# §1. Vector Spaces

1.A Algebraic structures 1A/1 – 1A/30
(Monoids, Groups, Rings and Fields)

1.B Vector spaces — 1B/1 – 1B/9

1.C Subspaces — 1C/1 – 1C/16

# 1.A Algebraic Structures

## (Monoids, Groups, Rings and fields)

In an attempt to analyze and understand (usual) addition and multiplication of numbers, one led to the fundamental algebraic concept of a binary operation on a set.

**1.A.1 Definition** A **binary operation** on a set $G$ is a map

$$G \times G \longrightarrow G$$

usually denoted by $(x, y) \longmapsto xy$ in the multiplicative notation or by $(x, y) \longmapsto x + y$ in the additive notation. The other notations $x * y$, $x \sqcap y$, $x \sqcup y$, $x \wedge y$, $x \vee y$, $x \square y$, $x \circ y$, ... are also used.

**1.A.2 Examples** (1) On the sets $\mathbb{N} = \{0, 1, \cdots\}$, $\mathbb{Z} = \{0, \pm 1, \pm 2, \cdots\}$, $\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\}$, $\mathbb{R}$ and $\mathbb{C}$ of natural numbers, integers, rational numbers, real and complex

numbers, respectively, the usual addition + and the usual multiplication · are binary operations

(2) On the power set $\mathcal{P}(X)$ of a set $X$, union $\cup$, intersection $\cap$, complement $\setminus$, and symmetric difference are binary operations.

(4) On the sets $X^X = \mathrm{Maps}(X, X)$ of maps from a set $X$ into itself and $G(X) := \{f \in X^X \mid f \text{ is bijective}\}$ of permutations of a set $X$, the composition $\circ$ of maps is a binary operation.

1.A.3 Definitions Let $G$ be a set with a binary operation $G \times G \longrightarrow G$, $(x, y) \longmapsto xy$. Then:

(1) This binary operation is commutative or abelian if (and only if)[1] $xy = yx$ for

[1] It is customary in mathematics to omit words "and only if" from a definition. Definitions are always understood to be if and only if statements. Theorems are not always if and only if statements and no such convention is ever used for theorems.

all $x, y \in G$ ($x+y = y+x$ for all $x, y \in G$ in the additive notation); is called <u>associative</u> if $(xy)z = x(yz)$ for all $x, y, z \in G$ (in the additive notation $(x+y)+z = x+(y+z)$ for all $x, y, z \in G$.)

It is not difficult to show that if the binary operation $(x, y) \mapsto xy$ is associative, then longer expressions such as $(\cdots((x_1 x_2)x_3)x_4 \cdots)x_n$ (<u>standard-parentheses</u>) are not ambiguous (prove this by induction on $n$). Parentheses may be inserted in any fashion for purpose of computations, the final result of two such computations will be the same.

(3) An element $e \in G$ is called a <u>neutral element</u> or an <u>identity element</u> if

$$e \cdot x = x = x \cdot e \text{ for all } x \in G.$$

<u>If neutral element exists, then it is unique</u>: For if $e, e'$ are two neutral elements then $e = e \cdot e' = e'$ by definition.

(4) $G$ is called a <u>monoid</u> if the binary operation of $G$ is associative and has a neutral element.

(4) Suppose that $G$ is a monoid with neutral element $e_G = e$. An element $x' \in G$ is called an inverse of the element $x \in G$ if $x' \cdot x = e = x \cdot x'$.

For example, $e$ is a inverse of $e$, since $e \cdot e = e = e \cdot e$.

If the element $x \in G$ has an inverse then it is unique: For, if $x'$ and $x''$ are inverses of $x$, then $x' = x'e = x'(xx'') = (x'x) \cdot x'' = e \cdot x'' = x''$.

