Denote by B any one of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.	Regard $\mathbb{R}^n$ as the set of all vectors on the 'real n-dimensional space'.	
⓪ For any $s, t \in B$, $s+t \in B$.	⓪ For any $v, w \in \mathbb{R}^n$, $v+w \in \mathbb{R}^n$.	⓪ Law of Closedness (for Addition).
① For any $r, s, t \in B$, $(r+s)+t = r+(s+t)$.	① For any $u, v, w \in \mathbb{R}^n$, $(u+v)+w = u+(v+w)$.	① Law of Associativity (for Addition).
② $0 \in B$, and for any $r \in B$, $r+0 = r = 0+r$.	② $0 \in \mathbb{R}^n$, and for any $u \in \mathbb{R}^n$, $u+0 = u = 0+u$.	② Law of Existence of (Additive) Identity.
③ For any $r \in B$, ($-r \in B$ and $(-r)+r = 0 = r+(-r)$).	③ For any $u \in \mathbb{R}^n$, ($-u \in \mathbb{R}^n$ and $(-u)+u = 0 = u+(-u)$).	③ Law of Existence of (Additive) Inverse.
④ For any $s, t \in B$, $s+t = t+s$.	④ For any $v, w \in \mathbb{R}^n$, $v+w = w+v$.	④ Law of Commutativity (for Addition).

Denote by B any one of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.	Regard $\mathbb{R}^n$ as the set of all vectors in the 'real n-dimensional space'.	Denote by B^* any one of $\mathbb{Q}\setminus\{0\}, \mathbb{R}\setminus\{0\}, \mathbb{C}\setminus\{0\}$.	
⓪ For any $s, t \in B$, $s+t \in B$.	⓪ For any $v, w \in \mathbb{R}^n$, $v+w \in \mathbb{R}^n$.	⓪ For any $s, t \in B^*$, $s \cdot t \in B^*$.	⓪ Law of Closedness (for Multiplication).
① For any $r, s, t \in B$, $(r+s)+t = r+(s+t)$.	① For any $u, v, w \in \mathbb{R}^n$, $(u+v)+w = u+(v+w)$.	① For any $r, s, t \in B^*$, $(r \cdot s) \cdot t = r \cdot (s \cdot t)$.	① Law of Associativity (for Multiplication).
② $0 \in B$, and for any $r \in B$, $r+0 = r = 0+r$.	② $0 \in \mathbb{R}^n$, and for any $u \in \mathbb{R}^n$, $u+0 = u = 0+u$.	② $1 \in B^*$, and for any $r \in B^*$, $r \cdot 1 = r = 1 \cdot r$.	② Law of Existence of (Multiplicative) Identity.
③ For any $r \in B$, ($-r \in B$ and $(-r)+r = 0 = r+(-r)$).	③ For any $u \in \mathbb{R}^n$, ($-u \in \mathbb{R}^n$ and $(-u)+u = 0 = u+(-u)$).	③ For any $r \in B^*$, ($r^{-1} \in B^*$ and $r^{-1} \cdot r = 1 = r \cdot r^{-1}$).	③ Law of Existence of (Multiplicative) Inverse.
④ For any $s, t \in B$, $s+t = t+s$.	④ For any $v, w \in \mathbb{R}^n$, $v+w = w+v$.	④ For any $s, t \in B^*$, $s \cdot t = t \cdot s$.	④ Law of Commutativity (for Multiplication).

Denote by B any one of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.	Regard $\mathbb{R}^n$ as the set of all vectors on the 'real n-dimensional space'.	Denote by M the set of all $(m \times n)$-matrices with real entries.	
⓪ For any $s, t \in B$, $s+t \in B$.	⓪ For any $v, w \in \mathbb{R}^n$, $v+w \in \mathbb{R}^n$.	⓪ For any $J, K \in M$, $J+K \in M$.	⓪ Law of Closedness (for Addition).
① For any $r, s, t \in B$, $(r+s)+t = r+(s+t)$.	① For any $u, v, w \in \mathbb{R}^n$, $(u+v)+w = u+(v+w)$.	① For any $H, J, K \in M$, $(H+J)+K = H+(J+K)$.	① Law of Associativity (for Addition).
② $0 \in B$, and for any $r \in B$, $r+0 = r = 0+r$.	② $0 \in \mathbb{R}^n$, and for any $u \in \mathbb{R}^n$, $u+0 = u = 0+u$.	② $O \in M$, and for any $H \in M$, $H+O = H = O+H$.	② Law of Existence of (Additive) Identity.
③ For any $r \in B$, ($-r \in B$ and $(-r)+r = 0 = r+(-r)$).	③ For any $u \in \mathbb{R}^n$, ($-u \in \mathbb{R}^n$ and $(-u)+u = 0 = u+(-u)$).	③ For any $H \in M$, ($-H \in M$ and $(-H)+H = O = H+(-H)$).	③ Law of Existence of (Additive) Inverse.
④ For any $s, t \in B$, $s+t = t+s$.	④ For any $v, w \in \mathbb{R}^n$, $v+w = w+v$.	④ For any $J, K \in M$, $J+K = K+J$.	④ Law of Commutativity (for Addition).

