0.A Rings and Fields

A fundamental algebraic concept is that of a binary operation on a set.

A <u>binary operation</u> on a set G is a map

$$G \times G \longrightarrow G,$$

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

For example, on the sets $\mathbb{N} = \{0,1,2,\cdots\}$, $\mathbb{Z} = \{0, \pm 1, \pm 2, \cdots\}$, $\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z},\ b \neq 0\}$, $\mathbb{R}$ and $\mathbb{C}$, of natural numbers, integers, rational numbers, real numbers, complex numbers, respectively, the usual addition $+$ and the usual multiplication $\cdot$ are binary operation On the power set $\mathcal{P}(X)$ of a set X, union $\cup$, intersection $\cap$ and symmetric difference Δ are binary operations. On the sets $X^X = \mathrm{Maps}(X,X)$ of maps from a set X into itself or $\mathfrak{S}(X) = \{f \in X^X \mid f \text{ is bijective}\}$ of permutations of a set X, the composition $\circ$ of maps is a binary operation.

0.A.1 Definition A binary operation on a set G $G \times G \longrightarrow G$, $(x,y) \longmapsto xy$, is <u>commutative if</u>[1] (and <u>or abelian</u>)

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

only if) $xy = yx$ for all $x, y \in G$. The operation is <u>associative</u> if $(xy)z = x(yz)$ for all $x, y, z \in G$. It is not difficult to show that if the binary operation is associative, then longer expressions such as $(\cdots((x_1 x_2)x_3)x_4\cdots)x_n$ (standard-parentheses) are not ambiguous. Parentheses may be inserted in any fashion for purposes of computation, the final result of two such computations will be the same.

<u>O.A.2 Definitions</u> Let G be a set with a binary operation $G \times G \longrightarrow G$, $(x, y) \longmapsto xy$.

(1) An element $e \in G$ is called a <u>neutral element</u> if $ex = xe = x$ for all $x \in G$. (if neutral element exists, then it is unique: $e = e \cdot e' = e'$)

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

(3) Suppose that G is a monoid with neutral element $e_G = e$. An element $x' \in G$ is called an <u>inverse</u> of the element $x \in G$ if $xx' = x'x = e$. For example e is an inverse of e; $ee = ee = e$. If the element $x \in G$ has an inverse in G, then it is unique and hence denoted by x^{-1} (if x' and x'' are inverses of x, then $x' = x'e = x'(xx'') = (x'x)x'' = ex'' = x''$). Therefore $xx^{-1} = x^{-1}x = e$

(The inverse of an element x (if it exists), in the

multiplicative notation is denoted by x^{-1}, in the additive notation is denoted by $-x$. The neutral element e, in the multiplicative notation is denoted by 1_G or 1 (usually called the negative of x); in the additive notation is denoted by 0_G or 0 (usually called the one or unity in G) (usually called the zero in G).

(4) An element x in a monoid G is called invertible or an unit if x has an inverse in G.
Let $x, y \in G$ be invertible elements in G. Then x^{-1} and xy are also invertible in G. Moreover, $(x^{-1})^{-1} = x$ and $(xy)^{-1} = y^{-1}x^{-1}$. Therefore the binary operation of a monoid G induces a binary operation on the subset $G^\times = \{x \in G \mid x \text{ has an inverse}\} \subseteq G$ of all invertible elements in G, i.e. $G^\times \times G^\times \longrightarrow G^\times$, $(x, y) \longmapsto xy$

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

For example, the monoids $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are groups, but the monoids $(\mathbb{N}, +)$, $(\mathbb{N}^* = \mathbb{N}\setminus\{0\}, \cdot)$, $(\mathbb{Z}, \cdot)$ are not groups, in fact, $(\mathbb{N}, +)^\times = \{0\}$, $(\mathbb{N}^*, \cdot)^\times = \{1\}$ and $(\mathbb{Z}, \cdot)^\times = \{\pm 1\}$. However, the monoids $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ and $(\mathbb{C}^*, \cdot)$ are groups.