Therefore if an element $x \in G$ has the inverse, then it is denoted by $\bar{x}^{-1}$ (in the multiplicative notation) (and usually called the inverse of $x$) and $-x$ (in the additive notation) (and usually called the negative of $x$). The neutral element $e \in G$ is denoted usually by $0_G = 0$ (in the additive notation) (and usually called the zero in $G$) and by $1_G = 1$ (in the multiplicative notation). Therefore we have: (and is usually called one or unity in $G$)

$$\bar{x}^{-1} \cdot x = 1 = x \cdot \bar{x}^{-1} \quad \text{(in multiplicative notation)}$$

$$(-x) + x = 0 = x + (-x) \quad \text{(in additive notation)}$$

(5) An element $x \in G$ in a monoid $G$ is called invertible or an unit in $G$ if $x$ has an inverse in $G$. For example the neutral element $e$ is invertible; $\bar{e}^{1} = e$.

If $x, y \in G$ are invertible elements in a monoid $G$, then $x^{-1}$ and $xy$ are also invertible in $G$. Moreover, $(x^{-1})^{-1} = x$ and $(xy)^{-1} = y^{-1} \cdot x^{-1}$,

since $x \cdot x^{-1} = e = x^{-1} \cdot x$, i.e. $x$ is the inverse of $x^{-1}$ and $(y^{-1} \cdot x^{-1})(xy) = y^{-1}(x^{-1} \cdot x)y = y^{-1}ey = y^{-1}y = e = x \cdot x^{-1} = xe \cdot x^{-1} = xyy^{-1} \cdot x^{-1} = (xy)(y^{-1} \cdot x^{-1})$, i.e. $y^{-1} \cdot x^{-1}$ is the inverse of $xy$.

Therefore the binary operation of a monoid $G$ induce a binary operation on the subset $G^\times = \{x \in G \mid x \text{ is invertible in } G\} \subseteq G$ of all invertible elements in $G$, i.e. $G^\times \times G^\times \longrightarrow G^\times$, $(x, y) \longmapsto xy$.

(6) A monoid $G$ is called a group if every element $x \in G$ has an inverse in $G$, i.e. $G^\times = G$.

1.A.4 Examples (1) The usual addition $+$ and the usual multiplication $\cdot$ on the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, are commutative and associative binary operations with

neutral elements 0 and 1, respectively. Therefore $(\mathbb{N},+)$, $(\mathbb{N},\cdot)$, $(\mathbb{Z},+)$, $(\mathbb{Z},\cdot)$, $(\mathbb{Q},+)$, $(\mathbb{Q},\cdot)$, $(\mathbb{R},+)$, $(\mathbb{R},\cdot)$, $(\mathbb{C},+)$, $(\mathbb{C},\cdot)$ are all commutative monoids. Further, the monoids $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ and $(\mathbb{C},+)$ are all groups, but $(\mathbb{N},+)$, $(\mathbb{N},\cdot)$, $(\mathbb{Z},\cdot)$ are not groups, in fact, $(\mathbb{N},+)^\times=\{0\}$, $(\mathbb{N},\cdot)^\times=\{1\}$ and $(\mathbb{Z},\cdot)^\times=\{\pm 1\}$. However the monoids $(\mathbb{Q}\setminus\{0\},\cdot)$, $(\mathbb{R}\setminus\{0\},\cdot)$ and $(\mathbb{C}\setminus\{0\},\cdot)$ are groups, since $(\mathbb{Q},\cdot)^\times=\mathbb{Q}\setminus\{0\}$, $(\mathbb{R},\cdot)^\times=\mathbb{R}\setminus\{0\}$ and $(\mathbb{C},\cdot)=\mathbb{C}\setminus\{0\}$.

(2) For any set $X$, the composition $\circ$ is an associative binary operation on $X^X$ and $G(X)$. This binary operation on $G(X)$ is not commutative if $X$ has at least three elements. For if $x_1, x_2, x_3 \in X$ (distinct) and $f: X \to X$, $g: X \to X$ are defined by

$$f(x)=\begin{cases} x_2, & \text{if } x=x_1 \\ x_3, & \text{if } x=x_2 \\ x_1, & \text{if } x=x_3 \\ x, & \text{if } x\notin\{x_1,x_2,x_3\} \end{cases} \qquad g(x)=\begin{cases} x_2, & \text{if } x=x_1 \\ x_1, & \text{if } x=x_2 \\ x, & \text{if } x\notin\{x_1,x_2\} \end{cases}$$

$f, g$ are bijective, i.e. $f, g \in \mathfrak{S}(X)$ and Then $gf \neq fg$, since $(gf)(x_1) = g(f(x_1)) = g(x_2) = x_1 \neq x_3 = f(x_2) = f(g(x_1)) = (fg)(x_1)$.