1. **Definition.**

Let K, L, M be non-empty sets, and $\varphi : K^2 \longrightarrow L$ be a function.

Suppose M is both a subset of K and a subset of L.

Then φ is said to define a **closed binary operation** *on M if $\varphi(x, y) \in M$ for any $x, y \in M$.*

Remark on notation.

Where φ is a indeed a closed binary operation on M, we agree to write

$$\varphi(x, y)$$

as

$$x\varphi y$$

for any $x, y \in M$.

2. **Definition.**

Let A be a non-empty set, and $\bullet$ be a closed binary operation on A.

We say $(A, \bullet)$ is an **abelian group** *(or, A forms an abelian group under $\bullet$,) if it satisfies the conditions* (AG1)-(AG4) *below:*

(AG1) *For any $r, s, t \in A$, $(r \bullet s) \bullet t = r \bullet (s \bullet t)$.*

(AG2) *There exists some $e \in A$ such that for any $r \in A$, $e \bullet r = r = r \bullet e$.*

(AG3) *For any $r \in A$, there exists some $v \in A$ such that $v \bullet r = r \bullet v = e$.*

(AG4) *For any $s, t \in A$, $s \bullet t = t \bullet s$.*

Remarks on terminologies.

- By virtue of (AG1), we say the **Law of Associativity** holds in $(A, \bullet)$.
- By virtue of (AG2), we say the **Law of Existence of Identity** holds in $(A, \bullet)$, and e is called an **identity element** of $(A, \bullet)$.
- By virtue of (AG3), we say the **Law of Existence of Inverse** holds in $(A, \bullet)$, and each such v is called an **inverse** of the corresponding r in $(A, \bullet)$.
- By virtue of (AG4), we say the **Law of Commutativity** holds in $(A, \bullet)$.

Denote by B any one of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

⓪ For any $s, t \in B$, $s + t \in B$.

① For any $r, s, t \in B$, $(r+s)+t = r+(s+t)$.

② $0 \in B$, and for any $r \in B$, $r+0 = r = 0+r$.

③ For any $r \in B$, $(-r \in B$ and $(-r)+r = 0 = r+(-r))$.

④ For any $s, t \in B$, $s+t = t+s$.

Regard $\mathbb{R}^n$ as the set of all vectors in the 'real n-dimensional space'.

⓪ For any $v, w \in \mathbb{R}^n$, $v+w \in \mathbb{R}^n$.

① For any $u, v, w \in \mathbb{R}^n$, $(u+v)+w = u+(v+w)$.

② $0 \in \mathbb{R}^n$, and for any $u \in \mathbb{R}^n$, $u+0 = u = 0+u$.

③ For any $u \in \mathbb{R}^n$, $(-u \in \mathbb{R}^n$ and $(-u)+u = 0 = u+(-u))$.

④ For any $v, w \in \mathbb{R}^n$, $v+w = w+v$.

Examples of abelian groups.

Definition for the notion of abelian groups.

Let A be a non-empty set, and $\bullet$ be a closed binary operation on A.

$(A, \bullet)$ is said to be an abelian group if ((AG0) and) (AG1)–(AG4) are all satisfied:

((AG0) For any $s, t \in A$, $s \bullet t \in A$.) [Law of Closedness.]

(AG1) For any $r, s, t \in A$, $(r \bullet s) \bullet t = r \bullet (s \bullet t)$. [Law of Associativity.]

(AG2) There exists some $e \in A$ such that for any $r \in A$, $r \bullet e = r = e \bullet r$. [Law of Existence of Identity.]

(AG3) For any $r \in A$, there exists some $v \in A$ such that $v \bullet r = e = r \bullet v$. [Law of Existence of Inverse.]

(AG4) For any $s, t \in A$, $s \bullet t = t \bullet s$. [Law of Commutativity.]

