positive integer.

We prove $\mathbb{Z}_p$ is a field iff $p$ is prime.

We first prove if $\mathbb{Z}_p$ is a field, then $p$ is prime.

Suppose $\mathbb{Z}_p$ is a field.

To prove $p$ is prime, we must prove 1 and $p$ are the only positive divisors of $p$.

Since $1|p$ and $p|p$, then this implies we must prove there is no integer $n$ such that $1 < n < p$ and $n|p$.

Suppose for the sake of contradiction that there is an integer $n$ such that $1 < n < p$ and $n|p$.

Since $1 < n < p$, then $1 < n$.

Since $n \in \mathbb{Z}$ and $n > 1$, then $n$ is a positive integer.

Since $n$ is a positive integer and $p$ is a positive integer and $n|p$, then $\gcd(n, p) = n$.

Since $n \in \mathbb{Z}$ and $1 < n < p$, then $[n] \in \mathbb{Z}_p$ and $[n] \neq [0]$, so $[n]$ is a non-zero element of $\mathbb{Z}_p$.

Since $\mathbb{Z}_p$ is a field, then every nonzero element of $\mathbb{Z}_p$ has a multiplicative inverse.

Hence, $[n]$ has a multiplicative inverse in $\mathbb{Z}_p$.

Any element $[a] \in \mathbb{Z}_p$ has a multiplicative inverse in $\mathbb{Z}_p$ iff $\gcd(a, p) = 1$.

Since $[n]$ has a multiplicative inverse in $\mathbb{Z}_p$, then this implies $\gcd(n, p) = 1$.

Thus, $n = \gcd(n, p) = 1$, so $n = 1$.

But, this contradicts the fact that $n > 1$.

Hence, there is no integer $n$ such that $1 < n < p$ and $n|p$.

Therefore, $p$ is prime. □

*Proof.* Conversely, we prove if $p$ is prime, then $\mathbb{Z}_p$ is a field.

Suppose $p$ is prime.

To prove $\mathbb{Z}_p$ is a field, we must prove $\mathbb{Z}_p$ is a commutative ring with $[1] \neq [0]$ such that every nonzero element has a multiplicative inverse.

Since $\mathbb{Z}_p$ is a commutative ring, then we need only prove $[1] \neq [0]$ and every nonzero element has a multiplicative inverse.

Let $[1]$ be the unity of $\mathbb{Z}_p$ and $[0]$ be the zero of $\mathbb{Z}_p$.

We first prove $[1] \neq [0]$.

Since $p$ is prime and $p$ is a positive integer, then $p \geq 2$.

Hence, $|\mathbb{Z}_p| = p \geq 2$, so $\mathbb{Z}_p$ contains at least two elements.

Since the zero ring has exactly one element, then $\mathbb{Z}_p$ is not the zero ring.

Since the zero ring is the only ring such that the unity element equals the zero element and $\mathbb{Z}_p$ is not the zero ring, then the unity element of $\mathbb{Z}_p$ does not equal the zero element of $\mathbb{Z}_p$.

Therefore, $[1] \neq [0]$.

We next prove every nonzero element has a multiplicative inverse.

Since $[1] \neq [0]$, then $\mathbb{Z}_p$ contains at least one nonzero element.

Let $[a]$ be an arbitrary nonzero element of $\mathbb{Z}_p$.

Then $[a] \in \mathbb{Z}_p$ and $[a] \neq [0]$.

Thus, $a \in \mathbb{Z}$ and $1 \leq a < p$.

Since $0 < 1 \leq a < p$, then $0 < a$ and $a < p$.

Since $a \in \mathbb{Z}$ and $a > 0$, then $a$ is a positive integer.

Since $a$ and $p$ are positive integers, then if $p|a$, then $p \leq a$.

Hence, if $p > a$, then $p \not| a$.

Since $p$ is prime, then either $p|a$ or $\gcd(p, a) = 1$.

Since $p \not| a$, then we conclude $\gcd(p, a) = 1$, so $\gcd(a, p) = 1$.