Therefore $\circ$ is not commutative on bigger set $X^X$.

Moreover, $(X^X, \circ)^\times = \mathfrak{S}(X)$ and so $(\mathfrak{S}(X), \circ)$ is a group. For $f \in \mathfrak{S}(X)$, the inverse map $f^{-1}$ of $f$ is bijective $f^{-1} \in \mathfrak{S}(X)$ and it is the inverse of $f$ on the monoid $X^X$.

(Unit group of a monoid)

(3) More generally, if $G$ is a monoid, then the monoid $G^\times$ of all invertible elements in $G$ is a group. This group is called the unit group of the monoid $G$.

The group $(\mathfrak{S}(X), \circ)$ is called the permutation group on $X$, since its elements are precisely all permutations on the set $X$. If $X$ has exactly $n$ elements i.e.

$|X|=n$, then $G(X)$ has exactly $n!$ elements. Therefore $G(X)$ is a finite group. These are important examples of finite groups.

More generally, a group $G$ is called a finite group if it has finitely many elements i.e. $G$ is a finite set. In this case $|G|$ (the number of elements in $G$) is called the order of $G$.

## 1.A.5 Submonoids and subgroups

Let $G$ be a monoid. A subset $H \subseteq G$ is called a submonoid of $G$ if (i) $e \in H$. (The neutral element of $G$)

(ii) The product $xy \in H$ for all $x, y \in H$.

Therefore submonoid of a monoid $G$ is a monoid w.r.t to the induced binary operation of $G$.

If for every $x \in H$, the inverse of $x$ also belongs to $H$, then $H$ is called a subgroup of $G$.

For example, $\{\pm 1\}$ is a subgroup of

the monoid $(\mathbb{Z}, \cdot)$ and (for any set $X$) $G(X)$ is a subgroup of the monoid $(X^X, \circ)$.

1.A.6 (Powers of elements in a monoid)

Let $x_1, \dots, x_n$ be elements in a monoid $G$. Then the product $p = x_1 \cdots x_n$ is recursively defined by $p_0 := e$, $p_1 = x_1$, $\dots$, $p_{i+1} = p_i x_{i+1}$, $i = 0, \dots, n-1$ and $p := p_n$. (This is well-defined [prove this by induction on $n$] [Hence the binary operation is associative]). This is called general associativity law) product is denoted by $\prod_{i=1}^{n} x_i = x_1 \cdots x_n$ and by $\sum_{i=1}^{n} x_i = x_1 + \cdots + x_n$ in the additive notation and is called the sum of $x_1, \dots, x_n$. If the binary operation of $G$ is commutative, then the product $x_1 \cdots x_n$ does not depend on the order $x_1, \dots, x_n$ (this is general commutative law) and in this case for an arbitrary finite family $x_i$, $i \in I$ of elements in $G$ the product of $x_i$, $i \in I$

is denoted by $\prod_{i\in I} x_i$ and in the additive notation the sum of $x_i$, $i\in I$, is denoted by $\sum_{i\in I} x_i$.

For example, $\sum_{(i,j)\in I\times J} x_{ij} = \sum_{i\in I}\left(\sum_{j\in J} x_{ij}\right) =$

$\sum_{j\in J}\left(\sum_{i\in I} x_{ij}\right)$. In particular,

$$\sum_{\substack{1\le i\le m\\ 1\le j\le n}} x_{ij} = \sum_{i=1}^{m}\left(\sum_{j=1}^{n} x_{ij}\right) = \sum_{j=1}^{n}\left(\sum_{i=1}^{m} x_{ij}\right).$$