Denote by B any one of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.	Regard $\mathbb{R}^n$ as the set of all vectors in the 'real n-dimensional space'.	Denote by B^* any one of $\mathbb{Q}\backslash\{0\}, \mathbb{R}\backslash\{0\}, \mathbb{C}\backslash\{0\}$.	Denote by M the set of all $(m\times n)$-matrices with real entries.
⓪ For any $s, t \in B$, $s+t \in B$.	⓪ For any $v, w \in \mathbb{R}^n$, $v+w \in \mathbb{R}^n$.	⓪ For any $s, t \in B^*$, $s \cdot t \in B^*$	⓪ For any $J, K \in M$, $J+K \in M$.
① For any $r, s, t \in B$, $(r+s)+t = r+(s+t)$.	① For any $u, v, w \in \mathbb{R}^n$, $(u+v)+w = u+(v+w)$.	① For any $r, s, t \in B^*$, $(r\cdot s)\cdot t = r\cdot(s\cdot t)$.	① For any $H, J, K \in M$, $(H+J)+K = H+(J+K)$.
② $0 \in B$, and for any $r \in B$, $r+0 = r = 0+r$.	② $0 \in \mathbb{R}^n$, and for any $u \in \mathbb{R}^n$, $u+0 = u = 0+u$.	② $1 \in B^*$, and for any $r \in B^*$, $r\cdot 1 = r = 1\cdot r$.	② $0 \in M$ and for any $H \in M$, $H+0 = H = 0+H$.
③ For any $r \in B$, ($-r \in B$ and $(-r)+r = 0 = r+(-r)$).	③ For any $u \in \mathbb{R}^n$, ($-u \in \mathbb{R}^n$ and $(-u)+u = 0 = u+(-u)$).	③ For any $r \in B^*$, ($r^{-1} \in B^*$ and $r^{-1}\cdot r = 1 = r\cdot r^{-1}$).	③ For any $H \in M$, ($-H \in M$ and $(-H)+H = 0 = H+(-H)$).
④ For any $s, t \in B$, $s+t = t+s$.	④ For any $v, w \in \mathbb{R}^n$, $v+w = w+v$.	④ For any $s, t \in B^*$, $s\cdot t = t\cdot s$.	④ For any $J, K \; M$, $J+K = K+J$.

Examples of abelian groups.

Denote by B any one of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.	Regard $\mathbb{R}^n$ as the set of all vectors in the 'real n-dimensional space'.	Denote by S^1 the set $\{z \in \mathbb{C} : \lvert z \rvert = 1\}$. ($S^1$ is the set of all complex numbers of modulus 1.)	Define $Z_n = \{\zeta \in \mathbb{C} : \zeta^n = 1\}$. (Here n is a positive integer. Z_n is the set of all n-th roots of unity.)
⓪ For any $s, t \in B$, $s + t \in B$.	⓪ For any $v, w \in \mathbb{R}^n$, $v + w \in \mathbb{R}^n$.	⓪ For any $z, w \in S^1$, $z \cdot w \in S^1$.	⓪ For any $\zeta, \omega \in Z_n$, $\zeta \cdot \omega \in Z_n$.
① For any $r, s, t \in B$, $(r+s)+t = r+(s+t)$.	① For any $u, v, w \in \mathbb{R}^n$, $(u+v)+w = u+(v+w)$.	① For any $z, w, v \in S^1$, $(z \cdot w) \cdot v = z \cdot (w \cdot v)$.	① For any $\zeta, \omega, \eta \in Z_n$, $(\zeta \cdot \omega) \cdot \eta = \zeta \cdot (\omega \cdot \eta)$.
② $0 \in B$, and for any $r \in B$, $r + 0 = r = 0 + r$.	② $0 \in \mathbb{R}^n$, and for any $u \in \mathbb{R}^n$, $u + 0 = u = 0 + u$.	② $1 \in S^1$, and for any $z \in S^1$, $z \cdot 1 = z = 1 \cdot z$.	② $1 \in Z_n$, and for any $\zeta \in Z_n$, $\zeta \cdot 1 = \zeta = 1 \cdot \zeta$.
③ For any $r \in B$, ($-r \in B$ and $(-r) + r = 0 = r + (-r)$).	③ For any $u \in \mathbb{R}^n$, ($-u \in \mathbb{R}^n$ and $(-u) + u = 0 = u + (-u)$).	③ For any $z \in S^1$, ($z^{-1} \in S^1$ and $z^{-1} \cdot z = 1 = z \cdot z^{-1}$).	③ For any $\zeta \in Z_n$, ($\zeta^{-1} \in Z_n$ and $\zeta^{-1} \cdot \zeta = 1 = \zeta \cdot \zeta^{-1}$).
④ For any $s, t \in B$, $s + t = t + s$.	④ For any $v, w \in \mathbb{R}^n$, $v + w = w + v$.	④ For any $z, w \in S^1$, $z \cdot w = w \cdot z$.	④ For any $\zeta, \omega \in Z_n$, $\zeta \cdot \omega = \omega \cdot \zeta$.

Examples of abelian groups.

3. **Theorem (1).**

Let $(A, \bullet)$ be an abelian group. The following statements hold:

(a) *$(A, \bullet)$ has a unique identity element.*

(b) *Every element of A has a unique inverse in $(A, \bullet)$.*

(c) *For any $r, s \in A$, there exists some unique $t \in A$ such that $r = s \bullet t$.* (Or equivalent, *for any $r, s \in A$, the equation $r = s \bullet u$ with unknown u in A has a unique solution.*)

Remarks on terminologies and notations.