Since $[a]$ has a multiplicative inverse iff $\gcd(a, p) = 1$, then this implies $[a]$ has a multiplicative inverse. □

# Polynomial Rings

**Theorem 9.** *Let $R[x]$ be the set of all polynomials in variable $x$ over a ring $R$. Then $(R[x], +, *)$ is a ring with unity .*

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

Observe that $R[x] = \{\sum_{k=0}^{n} a_k x^k : (\exists n \in \tilde{N})(\forall k = 0, 1, ..., n)(a_k \in R)\}$.

We prove $(R[x], +)$ is an abelian group.

We prove $R[x]$ is closed under addition of polynomials.

Let $p, q \in R[x]$.

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 $q = \sum_{k=0}^{n} b_k x^k$.

Either $m = n$ or $m \neq n$.

Suppose $m = n$. Then $a_0, a_1, ..., a_n \in R$ and $p_k = 0$ for all $k > n$ and $p_k = a_k$ if $k \leq n$ and $p = \sum_{k=0}^{n} a_k x^k$.

Let $k \in \tilde{N}$. Either $k \leq n$ or $k > n$. If $k \leq n$, then $p_k + q_k = a_k + b_k \in R$. If $k > n$, then $p_k + q_k = 0 + 0 = 0 \in R$. Hence,

$$\begin{aligned} p + q &= \sum a_k x^k + \sum b_k x^k \\ &= \sum (p_k + q_k) x^k \\ &= \sum (a_0 + b_0) + (a_1 + b_1)x + ... + (a_n + b_n)x^n + 0 + 0 + ... \\ &= \sum (a_0 + b_0) + (a_1 + b_1)x + ... + (a_n + b_n)x^n \\ &= \sum_{k=0}^{n} (a_k + b_k)x^k. \end{aligned}$$

Therefore, $p + q \in R[x]$.

Suppose $m \neq n$. Then either $m < n$ or $m > n$. Without loss of generality, assume $m < n$. Then we may add $n - m$ zero terms of the form $0x^k$ to $p$ so that $p$ and $q$ have the same number of terms. Thus,

$$\begin{aligned} p &= a_0 + a_1 x + a_2 x^2 + ... + a_m x^m \\ &= a_0 + a_1 x + a_2 x^2 + ... + a_m x^m + 0x^{m+1} + 0x^{m+2} + ... + 0x^n \end{aligned}$$

and $q = b_0 + b_1 x + b_2 x^2 + ... + b_n x^n$.

Observe that

$$\begin{aligned} p + q &= \sum a_k x^k + \sum b_k x^k \\ &= \sum (p_k + q_k) x^k \\ &= \sum (a_0 + b_0) + (a_1 + b_1)x + ... + (a_m + b_m)x^m + (0 + b_{m+1})x^{m+1} + ... + (0 + b_n)x^n + 0 + ... \\ &= \sum (a_0 + b_0) + (a_1 + b_1)x + ... + (a_m + b_m)x^m + (0 + b_{m+1})x^{m+1} + ... + (0 + b_n)x^n \\ &= \sum (a_0 + b_0) + (a_1 + b_1)x + ... + (a_n + b_n)x^n \\ &= \sum_{k=0}^{n} (a_k + b_k)x^k. \end{aligned}$$

Consequently, $p + q \in R[x]$.

Thus, $R[x]$ is closed under addition of polynomials.

We prove polynomial addition is well defined. Let $(p, q)$ and $(r, s)$ be arbitrary elements of $R[x] \times R[x]$ such that $(p, q) = (r, s)$. Then $p = r$ and $q = s$. Thus, there exist $m, n \in \mathbb{Z}, m, n \geq 0$ such that $p = \sum_{k=0}^{m} a_k x^k$ and $q = \sum_{k=0}^{n} b_k x^k$ and $r = \sum_{k=0}^{m} c_k x^k$ and $s = \sum_{k=0}^{n} d_k x^k$ and $a_k, c_k \in R$ for each $k = 0, 1, ..., m$ and $b_k, d_k \in R$ for each $k = 0, 1, ..., n$.