The last equality can be proved by the following scheme:

$$\begin{array}{l|l}
x_{11}+x_{12}+\cdots+x_{1n} & \sum_{j=1}^{n} x_{1j}\\
+\ x_{21}+x_{22}+\cdots+x_{2n} & +\sum_{j=1}^{n} x_{2j}\\
\vdots & \vdots\\
+\ x_{m1}+x_{m2}+\cdots+x_{mn} & +\sum_{j=1}^{n} x_{mj} = \sum_{i=1}^{m}\left(\sum_{j=1}^{n} x_{ij}\right)\\
\hline
\sum_{i=1}^{m} x_{i1}+\sum_{i=1}^{m} x_{i2}+\cdots+\sum_{i=1}^{m} x_{in} & \\
= \sum_{j=1}^{n}\left(\sum_{i=1}^{m} x_{ij}\right) &
\end{array}$$

Products with the same factor $x\in G$ are written as powers. For $x\in G$ and

$n \in \mathbb{N}$, the $n$-th power of $x$ is the $n$-fold product of $x$ with itself ($n$-times) and is denoted by $x^n$. Moreover, if $x$ is invertible element in $G$, then $x^{-n}$ is defined as $(x^{-1})^n = (x^n)^{-1}$.

In the additive notation the multiple $n \cdot x$ are defined similarly.

With these definitions, we have the following elementary rules: for all $x, y \in G$ and all $m, n \in \mathbb{N}$

$$x^{m+n} = x^m \cdot x^n, \quad (x^m)^n = x^{mn} = (x^n)^m$$

and if $x, y$ commute, then

$(xy)^m = x^m \cdot y^m$. Further, if $x$ and $y$ are invertible, then these rules hold for all $n \in \mathbb{Z}$. In the additive notation these rules are:

$(m+n)x = mx + nx$, $n(mx) = (mn)x$, $(mn)x$, $m(x+y) = mx + my$.

In the group $G$ the equations of the form $ax = b$ and $ya = b$ have unique solutions:

**1.A.7 Theorem** Let $G$ be a group. For given elements $a, b \in G$, there are unique elements $x$ and $y$ in $G$ such that $ax = b$ and $ya = b$. In fact $x = \bar{a}^1 b$ and $y = b\bar{a}^1$

**Proof** Since $a(\bar{a}^1 b) = (a\bar{a}^1)b = eb = b$ and $(b\bar{a}^1)a = b(\bar{a}^1 a) = b \cdot e = b$, $x := \bar{a}^1 b$ and $y := b\bar{a}^1$ satisfy the given equations. Conversely, if $x$ and $y$ are of $ax = b$ and $ya = b$ in $G$, then multiplying the first equation by $\bar{a}^1$ on the left and the second equation by $\bar{a}^1$ on the right, we get $\bar{a}^1 b = \bar{a}^1(ax) = (\bar{a}^1 \cdot a)x = e \cdot x = x$ and $b\bar{a}^1 = (ya)\bar{a}^1 = y(a\bar{a}^1) = y \cdot e = y$. ∎

In an additively written abelian group $G$ the solution $x = b + (-a)$ of the equation $a + x = b$ is the difference of $b$ and $a$ and is denoted by $b - a$. Then $-(a+b) = (-a) + (-b) = -a - b$.

From 1.A.7 the cancellation laws follow.

1.A.8 Definition Let $M$ be a monoid (not necessary commutative) We say that left-cancellation law holds in $M$ if for all $x, y, z \in M$, from $xy = xz$, it follows that $y = z$.

Similarly, the right-cancellation law holds in $M$ if for all $x, y, z \in M$, from $yx = zx$, it follow that $y = z$.

For example, if $M = G$ is a group, then both cancellation-laws hold in $G$ by 1.A.7.

Let $M$ be a monoid and let $x \in M$. Let $\lambda_x : M \longrightarrow M$ be the left-translation by $x$ : $y \longmapsto xy$ and let $\rho_x : M \longrightarrow M$ be the right-translation by $x$ : $y \longmapsto yx$.

An element $x \in M$ in a monoid $M$

is called left-regular in $M$ (resp. right regular) if $\lambda_x$ is injective (resp. $\rho_x$ is injective). Then:

The left (resp. right) cancellation law holds in $M$ if and only if every element $x \in M$ is left (resp. right) regular in $M$.

We say that $x$ is regular in $M$ if it is both left and right regular in $M$

# Rings and Fields

Familiar examples of sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ of numbers with usual binary operations + (addition) and · (multiplication) show that a study of sets on which there are two binary operations are of great importance. The most general system of this kind that is important to study is a ring. We begin with the definition of a ring.