(a) When the symbol for the closed binary operation in an abelian group is '$+$' or '$\oplus$', we tend to refer to it as 'addition', and refer to the abelian group as an additive group.

We tend to denote its identity element denoted by '0' and call it 'zero'.

We tend to denote the inverse of any r in the additive group as $-r$ and call it 'minus r'.

For any $r, s \in A$, we present the unique solution to the equation $r = s + u$ with unknown u in A as $u = r - s$, and refer to '$r - s$' as the difference of r from s, or the resultant of s subtracted from r.

(b) When the symbol for the closed binary operation in an abelian group is '$\times$' or '$\cdot$' or '$\bullet$', we tend to refer to it as 'multiplication', and refer to the abelian group as a multiplicative group.

We tend to write '$r \bullet s$' as 'rs', omitting the symbol for the closed binary operation altogether.

We tend to denote its identity element denoted by '1' and call it 'one'.

We tend to denote the inverse of any r in the multiplicative group as r^{-1} and call it 'r-inverse'.

For any $r, s \in A$, we present the unique solution to equation $r = su$ with unknown u in A as $u = rs^{-1}$, and refer to 'rs^{-1}' as the quotient of r over s, or the resultant of r divided by s.

4. **Examples and non-examples of abelian groups.**

(a) Each of $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ is an abelian group. Here $+$ is the usual addition of numbers.

(b) $(\mathbb{R}, -)$ is not an abelian group, because it fails to satisfy (AG1).

(c) $(\mathbb{N}, +)$ is not an abelian group, because it fails to satisfy (AG3).

(d) Each of $(\mathbb{Q}\backslash\{0\}, \cdot)$, $(\mathbb{R}\backslash\{0\}, \cdot)$, $(\mathbb{C}\backslash\{0\}, \cdot)$ is an abelian group. Here $\cdot$ is the usual multiplication of numbers.

$(\mathbb{N}, \cdot)$ is not an abelian group, because it fails to satisfy (AG3).

(e) $((0, +\infty), \cdot)$ is an abelian group.

$((0, +\infty), +)$ is not an abelian group, because it fails to satisfy (AG2).

(f) Denote by $\mathbb{S}^1$ the set $\{z \in \mathbb{C} : |z| = 1\}$.

$(\mathbb{S}^1, \cdot)$ is an abelian group.

(g) For each $n \in \mathbb{N}\backslash\{0\}$, define $Z_n = \{\zeta \in \mathbb{C} : \zeta^n = 1\}$. ($Z_n$ is the set of all n-th roots of unity.)

$(Z_n, \cdot)$ is an abelian group.

(h) Denote by $\mathsf{Mat}_{m\times n}(\mathbb{R})$ the set of all $(m \times n)$-matrices with real entries.

$(\mathsf{Mat}_{m\times n}(\mathbb{R}), +)$ is an abelian group. Here $+$ is the usual matrix addition.

$(\mathsf{Mat}_{m\times n}(\mathbb{R}), \cdot)$ is not an abelian group because it fails to satisfy (AG3). Here $\cdot$ is the usual matrix multiplication.

(i) Denote by $\mathsf{GL}(\mathbb{R}^n)$ the set of all $(n \times n)$-invertible matrices with real entries.

When $n \geq 2$, $(\mathsf{GL}(\mathbb{R}^n), \cdot)$ is a not an abelian group, because it fails to satisfy (AG4).

5. **Theorem (2).**

Let $(A, +)$ be an abelian group. The statements below hold:

(a) *For any $r, s, t \in A$, if $r + t = s + t$ then $r = s$.*

(b) *For any $r \in A$, $-(-r) = r$.*

(c) *For any $r, s \in A$, $r + (-s) = r - s$.*

(d) *For any $r, s \in A$, $-(r + s) = (-r) + (-s)$.*

6. **Comments.**

You may wonder why we still bother to introduce such abstract notions like *abelian groups*, when this concept apparently yields 'nothing' we don't know already from the 'concrete examples' of these mathematical objects.

(Do we not under how 'addition' and 'multiplication' in the world of numbers behave, without ever knowing anything about *abelian groups*?)

In fact, the power of *algebra* is in the

unifying of (seemingly unrelated) concepts.

Theorem (1) together with Theorem (2) is a case in point. Having proved them, which applies to arbitrary abelian groups, there will be no need to verify them again on any mathematical object which is known to be an abelian group. (We can simply state that because so-and-so is an abelian group, it will possess the properties as described in Theorem (1) and Theorem (2).)

This will save a lot of time and effort, (which can be put to better use elsewhere).