Thus, $a_k = c_k$ for each $k = 0, 1, ..., m$ and $b_k = d_k$ for each $k = 0, 1, ..., n$. If $m \neq n$, we may assume without loss of generality $m < n$. Thus, we may add $n - m$ zero terms to $p$ so that $p$ and $q$ contain the same number of terms.

Observe that

$$\begin{aligned} p + q &= \sum_{k=0}^{m} a_k x^k + \sum_{k=0}^{n} b_k x^k \\ &= \sum_{k=0}^{n} a_k x^k + \sum_{k=0}^{n} b_k x^k \\ &= \sum_{k=0}^{n} (a_k + b_k) x^k \\ &= \sum_{k=0}^{n} (c_k + d_k) x^k \\ &= \sum_{k=0}^{n} c_k x^k + \sum_{k=0}^{n} d_k x^k \\ &= \sum_{k=0}^{m} c_k x^k + \sum_{k=0}^{n} d_k x^k \\ &= r + s. \end{aligned}$$

Therefore, addition of polynomials is well defined. Hence, addition of polynomials is a binary operation on $R[x]$.

We prove addition of polynomials is associative. Let $p, q, r \in R[x]$. Then there exists $n \in \mathbb{Z}, n \geq 0$ such that $p = \sum_{k=0}^{n} a_k x^k$ and $q = \sum_{k=0}^{n} b_k x^k$ and $r = \sum_{k=0}^{n} c_k x^k$ and $a_k, b_k, c_k \in R$ for each $k = 0, 1, ..., n$.

Thus,

$$\begin{aligned}(p+q)+r &= (\sum_{k=0}^{n} a_k x^k + \sum_{k=0}^{n} b_k x^k) + \sum_{k=0}^{n} c_k x^k \\ &= \sum_{k=0}^{n}(a_k+b_k)x^k + \sum_{k=0}^{n} c_k x^k \\ &= \sum_{k=0}^{n}[(a_k+b_k)+c_k]x^k \\ &= \sum_{k=0}^{n}[a_k+(b_k+c_k)]x^k \\ &= \sum_{k=0}^{n} a_k x^k + \sum_{k=0}^{n}(b_k+c_k)x^k \\ &= \sum_{k=0}^{n} a_k x^k + (\sum_{k=0}^{n} b_k x^k + \sum_{k=0}^{n} c_k x^k) \\ &= p+(q+r).\end{aligned}$$

Therefore, addition of polynomials is associative.

We prove addition of polynomials is commutative. Observe that

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

Therefore, addition of polynomials is commutative.

We prove the zero polynomial is additive identity. Let $p \in R[x]$. Then there exists $n \in \mathbb{Z}, n \geq 0$ such that $p = \sum_{k=0}^{n} a_k x^k$ and $a_k \in R$ for each $k = 0, 1, ..., n$. Since $0 = 0x^k$ for each $k = 0, 1, ..., n$, then $0 = \sum_{k=0}^{n} 0x^k$. Thus, $0 \in R[x]$.

Observe that

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

Hence, the zero polynomial is an additive identity in $R[x]$.

We prove each element of $R[x]$ has an additive inverse. Let $p \in R[x]$. Then there exists $n \in \mathbb{Z}, n \geq 0$ such that $p = \sum_{k=0}^{n} a_k x^k$ and $a_k \in R$ for each $k = 0, 1, ..., n$. Since $R$ is a ring, then $(R, +)$ is an abelian group, so each element of $R$ has an additive inverse in $R$. Thus, $-a_k \in R$ for each $k = 0, 1, ..., n$.

Let $q = \sum_{k=0}^{n}(-a_k)x^k$. Then $q \in R[x]$ and

$$\begin{aligned}
p+q &= \sum_{k=0}^{n} a_k x^k + \sum_{k=0}^{n}(-a_k)x^k \\
&= \sum_{k=0}^{n}[a_k+(-a_k)]x^k \\
&= \sum_{k=0}^{n} 0x^k \\
&= \sum_{k=0}^{n}[-a_k+a_k]x^k \\
&= \sum_{k=0}^{n}(-ak)x^k + \sum_{k=0}^{n} a_k x^k \\
&= q+p.
\end{aligned}$$

Hence, $\sum_{k=0}^{n}(-a_k)x^k$ is an additive inverse of $\sum_{k=0}^{n} a_k x^k$. Thus, each element in $R[x]$ has an additive inverse in $R[x]$.