1.A.9 Definition Let $R$ be a set with two binary operations, usually denoted by + (addition) and · (multiplication) with neutral elements $0_R = 0$ and $1_R = 1$, respectively. Then $(R, +, \cdot)$ is called a ring if the following (ring)-axioms[1] are satisfied:

---

1 The ring-axioms have been formulated for the first time by A. FRÄNKEL in the article in: Journal für die reine und angewandte Mathematik, vol 145, (1914).

$R_1$: $(R, +)$ is an abelian group (this abelian group is called the <u>additive group</u> of the ring $(R, +, \cdot)$.)

$R_2$: $(R, \cdot)$ is a monoid (this monoid is called the <u>multiplicative monoid</u> of the ring $(R, +, \cdot)$.)

$R_3$: (<u>Distributive Laws</u>) For all $a, b, c \in R$

$a(b+c) = (ab) + (ac)$

$(b+c)a = (ba) + (ca)$ hold.

We shall observe the standard-convention that the multiplication is performed before addition, so that $a(b+c) = ab + ac$ without the parentheses on the right side of the above equation. Usually we make strong use of the distributive laws; these distributive laws are the only means to relate additive concepts to multiplicative concepts in a ring.

The neutral element $0_R = 0$ of the additive group $(R,+)$ of a ring $R$ is called the zero-element of the ring $R$ and the additive inverse of an element $a \in R$ is denoted by $-a$ and is called the negative of $a$ in $R$. The neutral element $1_R = 1$ of the multiplicative monoid $(R,\cdot)$ of $R$ is called the unity or identity of $R$.

We say that a ring $(R,+,\cdot)$ is commutative if the multiplicative monoid $(R,\cdot)$ of $R$ is commutative, i.e. if the multiplication in $R$ is commutative: $ab = ba$ for all $a, b \in R$.

We shall Mostly consider only commutative rings.

From the ring-axioms we have the following rules which are useful for computations in a ring:

**1.A.10** Let $R = (R, +, \cdot)$ be a ring. Then for all $a, b, c \in R$, we have:

(1) $0 + a = a = a + 0$

$a + (b + c) = (a + b) + c$

$a + b = b + c$

$a + (-a) = 0 = (-a) + a$

$-(-a) = a.$

(2) The distributive laws also hold for substraction:

$a(b - c) = ab - ac, \quad (b - c)a = ba - ca.$

(3) $1 \cdot a = a \cdot 1 = a$

$a(bc) = (ab) \cdot c$

$0 \cdot a = a \cdot 0 = 0$

$a \cdot (-b) = (-a) \cdot b = -ab$

$(-a)(-b) = ab.$

**1.A.11** The unit group of a ring

Let $R = (R, +, \cdot)$ be a ring. Multiplicative inverses are simply referred as inverses. Therefore an inverse of $a \in R$ in $(R, \cdot)$ is an element $a' \in R$

such that $aa' = 1 = a'a$, this element $a'$ is uniquely determined by $a$ and hence denoted by $\bar{a}^1$. The unit element 1 has inverse 1. Similarly the negative $-1$ of 1 is its own inverse, i.e. $(-1)^{-1} = -1$.

If $R$ is not a zero-ring ($= \{0\}$), then the elements 0 and 1 are distinct elements of $R$. For, if $a \neq 0$, then $a \cdot 0 = 0$ and $a \cdot 1 = a \neq 0$ and hence $0 \neq 1$.

In a non-zero ring $R$, the element 0 has no inverse (since $0 \cdot \bar{a} = 0 \neq 1$) and hence the multiplicative monoid $(R, \cdot)$ of $R$ is not a group (under multiplication)