$\mathbb{F}$ is one of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.	$\mathbb{Z}$	
⓪ $(\mathbb{F}, +)$ is an abelian group with additive identity 0.	⓪ $(\mathbb{Z}, +)$ is an abelian group with additive identity 0.	
① $a \cdot b \in \mathbb{F}$ for any $a, b \in \mathbb{F}$.	① $m \cdot n \in \mathbb{Z}$ for any $m, n \in \mathbb{Z}$.	① Law of Closedness for Multiplication.
② $a \cdot b = b \cdot a$ for any $a, b \in \mathbb{F}$.	② $m \cdot n = n \cdot m$ for any $m, n \in \mathbb{Z}$.	② Law of Commutativity for Multiplication.
③ $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for any $a, b, c \in \mathbb{F}$.	③ $(m \cdot n) \cdot p = m \cdot (n \cdot p)$ for any $m, n, p \in \mathbb{Z}$.	③ Law of Associativity for Multiplication.
④ $1 \in \mathbb{F}$, and $a \cdot 1 = a = 1 \cdot a$ for any $a \in \mathbb{F}$.	④ $1 \in \mathbb{Z}$, and $m \cdot 1 = m = 1 \cdot m$ for any $m \in \mathbb{Z}$.	④ Law of Existence of Multiplicative Identity.
⑤ $\begin{cases} a \cdot (b+c) = (a \cdot b) + (a \cdot c) \\ (b+c) \cdot a = (b \cdot a) + (c \cdot a) \end{cases}$ for any $a, b, c \in \mathbb{F}$.	⑤ $\begin{cases} m \cdot (n+p) = (m \cdot n) + (m \cdot p) \\ (n+p) \cdot m = (n \cdot m) + (p \cdot m) \end{cases}$ for any $m, n, p \in \mathbb{Z}$.	⑤ Distributive Laws for Addition and Multiplication.
⑥ For any $a, b \in \mathbb{F}$, if $a \cdot b = 0$ then $a = 0$ or $b = 0$.	⑥ For any $m, n \in \mathbb{Z}$, if $m \cdot n = 0$ then $m = 0$ or $n = 0$.	⑥ Law of Non-existence of Zero Divisors.
⑦ For any $a \in \mathbb{F} \setminus \{0\}$, there exists some $b \in \mathbb{F}$, namely $b = 1/a$, such that $ab = 1 = ba$.		⑦ Law of Existence of Multiplicative Inverse.

$\mathbb{F}$ is one of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.	$\mathbb{Z}$	Denote by $\mathbb{R}[x]$ the set of all polynomials with real coefficients and with indeterminate x.
⓪ $(\mathbb{F}, +)$ is an abelian group with additive identity 0.	⓪ $(\mathbb{Z}, +)$ is an abelian group with additive identity 0.	⓪ $(\mathbb{R}[x], +)$ is an abelian group with additive identity 0.
① $a \cdot b \in \mathbb{F}$ for any $a, b \in \mathbb{F}$.	① $m \cdot n \in \mathbb{Z}$ for any $m, n \in \mathbb{Z}$.	① $f(x) \cdot g(x) \in \mathbb{R}[x]$ for any $f(x), g(x) \in \mathbb{R}[x]$.
② $a \cdot b = b \cdot a$ for any $a, b \in \mathbb{F}$.	② $m \cdot n = n \cdot m$ for any $m, n \in \mathbb{Z}$.	② $f(x) \cdot g(x) = g(x) \cdot f(x)$ for any $f(x), g(x) \in \mathbb{R}[x]$.
③ $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for any $a, b, c \in \mathbb{F}$.	③ $(m \cdot n) \cdot p = m \cdot (n \cdot p)$ for any $m, n, p \in \mathbb{Z}$.	③ $(f(x) \cdot g(x)) \cdot h(x) = f(x) \cdot (g(x) \cdot h(x))$ for any $f(x), g(x), h(x) \in \mathbb{R}[x]$.
④ $1 \in \mathbb{F}$, and $a \cdot 1 = a = 1 \cdot a$ for any $a \in \mathbb{F}$.	④ $1 \in \mathbb{Z}$, and $m \cdot 1 = m = 1 \cdot m$ for any $m \in \mathbb{Z}$.	④ $1 \in \mathbb{R}[x]$, and $f(x) \cdot 1 = f(x) = 1 \cdot f(x)$ for any $f(x) \in \mathbb{R}[x]$.
⑤ $\begin{cases} a \cdot (b+c) = (a \cdot b) + (a \cdot c) \\ (b+c) \cdot a = (b \cdot a) + (c \cdot a) \end{cases}$ for any $a, b, c \in \mathbb{F}$.	⑤ $\begin{cases} m \cdot (n+p) = (m \cdot n) + (m \cdot p) \\ (n+p) \cdot m = (n \cdot m) + (p \cdot m) \end{cases}$ for any $m, n, p \in \mathbb{Z}$.	⑤ $\begin{cases} f(x) \cdot (g(x) + h(x)) = (f(x) \cdot g(x)) + (f(x) \cdot h(x)) \\ (g(x) + h(x)) \cdot f(x) = (g(x) \cdot f(x)) + (h(x) \cdot f(x)) \end{cases}$ for any $f(x), g(x), h(x) \in \mathbb{R}[x]$.
⑥ For any $a, b \in \mathbb{F}$, if $a \cdot b = 0$ then $a = 0$ or $b = 0$.	⑥ For any $m, n \in \mathbb{Z}$, if $m \cdot n = 0$ then $m = 0$ or $n = 0$.	⑥ For any $f(x), g(x) \in \mathbb{R}[x]$, if $f(x) \cdot g(x) = 0$ then $f(x) = 0$ or $g(x) = 0$.
⑦ For any $a \in \mathbb{F} \setminus \{0\}$, there exists some $b \in \mathbb{F}$, namely $b = 1/a$, such that $ab = 1 = ba$.		