Therefore, $(R[x], +)$ is an abelian group.

We prove $R[x]$ is closed under multiplication of polynomials.

Let $p, q \in R[x]$. Then there exist $m, n \in \mathbb{Z}, m, n \geq 0$ such that $p = \sum_{k=0}^{m} a_k x^k$ and $a_k \in R$ for each $k = 0, 1, ..., m$ and $q = \sum_{k=0}^{n} b_k x^k$ and $b_k \in R$ for each $k = 0, 1, ..., n$.

Observe that $pq = \sum_{k=0}^{n} a_k x^k \sum_{k=0}^{n} b_k x^k = \sum_{k=0}^{m+n} (c_k) x^k$, where $c_k = \sum_{i=0}^{k} a_i b_{k-i}$.

To prove $pq \in R[x]$, we must prove:

1. $m + n \in \mathbb{Z}$.

2. $m + n \geq 0$.

3. for each $k = 0, 1, ..., m + n, c_k \in R$.

Since $\mathbb{Z}$ is closed under addition, then $m + n \in \mathbb{Z}$. Since $m \geq 0$ and $n \geq 0$, then $m + n \geq 0$.

We prove $c_k \in R$ for each $k = 0, 1, ..., m + n$.

Let $K = \{0, 1, ..., m + n\}$. Then $K = \{k \in \mathbb{Z} : 0 \leq k \leq m + n\}$.

Let $a_k = 0$ for each $k = m + 1, m + 2, ..., m + n$. Since $0 \in R$, then $a_k \in R$ for each $k = m + 1, m + 2, ..., m + n$. Since $a_k \in R$ for each $k = 0, 1, ..., m$ and $a_k \in R$ for each $k = m + 1, m + 2, ..., m + n$, then $a_k \in R$ for each $k \in K$.

Let $b_k = 0$ for each $k = n + 1, n + 2, ..., n + m$. Since $0 \in R$, then $b_k \in R$ for each $k = n + 1, n + 2, ..., n + m$. Since $b_k \in R$ for each $k = 0, 1, ..., n$ and $b_k \in R$ for each $k = n + 1, n + 2, ..., n + m$, then $b_k \in R$ for each $k \in K$.

Hence, $a_k \in R$ and $b_k \in R$ for each $k \in K$.

Let $k \in K$. Then $k \in \mathbb{Z}$ and $0 \leq k \leq m + n$.

To prove $c_k \in R$, we must prove $\sum_{i=0}^{k} a_i b_{k-i} \in R$.

We prove $a_i \in R$ and $b_{k-i} \in R$ for each $i = 0, 1, ..., k$.

We first prove $a_i \in R$.

Let $I_k = \{0, 1, ..., k\}$. Then $I_k = \{i \in \mathbb{Z} : 0 \leq i \leq k\}$.

Let $i \in I_k$. Then $i \in \mathbb{Z}$ and $0 \leq i \leq k$. Thus, $0 \leq i$ and $i \leq k$. Since $0 \leq k \leq m + n$, then $0 \leq k$ and $k \leq m + n$. Since $i \leq k$ and $k \leq m + n$, then $i \leq m + n$. Since $0 \leq i$ and $i \leq m + n$, then $0 \leq i \leq m + n$. Hence, $i \in K$. Thus, $i \in I_k$ implies $i \in K$, so $I_k \subset K$. Since $i \in K$, then $a_i \in R$.

We prove $b_{k-i} \in R$.

Since $\mathbb{Z}$ is closed under subtraction, then $k - i \in \mathbb{Z}$.