An element $a \in R$ is called a unit or invertible in $R$ if $a$ has an inverse in $R$. The elements 1 and $-1$ are units in $R$. Moreover, if $a$ and $b$ are units in $R$, then $\bar{a}^1$ and $a \cdot b$ are also units in $R$. Therefore in any ring $R$ (with identity)

the set of all units form a group (with respect to multiplication). This group is called the unit group of $R$, (it's precisely the unit group of the multiplicative monoid $(R,\cdot)$ of $R$) and is denoted by $R^\times$. Therefore

$$R^\times = \{a \in R \mid a \text{ is a unit in } R\}.$$

1.A.20 Examples (1) With the usual addition $+$ and usual multiplication $\cdot$, $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ and $(\mathbb{C},+,\cdot)$ are all commutative rings with the usual 0 as the zero-element and the usual 1 as the identity element. Further, the unit groups are $\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{Q}^\times = \mathbb{Q}\setminus\{0\}$, $\mathbb{R}^\times = \mathbb{R}\setminus\{0\}$ and $\mathbb{C}^\times = \mathbb{C}\setminus\{0\}$, respectively.

(2) A ring $R$ which contains only the zero-element is called the zero-ring. A ring $R$ is a zero-ring if and only if $1_R = 0_R$ (Proof!).

(3) Power-set ring Let $X$ be a non-empty set and let $\mathfrak{P}(X)$ be the power set of $X$. Then $(\mathfrak{P}(X), \Delta, \cap)$ is a commutative ring, where $\Delta$ is the symmetric difference of sets:

$A \Delta B := (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$

$\Delta$ is the addition with the zero element $0 = \emptyset$ (empty set) and the identity element $1 = X$. This ring is called the power-set ring of $X$.

1.A.21 General distributive law: Let $a_i$, $i \in I$, and $b_j$, $j \in J$, be finite families of elements in a ring $R$. Then

$$\left(\sum_{i \in I} a_i\right)\left(\sum_{j \in J} b_j\right) = \sum_{(i,j) \in I \times J} a_i b_j$$

(Proof similar to that of on page 1.A.10)

1.A.22 Multiples and Powers in a ring Let $R$ be a ring and let $a \in R$. For any $n \in \mathbb{Z}$, the multiple $na$ of $a$ is

defined as (in the additive group $(R,+)$)

$$na := a+\cdots+a \quad (n\text{-times}, \text{ if } n>0)$$
$$= (-a)+\cdots+(-a) \quad (|n|\text{-times}, \text{ if } n<0)$$
$$= 0 \quad \text{if } n=0.$$

Similarly, the power $a^n$ of $a$ is defined by any $n \geq 0$ : $a^n = a\cdots a$ ($n$-times); $a^0 := 1$. If in addition $a$ is a unit in $R$, i.e. if $\bar{a}^1$ exists, then $a^n$ is defined for all integers $n \in \mathbb{Z}$ ($a^n := (\bar{a}^1)^{|n|}$ if $n<0$).

The following rules for multiples and powers are easy to verify: Let $a, b$ be elements in a ring $R$ and $m, n \in \mathbb{Z}$. Then

(1) $(m+n)a = ma+na$, $m(a+b) = ma+mb$,
$(mn)a = m(na)$, $(ma)(nb) = (mn)(ab)$

(2) $a^m \cdot a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$ if $m, n \in \mathbb{N}$. Moreover, if $\bar{a}^1$ exists, then $a^m \cdot a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$ for all $m, n \in \mathbb{Z}$. Further, if $a$ and $b$ commute, i.e. $ab = ba$, then $(ab)^n = a^n b^n$ for all $n \in \mathbb{N}$ and $a^m b^n = b^n a^m$ for all $m, n \in \mathbb{N}$. Moreover, if $\bar{a}^1$ and $\bar{b}^1$ exists then

$(ab)^n = a^n b^n$ and
$a^m b^n = b^n a^m$ for all $m, n \in \mathbb{Z}$.

(3) Binomial Theorem If $a$ and $b$ are two elements in $R$ with $ab = ba$, then

$$(a+b)^n = \sum_{m=0}^{n} \binom{n}{m} a^m b^{n-m}.$$

More generally, for commuting elements $a_1, \dots, a_r$ in a ring $R$, we have:

Polynomial Theorem

$$(a_1 + \cdots + a_r)^n = \sum_{m \in \mathbb{N}^r, |m| = n} \binom{n}{m} a^m,$$

where $|m| = m_1 + \cdots + m_r$ and $a^m = a_1^{m_1} \cdots a_r^{m_r}$ for $m = (m_1, \dots, m_r) \in \mathbb{N}^r$ and

$$\binom{n}{m} = \frac{n!}{m!} = \frac{n!}{m_1! \cdots m_r!}.$$

1.A.23 Definition A ring $(R, +, \cdot)$ is called a skew-field or division ring if $(R \setminus \{0\}, \cdot)$ is a group, i.e. if $0 \neq 1$ and

every element $a \in R$, $a \neq 0$, is invertible (with resp. to multiplication).
A field is a commutative division ring.

