1. Binary operations.

Suppose X is a set

Definition 1.1. We say β is a **binary operation on** X if

$$\beta : X \times X \to X.$$

We say such a binary operation β is **commutative** or **Abelian** if

$$\beta(x, y) = \beta(y, x) \quad \text{whenever } x, y \in X.$$

Definition 1.2. We say $e \in X$ is an **identity element (for the binary operation** β on X) if

$$\beta(x, e) = x \quad \text{and} \quad \beta(e, x) = x \quad \text{whenever } x \in X.$$

If e_1 and e_2 are identity elements for β we have

$$e_1 = \beta(e_1, e_2) = e_2.$$

Thus an identity element for a binary operation, if it exists, is unique and we may speak of *the* identity element for the binary operation.

Definition 1.3. We say the binary operation β on X is **associative** if

$$\beta(\beta(x_1, x_2), x_3) = \beta(x_1, \beta(x_2, x_3)) \quad \text{whenever } x_1, x_2, x_3 \in X.$$

Suppose β is associative. For each positive integer $n \geq 2$ and each $j \in \{1, \ldots, n-1\}$ we define the map

$$\beta_{j,n} : X^n \to X^{n-1}$$

on $(x_1, \ldots, x_n) \in X^n$ by requiring the i-th coordinate of its image under $\beta_{j,n}$ to be x_i if $i < j$; to be $\beta(x_j, x_{j+1})$ if $i = j$; and to be x_{i+1} if $j < i \leq n-1$. We set

$$\beta_n = \beta_{1,2} \circ \ldots \beta_{1,n-1} \circ \beta_{1,n}.$$

Note that

$$\beta_n : X^n \to X.$$

We leave it to the reader to prove that

$$\beta_{\mu(1),2} \circ \ldots \beta_{\mu(n-2),n-1} \circ \beta_{\mu(n-1),n} = \beta_n$$

whenever $\mu : \{1, \ldots, n-1\} \to \{1, \ldots, n\}$ is such that $\mu(i) < i + 1$ for each $i \in \{1, \ldots, n-1\}$, thus verifying the **general associative law**. One frequently writes

$$x_1 \cdots x_n$$

instead of $\beta_n(x_1 \ \ldots, x_n)$.

Definition 1.4. Suppose β is a binary operation on X with identity e. Suppose $x \in X$. We say w is a **left inverse to** X if $w \in X$ and $\beta(w, x) = e$. We say y is a **right inverse to** x if $y \in X$ and $\beta(x, y) = e$. We say z is an inverse to x if z is a left inverse to x and z is a right inverse to x; if z is the unique element with this property, we say z is *the* **inverse to** x. We say x is **invertible** if there is an inverse to x.

Suppose β is associative. Suppose $x \in X$, w is a left inverse to x and y is a right inverse to x then

$$w = we = w(xy) = (wx)y = ey = y.$$

Thus there is a unique left inverse to x, there is a unique right inverse to x, the unique left inverse to x equals the unique right inverse to x and this element is the unique inverse to x.

1.1. **Groups.**

Definition 1.5. A **group** is an ordered triple

$$(G, \mu, e)$$

such that G is a set, μ is an associative binary operation on G with identity e, and every element of G is invertible. It is customary to say

"G is a group"

instead of "(G, μ, e) is a group". Very often one writes

$$gh$$

for $\mu(g, h)$ and one writes

$$g^{-1}$$

for the inverse to the element g of G. When G is Abelian, very often one writes

$$0$$

for the identity element,

$$g + h$$

for gh whenever $g, h \in G$ and one writes

$$-g$$

for g^{-1} whenever $g \in G$.

1.2. **Finite summation.** Let X be a set.

1.3. **Finite summation.** Suppose Y is a set and

$$\cdot + \cdot : Y \times Y \to Y$$

is such that

(i) $x + (y + z) = (x + y) + z$ whenever $x, y, z \in Y$;
(ii) $x + y = y + x$ whenever $x, y \in Y$;
(iii) there is $0 \in Y$ such that $y + 0 = y = 0 + y$ whenever $y \in Y$.

For example, Y could be an Abelian group or Y could be $[0, \infty]$ where $+$ on $[0, \infty) \times [0, \infty)$ is addition in the Abelian group of $\overline{\mathbb{R}}$ and where

$$y + \infty = \infty = \infty + y \quad \text{whenever } y \in [0, \infty].$$

Definition 1.6. For $f, g \in Y^X$ we define $f + g \in Y^X$ by letting

$$(f + g)(x) = f(x) + g(x) \quad \text{for } x \in X$$

and we note that appropriately reformulated versions of (i),(ii) and (iii) hold. We let

$$0 : X \to Y$$

be such that $0(x) = 0$ for $x \in X$.