Since $i \leq k$, then $0 \leq k - i$. Since $0 \leq i$, then $0 \geq -i$. Hence, $k \geq k - i$, so $k - i \leq k$. Thus, $0 \leq k - i$ and $k - i \leq k$, so $0 \leq k - i \leq k$. Therefore, $k - i \in I_k$. Since $I_k \subset K$, then $k - i \in K$. Hence, $b_{k-i} \in R$.

Since $R$ is a ring, then $R$ is closed under multiplication. Thus, $a_i b_{k-i} \in R$.

Since $k$ is arbitrary, then $a_i b_{k-i} \in R$ for each $k \in K$. Thus, $a_i b_{k-i} \in R$ for each $k = 0, 1, ..., m + n$.

Since $R$ is closed under addition, then $\sum_{i=0}^{k} a_i b_{k-i} \in R$. Therefore, $c_k \in R$.

Hence, $pq \in R[x]$.

Thus, $R[x]$ is closed under multiplication of polynomials.

We prove polynomial multiplication is well defined. Let $(p, q)$ and $(r, s)$ be arbitrary elements of $R[x] \times R[x]$ such that $(p, q) = (r, s)$. Then $p = r$ and $q = s$. Hence, there exist $m, n \in \mathbb{Z}, m, n \geq 0$ such that $p = \sum_{k=0}^{m} a_k x^k$ and $q = \sum_{k=0}^{n} b_k x^k$ and $r = \sum_{k=0}^{m} c_k x^k$ and $s = \sum_{k=0}^{n} d_k x^k$ and $a_k, c_k \in R$ for each $k = 0, 1, ..., m$ and $b_k, d_k \in R$ for each $k = 0, 1, ..., n$ and $a_k = c_k$ for each $k = 0, 1, ..., m$ and $b_k = d_k$ for each $k = 0, 1, ..., n$.

Observe that $pq = \sum_{k=0}^{m+n} e_k x^k$, where $e_k = \sum_{i=o}^{k} a_i b_{k-i}$ and $rs = \sum_{k=0}^{m+n} f_k x^k$, where $f_k = \sum_{i=o}^{k} c_i d_{k-i}$.

To prove $pq = rs$, we must prove $e_k = f_k$ for each $k = 0, 1, ..., m + n$.

Let $a_k = c_k = 0$ for each $k = m + 1, m + 2, ..., m + n$. Since $a_k = c_k$ for each $k = 0, 1, ..., m$, then this implies $a_k = c_k$ for each $k = 0, 1, ..., m + n$.

Let $b_k = d_k = 0$ for each $k = n + 1, n + 2, ..., n + m$. Since $b_k = d_k$ for each $k = 0, 1, ..., n$, then this implies $b_k = d_k$ for each $k = 0, 1, ..., n + m$.

Thus, $a_k = c_k$ and $b_k = d_k$ for each $k = 0, 1, ..., m + n$.

Let $K = \{0, 1, ..., m + n\}$. Then $a_k = c_k$ and $b_k = d_k$ for all $k \in K$.

Let $k \in K$.

Let $I_k = \{0, 1, ..., k\}$. Then $I_k \subset K$. Hence, for all $i \in I_k, i \in K$. Thus, for all $i \in I_k$, $a_i = c_i$ and $b_i = d_i$. Consequently, for all $i = 0, 1, ..., k$, $a_i = c_i$ and $b_i = d_i$.

Observe that

$$\begin{aligned}
e_k &= \sum_{i=o}^{k} a_i b_{k-i} \\
&= a_0 b_k + a_1 b_{k-1} + ... + a_{k-1} b_1 + a_k b_0 \\
&= c_0 b_k + c_1 b_{k-1} + ... + c_{k-1} b_1 + c_k b_0 \\
&= c_0 d_k + c_1 d_{k-1} + ... + c_{k-1} d_1 + c_k d_0 \\
&= \sum_{i=0}^{k} c_i d_{k-i} \\
&= f_k.
\end{aligned}$$

Therefore $pq = rs$, so multiplication of polynomials is well defined. Hence, multiplication of polynomials is a binary operation on $R[x]$.

□