Usually one use the letter $K = (K, +, \cdot)$ to denote a field (= Körper). In the field the following very important rule hold:

(1) Let $a$ and $b$ be two elements in a field $K$. If $ab = 0$, then either $a = 0$ or $b = 0$. (or even a division ring)

Proof From $ab = 0$ and $a \neq 0$, it follows that $b = 1 \cdot b = (a^{-1}a) \cdot b = a^{-1}(ab) = a^{-1} \cdot 0 = 0$.

More generally, the cancellation-law (hold in a field (or division ring)):
If $ab = ac$ (or $ba = ca$) and $a \neq 0$, then $b = c$.

The most important examples of fields are:

1.A.24 Examples (1) With the usual addition $+$ and usual multiplication $\cdot$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$ are

fields, called the field of rational, real and complex numbers, respectively.

(2) The ring of integers $(\mathbb{Z}, +, \cdot)$ is a commutative ring which is not a field.

From the ring $\mathbb{Z}$, for $n \in \mathbb{N} \setminus \{0\}$, we construct the residue-class ring $\mathbb{Z}/\mathbb{Z}n$ which is commutative and has exactly $n$ elements as follows:

(3) (Residue class rings of $\mathbb{Z}$) Let $n \in \mathbb{N}^*$. Let $\equiv_n$ denote the relation congruent modulo $n$ on the set of integers $\mathbb{Z}$, i.e. For $a, b \in \mathbb{Z}$, $a \equiv_n b$ or $a \equiv b \pmod n$ or simply $a \equiv b(n)$ if $a - b$ is a multiple of $n$, i.e. $a - b = kn$ for some $k \in \mathbb{Z}$. Then $\equiv_n$ is an equivalence relation on $\mathbb{Z}$. The equivalence class of $a \in \mathbb{Z}$ under $\equiv_n$ is the subset $[a]_n := \{b \in \mathbb{Z} \mid a \equiv_n b\}$, is also called the residue class of $a$ modulo $n$; $[a_n] = \{a + kn \mid k \in \mathbb{Z}\}$. Let $\mathbb{Z}/\mathbb{Z}n$ denote the quotient set $\mathbb{Z}/\equiv_n$,

This set is also called the set of all residue classes modulo n and has exactly n elements, namely

$$\mathbb{Z}/\mathbb{Z}n = \mathbb{Z}/\equiv_n = \{[0]_n, [1]_n, \cdots, [n-1]_n\}.$$

For example, for $n=1$, $\mathbb{Z}/\mathbb{Z}\cdot 1 = \{[0]_1\}$

for $n=2$, $\mathbb{Z}/\mathbb{Z}\cdot 2 = \{[0]_2, [1]_2\}$, $[0]_2 =$ $\mathbb{Z}\cdot 2$ = the set of even integers and $[1]_2$ = the set of odd integers $= 1 + \mathbb{Z}\cdot 2$.

For integers $a, b$ with $a \neq b$ and $0 \leq a, b < n$, $[a]_n \neq [b]_n$, since $0 < |a-b| < n$.

The binary operations $+_n$ and $\cdot_n$ on $\mathbb{Z}/\mathbb{Z}n$ are defined as:

$$[a]_n +_n [b]_n := [a+b]_n$$

$$[a]_n \cdot_n [b]_n := [a-b]_n$$

Check that these binary operations are well-defined and that $(\mathbb{Z}/\mathbb{Z}n, +_n, \cdot_n)$ is a commutative ring; $0 = [0]_n$, $1 = [1]_n$

and $-[a]_n = [-a]_n$ for all $a \in \mathbb{Z}$.
This ring $(\mathbb{Z}/\mathbb{Z}n, +_n, \cdot_n)$ is called the residue-class ring of $\mathbb{Z}$ modulo $n$

It is easy to characterise $n \in \mathbb{N}^*$ for which the ring $\mathbb{Z}/\mathbb{Z}n$ is a field:

1.A.25 Theorem Let $n \in \mathbb{N}^*$. Then the residue-class ring $\mathbb{Z}/\mathbb{Z}n$ is a field if and only if $n$ is a prime number.