$\mathbb{F}$ is one of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.	$\mathbb{Z}$	Denote by $C(I)$ the set of all real-valued functions on some open interval I which is continuous on I.
⓪ $(\mathbb{F}, +)$ is an abelian group with additive identity 0.	⓪ $(\mathbb{Z}, +)$ is an abelian group with additive identity 0.	⓪ $(C(I), +)$ is an abelian group with additive identity 0.
① $a \cdot b \in \mathbb{F}$ for any $a, b \in \mathbb{F}$.	① $m \cdot n \in \mathbb{Z}$ for any $m, n \in \mathbb{Z}$.	① $f \cdot g \in C(I)$ for any $f, g \in C(I)$.
② $a \cdot b = b \cdot a$ for any $a, b \in \mathbb{F}$.	② $m \cdot n = n \cdot m$ for any $m, n \in \mathbb{Z}$.	② $f \cdot g = g \cdot f$ for any $f, g \in C(I)$.
③ $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for any $a, b, c \in \mathbb{F}$.	③ $(m \cdot n) \cdot p = m \cdot (n \cdot p)$ for any $m, n, p \in \mathbb{Z}$.	③ $(f \cdot g) \cdot h = f \cdot (g \cdot h)$ for any $f, g, h \in C(I)$.
④ $1 \in \mathbb{F}$, and $a \cdot 1 = a = 1 \cdot a$ for any $a \in \mathbb{F}$.	④ $1 \in \mathbb{Z}$, and $m \cdot 1 = m = 1 \cdot m$ for any $m \in \mathbb{Z}$.	④ $1 \in C(I)$, and $f \cdot 1 = f = 1 \cdot f$ for any $f \in C(I)$.
⑤ $\begin{cases} a \cdot (b+c) = (a \cdot b) + (a \cdot c) \\ (b+c) \cdot a = (b \cdot a) + (c \cdot a) \end{cases}$ for any $a, b, c \in \mathbb{F}$.	⑤ $\begin{cases} m \cdot (n+p) = (m \cdot n) + (m \cdot p) \\ (n+p) \cdot m = (n \cdot m) + (p \cdot m) \end{cases}$ for any $m, n, p \in \mathbb{Z}$.	⑤ $\begin{cases} f \cdot (g+h) = (f \cdot g) + (f \cdot h) \\ (g+h) \cdot f = (g \cdot f) + (h \cdot f) \end{cases}$ for any $f, g, h \in C(I)$.
⑥ For any $a, b \in \mathbb{F}$, if $a \cdot b = 0$ then $a = 0$ or $b = 0$.	⑥ For any $m, n \in \mathbb{Z}$, if $m \cdot n = 0$ then $m = 0$ or $n = 0$.	
⑦ For any $a \in \mathbb{F} \setminus \{0\}$, there exists some $b \in \mathbb{F}$, namely $b = 1/a$, such that $ab = 1 = ba$.		

7. **Definition.**

Let S be a set with at least two elements, and $+, \times$ be two closed binary operation on S, called addition and multiplication respectively.

We say $(S, +, \times)$ is a **commutative ring with unity** *(or, S forms a commutative ring with unity under addition $+$ and multiplication $\times$,) if it satisfies the conditions* (CR0)-(CR4) *below:*

(CR0) $(S, +)$ *is an abelian group, with additive identity* 0.

(CR1) *For any $a, b, c \in S$, $(a \times b) \times c = a \times (b \times c)$.*

(CR2) *There exists some $e \in S \backslash \{0\}$ such that for any $a \in S$, $e \times a = a = a \times e$.*

(CR3) *For any $a, b \in S$, $a \times b = b \times a$.*

(CR4) *For any $a, b, c \in S$, $a \times (b + c) = (a \times b) + (a \times c)$ and $(a + b) \times c = (a \times c) + (b \times c)$.*

Suppose $(S, +, \times)$ is indeed a commutative ring with unity.

