0. We have come across various types of 'algebraic systems' since school days: natural numbers, integers, rational numbers, real numbers, complex numbers, polynomials, and matrices.

   Inspecting the 'rules of arithmetic' valid in the respective systems, we observe that there are a lot of similar features for various systems. For instance:

   - *For any natural numbers p, q, r, $p(q+r) = pq + pr$.*
   - *For any complex numbers p, q, r, $p(q+r) = pq + pr$.*
   - *For any polynomials $p(x), q(x), r(x)$ with real coefficients, $p(x)(q(x)+r(x)) = p(x)q(x) + p(x)r(x)$.*
   - *For any $(n \times n)$-square matrices P, Q, R with real entries, $P(Q+R) = PQ + PR$.*

   Or, for instance:

   - *For any integers p, q, there is a unique solution for the equation $p + u = q$ with unknown integer u.*
   - *For any polynomials $p(x), q(x)$ with real coefficients, there is a unique solution for the equation $p(x) + u(x) = q(x)$ with unknown polynomial $u(x)$ with real coefficients.*
   - *For any $(m \times n)$-matrices P, Q with real entries, there is a unique solution for the equation $P + U = Q$ with unknown matrix U with real entries.*

   Evidence like the above suggests the presence of some common mathematical structures beneath each of these systems.

   We are going to introduce some of these mathematical structures (abelian groups, integral domains, fields), which provide a 'framework' for unifying our understanding of those various types of 'algebraic systems' that we have encountered since school days.

   General results on these mathematical structures will resemble the basic 'rules of arithmetic' valid for these 'algebraic systems'.

   This is not surprising at a philosophical level: these 'algebraic systems' are motivation for the respective definitions of the mathematical structures in the first place, and the choice of the 'axioms' (for the respective 'mathematical structures') takes into account that the corresponding statements in the 'algebraic systems' are believed to be 'fundamental' enough that everything else about the respective 'algebraic systems' can be deduced from them.

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 $(A, \bullet)$.

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 the 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.

   Proof of Theorem (1).

   Let $(A, \bullet)$ be an abelian group.

   (a) Let $e, e' \in A$. Suppose that both e, e' are identity elements, in the sense that both $(\dagger), (\dagger')$ hold:

   ($\dagger$) For any $r \in A$, $e \bullet r = r = r \bullet e$.

   ($\dagger'$) For any $r \in A$, $e' \bullet r = r = r \bullet e'$.

   Then by $(\dagger)$ we have $e \bullet e' = e'$. By $(\dagger')$, we have $e \bullet e' = e$
   Therefore $e' = e \bullet e' = e$.

   (b) Let $r \in A$, and v, v' be an inverses of r in A in the sense that both $(\ddagger), (\ddagger')$ hold:

   ($\ddagger$) $v \bullet r = e = r \bullet v$.

   ($\ddagger'$) $v' \bullet r = e = r \bullet v'$.

   Then we have $v' = e \bullet v' = (v \bullet r) \bullet v' = v \bullet (r \bullet v') = v \bullet e = v$.
   (The first and fifth equalities are due to (AG2). The second equality is due to $(\ddagger)$. The fourth equality is due to $(\ddagger')$. The third equality is due to (AG1).)

   (c) Let $r, s \in A$.

   $*$ [Existence?] There exists some $v \in A$ such that $v \bullet s = e = s \bullet v$.
   Define $t \in A$ by $t = v \bullet r$. Then $s \bullet t = s \bullet (v \bullet r) = (s \bullet v) \bullet r = e \bullet r = r$.

   $*$ [Uniqueness?] Let $t' \in A$. Suppose $r = s \bullet t'$. Then $s \bullet t = r = s \bullet t'$.
   Therefore (for the same v above), we have $t = e \bullet t = (v \bullet s) \bullet t = v \bullet (s \bullet t) = v \bullet (s \bullet t') = (v \bullet s) \bullet t' = e \bullet t' = t'$.

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

Proof of Theorem (2).

Let $(A, +)$ be an abelian group.

(a) Let $r, s, t \in A$. Suppose $r + t = s + t$.
By (AG4), there exists some $v \in A$ such that $t + v = 0 = v + t$.
Then $r = r + 0 = r + (t + v) = (r + t) + v = (s + t) + v = s + (t + v) = s + 0 = s$.
(The first and seventh equalities are due to (AG3).)

(b) Let $r \in A$. Write $s = -r$.
By (AG3), $r + (-r) = 0$.
Also by (AG3), $(-s) + s = 0$.
Then $r + (-r) = 0 = (-s) + s = [-(-r)] + (-r)$.
Therefore by the result in (a), $r = -(-r)$.

(c) Let $r, s \in A$. Write $t = r - s$. ($u = t$ is the unique solution of the equation $r = s + u$ with unknown u in A.)
Then $t + s = s + t = r$.
Note that $[r + (-s)] + s = r + [(-s) + s] = r + 0 = r$.
Then by the result in (a), we have $t = r + (-s)$.

(d) Exercise.

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).

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 $(F, +, \times)$.

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.*

Proof of Theorem (3). Exercise.

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 $(-a) \times (-b) = a \times b$.*

    Proof of Theorem (4).

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

    (a) Let $a \in S$.
    We have $0 + 0 = 0$.
    By (CR4), we have $(a \times 0) + (a \times 0) = a \times (0 + 0) = a \times 0 = (a \times 0) + 0$.
    By Theorem (2), $a \times 0 = 0$.

    (b) Exercise.

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 $b = c$.

    Proof of Theorem (5).

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

    Let $a, b, c \in D$. Suppose $a \neq 0$ and $a \times b = a \times c$.

    Then $a \times [b + (-c)] = (a \times b) + [a \times (-c)] = (a \times c) + [-(a \times c)] = 0$.

    (The first equality is due to (CR4). the second equality is due to the result in part (b).)

    By (ID), since $a \neq 0$, we have $b + (-c) = 0$. Then $b = c$. (Why?)

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 $a = b \times c$.*

    Proof of Theorem (6). By definition, $(F \backslash \{0\}, \times)$ is an abelian group. The other statements are the consequences of Theorem (1).

    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.

    Proof of Theorem (7).

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

    Let $a, b \in F$. Suppose $a \times b = 0$.

    Note that $a = 0$ or $a \neq 0$.

    - (Case 1). Suppose $a = 0$. Then $a = 0$ or $b = 0$.
    - (Case 2). Suppose $a \neq 0$. By (FI), there exists some $c \in F$ such that $c \times a = 1$.

    Then we have
    $$b = 1 \times b = (c \times a) \times b = c \times (a \times b) = c \times 0 = 0.$$

    (The first and third equalities are due to (CR2), (CR1) respectively.)

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 $ab^{-1} \in F$.

Proof of Theorem (8). Exercise.

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 $(\mathbb{Q}, +, \times)$.