Proof ($\Leftarrow$) Suppose that $n$ is a prime number. We have to show that: for every residue class $[a] \neq [0]$, there is an inverse $[b]$, i.e. $[ab] = [1]$. Since we can choose an arbitrary representative $a$ in $[a]$, we may assume that $0 < a < n$. Since $n$ is prime, $\gcd(a, n) = 1$ and hence by Bezout's lemma there exist integers $s, t \in \mathbb{Z}$ such that $1 = sa + tn$. Then

If follows that $[1] = [sa + tn] = [sa][t] = [s][a]$ and the residue class $[s]$ of $s$ is the required inverse of $[a]$ in $\mathbb{Z}/\mathbb{Z}n$.

($\Rightarrow$) Suppose that $n$ is not a prime number and $n > 1$. Then there exist integers $a, b \in \mathbb{N}^*$ with $0 < a < n$, $0 < b < n$ and $ab = n$. It follows that $[a] \cdot [b] = [ab] = [n] = [0]$ but $[a] \neq 0$ and $[b] \neq 0$.

Suppose that $[a]$ has inverse in $\mathbb{Z}/\mathbb{Z}n$, i.e. there is $[c] \in \mathbb{Z}/\mathbb{Z}n$ with $[c] \cdot [a] = [1]$. Then it follows that

$[b] = [1][b] = [c][a][b] = [c][ab]$
$= [c] \cdot [0] = [c \cdot 0] = [0]$ a contradiction to $[b] \neq [0]$. Therefore $[a]$ and analogously $[b]$) has no inverse in $\mathbb{Z}/\mathbb{Z}n$. This proves that $\mathbb{Z}/\mathbb{Z}n$ is not a field

$\mathbb{Z}/\mathbb{Z}\cdot 1$ is the zero-ring; $\mathbb{Z}/\mathbb{Z}\cdot 2$ is a field with 2 elements; $\mathbb{Z}/\mathbb{Z}\cdot 3$ is a field with 3 elements.

**1.A.26** (Rules for fractions in a field)

Let $K$ be a field and let $a, b \in K$, $b \neq 0$. Then $ab^{-1} \in K$, we often use fraction to write this element:

$$\frac{a}{b} := a/b := ab^{-1} = b^{-1}a.$$

We then have the following rules for fractions:

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'},$$

$$\frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}, \quad 1/(b/b') = (b/b')^{-1} = b'/b$$

for all $a, b, a', b' \in K$ with $b \neq 0, b' \neq 0$.

More generally, we use these fractions $a/b = ab^{-1}$ in an arbitrary commutative ring $R$ for the element $ab^{-1} = b^{-1}a$ for all $a, b \in R$ with $b \in R^*$ a unit in $R$.

**1.A.27** (Units in the residue-class ring $\mathbb{Z}/\mathbb{Z}\cdot n$) Let $n \in \mathbb{N}^*$. The

residue class $[a] \in \mathbb{Z}/\mathbb{Z}n$, $a \in \mathbb{Z}$ is a unit in the residue class ring $\mathbb{Z}/\mathbb{Z}n$ if and only if $a$ and $n$ are relatively prime, i.e. $\gcd(a,n) = 1$.

This is immediate from the following:

**Bezout's lemma** Let $a$ and $b$ be positive integers. Then there exist integers $s$ and $t$ such that

$$\gcd(a,b) = sa + tb$$

In particular, $a$ and $b$ are relatively prime natural numbers if and only if there exists integers $s, t \in \mathbb{Z}$ with $1 = sa + tb$.

**Proof** Repeated application of division with remainder (Euclidean algorithm)

In particular, the number of units in $\mathbb{Z}/\mathbb{Z}n$ is $\varphi(n)$, where $\varphi$ is the Euler's totient function. This can also be taken as the definition of $\varphi$.