(a) $(S, +, \times)$ *is called an* **integral domain** *if it satisfies the condition* (ID) *below:*

(ID) *For any $a, b \in S$, if $a \times b = 0$ then $a = 0$ or $b = 0$.*

(b) $(S, +, \times)$ *is called a* **field** *if it satisfies the condition* (FI) *below:*

(FI) *For any $a \in S \backslash \{0\}$, there exists some $v \in S$ such that $a \times v = v \times a = e$.*

Remarks on terminologies.

- By virtue of (CR1), we say the **Law of Associativity** holds for multiplication in $(S, +, \times)$.
- By virtue of (CR2), we say the **Law of Existence of Multiplicative Identity** holds in $(S, +, \times)$, and e is called a **multiplicative identity** of $(S, +, \times)$.
- By virtue of (CR3), we say the **Law of Commutativity** holds for multiplication in $(S, +, \times)$.
- By virtue of (CR4), we say the **Distributive Laws** holds in $(S, +, \times)$.
- The statement (ID) is referred to as the **Law of Non-existence of Zero Divisor** for the integral domain $(S, +, \times)$.
- The statement (FI) is referred to as the **Law of Existence of multiplicative inverse** for the field $(S, +, \times)$. Each such v is called a **multiplicative inverse** of the corresponding a in $(F, +, \times)$.

	Commutative Ring with Unity?	Integral Domain?	Field?
$(\mathbb{Q}, +, \cdot)$	Yes	Yes	Yes
$(\mathbb{R}, +, \cdot)$	Yes	Yes	Yes
$(\mathbb{C}, +, \cdot)$	Yes	Yes	Yes
$(\mathbb{Z}, +, \cdot)$	Yes	Yes	No
$(\mathbb{R}[x], +, \cdot)$	Yes	Yes	No
$(C(I), +, \cdot)$	Yes	No	No

8. **Examples and non-examples of commutative rings with unity, integral domains and fields.**

(a) Each of $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ is an integral domain.

Each of $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ is a field.

$(\mathbb{Z}, +, \times)$ is not a field.

(b) $(\mathbb{N}, +, \times)$ is not a commutative ring with unity, because it fails to satisfy (CR0).

(c) $((0, +\infty), +, \cdot)$ is not a commutative ring with unity, because it fails to satisfy (CR0).

(d) Whenever $n \geq 2$, $(\mathsf{Mat}_{n\times n}(\mathbb{R}), +, \cdot)$ is not a commutative ring with unity, because it fails to satisfy (CR3).

(e) Denote by $\mathbb{G}$ the set $\{z \in \mathbb{C} : \mathsf{Re}(z) \in \mathbb{Z} \text{ and } \mathsf{Im}(z) \in \mathbb{Z}\}$.

$(\mathbb{G}, +, \times)$ is an integral domain.

($\mathbb{G}$ is known as the 'system of Gaussian integers'.)

(f) Denote by $\mathbb{R}[x]$ the set of all polynomials with real coefficients.

$(\mathbb{R}[x], +)$ is an abelian group. Here $+$ is the usual polynomial addition.

$(\mathbb{R}[x], +, \times)$ is an integral domain. Here $\times$ is the usual polynomial multiplication.

$(\mathbb{R}[x], +, \times)$ is not a field.

(g) Let I be an open interval. Denote by $C(I)$ the set of all real-valued functions on I which are continuous on I.

$(C(I), +)$ is an abelian group. Here $+$ is the usual 'point-wise' addition for real-valued functions.

$(C(I), +, \times)$ is not an integral domain. Here $\times$ is the usual 'point-wise' multiplication for real-valued functions.

(h) Denote by $\mathbb{R}(x)$ the set of all rational functions with real coefficients. (Each element of $\mathbb{R}(x)$ is an expression of the form $\dfrac{f(x)}{g(x)}$ in which $f(x), g(x)$ are polynomials with real coefficients and $g(x)$ is not the zero polynomial.)

$(\mathbb{R}(x), +)$ is an abelian group.

$(\mathbb{R}(x), +, \times)$ is a field.

9. **Theorem (3).**

Let $(S, +, \times)$ be a commutative ring with unity.

The multiplicative identity of $(S, +, \times)$ is unique.

Remark on notation. We denote the multiplicative identity of $(S, +, \times)$ by 1, and call it **one**.

10. **Theorem (4).**

Let $(S, +, \times)$ be a commutative ring with unity.

(a) *For any $a \in S$, $a \times 0 = 0$.*

(b) *For any $a, b \in S$, $a \times (-b) = (-a) \times b = -(a \times b)$, and $(-a) \times (-b) = a \times b$.*

11. **Theorem (5).**

Let $(D, +, \times)$ be a integral domain.

For any $a, b, c \in D$, if $a \neq 0$ and $a \times b = a \times c$ then $b = c$.

12. **Theorem (6).**

Let $(F, +, \times)$ be a field.