The monoids $(X^X, \circ)$ and $(G(X), \circ)$ are not commutative if X has more than 2 elements. Moreover $(X^X, \circ)$ is not a group and $(G(X), \circ) = (X^X, \circ)^\times$ is a group (called the permutation group on X). More generally, if G is a monoid, then the monoid $G^\times$ of invertible elements is a group, the group is called the unit group of the monoid G.

Familiar examples of sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ of numbers 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 we shall study is a ring.

0.A.3 Definition A set R with two binary operations $+$ (addition) and $\cdot$ (multiplication) with neutral elements 0 and 1, respectively, is called a ring if the following axioms are satisfied:

(1) $(R, +)$ is an abelian group.

(2) $(R, \cdot)$ is a monoid.

(3) (Distributive laws) For all $a, b, c \in R$,

$$(a+b)c = (ac) + (bc) \text{ and } a(b+c) = (ab) + (ac)$$

hold.

For example, $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$ are rings, where $+$ and $\cdot$ denote the usual addition and multiplication.

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

For $a, b \in R$ and $m, n \in \mathbb{Z}$, we have:

(i) $0a = a0 = 0$.

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

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

(iv) $(m+n)a = ma + na$

(v) $m(a+b) = ma + mb$

(vi) $(mn)a = m(na)$

(vii) $(ma)(nb) = (mn)(ab)$

O.A.4 Examples (1) Let $n \in \mathbb{N}$ and let $\equiv_n$ denote the relation of multiplication modulo on $\mathbb{Z}$, i.e.

$k, l \in \mathbb{Z}$, $k \equiv_n l$ or $k \equiv l \bmod n$ if $l - k = an$ with $a \in \mathbb{Z}$. Then $\equiv_n$ is an equivalence relation on $\mathbb{Z}$ i.e.

$k \equiv_n k$ for all $k \in \mathbb{Z}$ (reflexive)

$k \equiv_n l \Rightarrow l \equiv_n k$ (Symmetric)

$k \equiv_n l$ and $l \equiv_n m \Rightarrow k \equiv_n m$ (transitive).

Let $[k]_n := \{ l \in \mathbb{Z} \mid k \equiv_n l \}$ be the equivalence class of k under $\equiv_n$ (also called the residue class of k modulo n).

$[k]_n = \{ k + an \mid a \in \mathbb{Z} \} = k + \mathbb{Z} \cdot n$. Let $\mathbb{Z}/\mathbb{Z}n$ denote the set of all residue classes modulo n.

$$\mathbb{Z}/\mathbb{Z}n = \{ [k]_n \mid k \in \mathbb{Z} \}$$

$n = 1$, $\mathbb{Z}/\mathbb{Z}n = \{ [0]_n \}$

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

$[1]_2 = 1 + \mathbb{Z}\cdot 2$ = the set of all odd integers.

For arbitrary $n \in \mathbb{N}$, $|\mathbb{Z}/\mathbb{Z}\cdot n| = n$,

$\mathbb{Z}/\mathbb{Z}n = \{ [0]_n, [1]_n, \cdots, [n-1]_n \} = \{ [k]_n \mid 0 \le k < n \}$.

For $k \neq l$, $0 \le k < n$, $0 \le l < n \Rightarrow k \not\equiv_n l$, since $0 < |k-l| < n$

The binary operations

$$[k]_n + [l]_n := [k+l]_n$$

$$[k]_n \cdot [l]_n := [kl]_n$$

$-[k]_n = [-k]$

$0_{\mathbb{Z}/\mathbb{Z}n} = [0]_n$, $1_{\mathbb{Z}/\mathbb{Z}n} = [1$

on $\mathbb{Z}/\mathbb{Z}n$ are well-defined and with this $(\mathbb{Z}/\mathbb{Z}n, +, \cdot)$ is a commutative ring.

(2) Let X be a non-empty set and let $\mathcal{P}(X)$ be the power set of X. Then $(\mathcal{P}(X), \Delta, \cap)$ is a commutative ring with $0 = \phi$ and $1 = X$. This ring is called the <u>power set ring</u> of X.

(3) Let I be any set and let R be any ring. The set R^I of R-valued functions on I with the binary operations: for $f, g \in R^I$,

$$(f+g)(i) = f(i) + g(i), \quad i \in I$$

$$(f \cdot g)(i) = f(i)g(i), \quad i \in I$$

form a ring. This ring is called the ring of R-valued functions on I, the addition is this ring is the componentwise addition (using the addition in R, and the componentwise multiplication (using the multiplication in R). The constant function 0_R and the constant function 1_R are the zero element 0_{R^I} and the unity 1_{R^I} in the ring R^I.

In particular, if $I = \{1, \cdots, n\}$ and if R is a ring, then $R^I = R^{\{1,\cdots,n\}} = R^n = R \times R \times \cdots \times R$ (n-times) is a

ring with componentwise addition and componentwise multiplication. In particular,

$\mathbb{Z}^n = \mathbb{Z} \times \cdots \times \mathbb{Z}$, $\mathbb{Q}^n$, $\mathbb{R}^n$, $\mathbb{C}^n$ are rings.

(4) (Polynomial rings) Let R be a ring. We think of a polynomial in indeterminate (or variable) X with coefficients in R is an expression (or symbol)

$$a_0 + a_1 X + \cdots + a_n X^n, \quad a_0, \cdots, a_n \in R, \quad n \in \mathbb{N}.$$

We can add and multiply such expressions by using the addition and multiplication in R. We denote $R[X] := \{ a_0 + a_1 X + \cdots + a_n X^n \mid a_0, \cdots, a_n \in R, n \in \mathbb{N} \}$. Then for $f = f(X) := a_0 + a_1 X + \cdots + a_n X^n \in R[X]$ and

$g = g(X) := b_0 + b_1 X + \cdots + b_m X^m \in R[X]$, define

$$f + g = \sum_{j \in \mathbb{N}} c_j X^j, \text{ where } c_j = a_j + b_j \text{ for } j \in \mathbb{N} \text{ and}$$

$$fg = \sum_{j \in \mathbb{N}} d_j X^j, \text{ where } d_j := \sum_{i=0}^{j} a_i b_{j-i} \text{ for } j \in \mathbb{N}.$$

Then $f+g$ and $fg \in R[X]$. Moreover, $(R[X], +, \cdot)$ is a ring with $0_{R[X]} = 0_R$ and $1_{R[X]} = 1_R$. Further, if R is commutative, then $R[X]$ is also commutative. This ring $(R[X], +, \cdot)$ is called the polynomial ring in X over R.

For a (non-zero) polynomial $f = a_0 + a_1 X + \cdots + a_n X^n \in R[X]$ with $a_n \neq 0$, the natural number n is called the degree of f and is denoted by $\deg f$. The degree of the zero

polynomial $0 = 0_{R[X]} = 0_R$ is defined to be $-\infty$. Polynomials of degree ≤ 0 are called the constant polynomials, of degree 1 are called linear, of degree 2 are called quadratic, of degree 3 are called cubic, of degree 4 are called biquadratic etc.

(5) (Ring of numerical functions) Let R be a commutative ring. On the set of sequences $R^{\mathbb{N}^*}$ with values in the ring R, define the addition componentwise, i.e. $(f+g)(n) := f(n) + g(n)$ for $f, g \in R^{\mathbb{N}^*}$, $n \in \mathbb{N}$. Further, define the multiplication by the formula

$$(f*g)(n) := \sum_{d|n} f(d) \cdot g(n/d)$$ (Dirichlet's convolution formula)

With these operations $(R^{\mathbb{N}^*}, +, *)$ is a commutative ring. This ring is called the ring of numerical functions with values in R; its elements are called numerical functions with values in R. The zero element $0_{R^{\mathbb{N}^*}}$ is the constant function 0_R on $\mathbb{N}^*$ and the unity $1_{R^{\mathbb{N}^*}}$ is the function $\varepsilon : \mathbb{N}^* \longrightarrow R$, $\varepsilon(1) = 1$ and $\varepsilon(n) = 0$ for all $n \geq 2$.