(a) $(F\backslash\{0\}, \times)$ *is an abelian group.*

(b) *Every element of* $F\backslash\{0\}$ *has a unique multiplicative inverse in* $(F, +, \times)$.

(c) *For any* $a, b \in F\backslash\{0\}$, *there exists some unique* $c \in F\backslash\{0\}$ *such that* $a = b \times c$.

Remark on terminologies and notations. For each $a \in F\backslash\{0\}$, we denote the multiplicative inverse of a by a^{-1}, and refer to it as 'a-inverse'. Statement (c) can be re-formulated as:

- *For any* $a, b \in F\backslash\{0\}$, *there is a unique solution, namely* $u = a \times b^{-1}$, *for the equation* $a = bu$ *with unknown* u *in* F.

13. **Theorem (7).**

Suppose $(F, +, \times)$ *is a field. Then* $(F, +, \times)$ *is an integral domain.*

Remark. The converse of Theorem (7) is false.

14. **Definition.**

Let $(F, +, \times)$, $(E, +, \times)$ *be fields, with the same addition and multiplication.*

We say that $(F, +, \times)$ *is a* **subfield** *of* $(E, +, \times)$, *or equivalently,* $(E, +, \times)$ *is a* **field extension** *of* $(F, +, \times)$, *if* F *is a subset of* E.

Theorem (8).

Let $(E, +, \times)$ *be a field. Suppose* F *is a subset of* E.

Then F *forms a field under addition* $+$ *and multiplication* $\times$ *iff the statements hold:*

(a) $0, 1 \in F$.

(b) For any $a, b \in F$, $a + b, a - b, a \times b \in F$.

(c) For any $a, b \in F$ if $b \neq 0$ then $ab^{-1} \in F$.

15. **More examples on fields.**

The claims below can be verified with the help of Theorem (8):

(a) For each positive prime number p, define
$\mathbb{Q}[\sqrt{p}] = \{r \mid r = a + b\sqrt{p} \text{ for some } a, b \in \mathbb{Q}\}$.
$(\mathbb{Q}[\sqrt{p}], +, \times)$ is a field.
It is a subfield of $(\mathbb{R}, +, \times)$ and it is a field extension of $(\mathbb{Q}, +, \times)$.

(b) For each positive prime number p, define
$\mathbb{Q}[\sqrt[3]{p}] = \{r \mid r = a + b\sqrt[3]{p} + c(\sqrt[3]{p})^2 \text{ for some } a, b, c \in \mathbb{Q}\}$.
$(\mathbb{Q}[\sqrt[3]{p}], +, \times)$ is a field.
It is a subfield of $(\mathbb{R}, +, \times)$ and it is a field extension of $(\mathbb{Q}, +, \times)$.

(c) Define $\mathbb{Q}[i] = \{\zeta \mid \zeta = a + bi \text{ for some } a, b \in \mathbb{Q}\}$.
$(\mathbb{Q}[i], +, \times)$ is a field.
It is a subfield of $(\mathbb{C}, +, \times)$ and it is a field extension of $(\mathbb{Q}, +, \times)$.

(d) For each positive prime number p, define

$\mathbb{Q}[i\sqrt{p}] = \{\zeta \mid \zeta = a + bi\sqrt{p} \text{ for some } a, b \in \mathbb{Q}\}$.

$(\mathbb{Q}[i\sqrt{p}], +, \times)$ is a field.

It is a subfield of $(\mathbb{C}, +, \times)$ and it is a field extension of $(\mathbb{Q}, +, \times)$.

(e) For each positive prime number p, define

$\mathbb{Q}[i, \sqrt{p}] = \{\zeta \mid \zeta = a + bi + c\sqrt{p} + di\sqrt{p} \text{ for some } a, b, c, d \in \mathbb{Q}\}$.

$(\mathbb{Q}[i\sqrt{p}], +, \times)$ is a field.

It is a subfield of $(\mathbb{C}, +, \times)$ and it is a field extension of each of $(\mathbb{Q}, +, \times)$, $(\mathbb{Q}[\sqrt{p}], +, \times)$, $(\mathbb{Q}[i], +, \times)$.

(f) Write $\omega = \cos\left(\dfrac{2\pi}{3}\right) + i\sin\left(\dfrac{2\pi}{3}\right)$.

Define $\mathbb{Q}[\omega] = \{\zeta \mid \zeta = a + b\omega + c\omega^2 \text{ for some } a, b, c \in \mathbb{Q}\}$.

It will turn out that $\mathbb{Q}[\omega] = \{\zeta \mid \zeta = a + b\omega \text{ for some } a, b \in \mathbb{Q}\}$.

$(\mathbb{Q}[\omega], +, \times)$ is a field.

It is a subfield of $(\mathbb{C}, +, \times)$ and it is a field extension of $(\mathbb{Q}, +, \times)$.