Definition 1.7. For $f \in Y^X$ we let

$$\mathbf{spt}\, f = \{x \in X : f(x) \neq 0\}$$

and call this subset of X the **support of f.** We let

$$\left(Y^X\right)_0 = \{f \in Y^X : \mathbf{spt}\, f \text{ is finite}\}$$

and note that $\left(Y^X\right)_0$ is closed under addition.

Definition 1.8. Whenever $A \subset X$ and $f \in Y^X$ we let

$$f_A \in Y^X$$

be such that

$$f_A(x) = \begin{cases} f(x) & \text{if } x \in A, \\ 0 & \text{if } x \in X \sim A. \end{cases}$$

Proposition 1.1. Suppose F is a finite subset of X. There is one and only one function

$$S_F : Y^X \to Y$$

such that

(i) $S_F(0) = 0$;
(ii) $S_F(f) = S(f_{X\sim\{a\}}) + f(a)$ whenever $f \in Y^X$ and $a \in A$;
(iii) $S_F(f + g) = S_F(f) + S_F(g)$ whenever $f, g \in Y^X$.

Proof. We define S_F by induction on $|F|$ as follows. We let $S_\emptyset(0) = 0$. If $|F| > 0$ we let

$$S_F = \{(f, S_{F\sim\{a\}}(f_{X\sim\{a\}}) + f(a)) : f \in \mathcal{F}_F \text{ and } a \in F\}.$$

It is obvious that S_F is a function if $|F| = 1$. To verify that S_F is a function in case $|F| > 1$ we suppose $f \in \mathcal{F}_F$, $a, b \in F$ and $a \neq b$ and we calculate

$$\begin{aligned} S_{F\sim\{a\}}(f_{X\sim\{a\}}) + f(a) &= (S_{F\sim\{a,b\}}(f_{X\sim\{a,b\}}) + f(b)) + f(a) \\ &= S_{F\sim\{a,b\}}(f_{X\sim\{a,b\}}) + (f(b) + f(a)) \\ &= S_{F\sim\{a,b\}}(f_{X\sim\{a,b\}}) + (f(a) + f(b)) \\ &= (S_{F\sim\{a,b\}}(f_{X\sim\{a,b\}} + f(a)) + f(b) \\ &= S_{F\sim\{b\}}(f_{X\sim\{b\}}) + f(b). \end{aligned}$$

We leave to the reader the straightforward verification using induction on $|F|$ that S_F satisfies (i)-(iii). □

1.4. **Summation.** Let A be an Abelian group and let X be a set. Then A^X is an Abelian group with respect to pointwise addition: Given $f, g \in A^X$ we set

$$(f + g)(x) = f(x) + g(x) \quad \text{for } x \in X.$$

We let

$$(A^X)_0 = \{f \in A^X : \{x \in X : f(x) \neq 0\} \text{ is finite}\}$$

and note that $(A^X)_0$ is a subgroup of A^X.

Theorem 1.1. There is one and only one homomorphism

$$\Sigma : (A^X)_0 \to A$$

such that

$$\Sigma(f) = f(w)$$

if $x \in X$ and $f : X \to A$ is such that

$$f(x) = 0 \quad \text{if } x \in X \sim \{w\}.$$

Proof. For each $n \in \mathbb{N}$ let

$$\mathcal{F}_n = \{f \in A^X : \mathbf{card}\,\{x \in X : f(x) \neq 0\} = n\}.$$

Show by induction on n that there is one and only one function

$$S_n : \mathcal{F}_n \to A$$

such that $S_0(f) = 0$ if $f \in \mathcal{F}_0$ and

$$S_n(f) = S_{n-1}(g) + f(w)$$

whenever $n > 0$, $g \in \mathcal{F}_{n-1}$, $w \in X$, $g(w) = 0$, and

$$f(x) = \begin{cases} g(x) & \text{if } g(x) \neq 0, \\ 0 & \text{if } g(x) = 0 \text{ and } x \neq w. \end{cases}$$

It will be necessary to use the associativity and commutativity of the group operation in carrying out the inductive step.

Show by induction on m that $S_m | \mathcal{F}_n = S_n$ whenever $m, n \in \mathbb{N}$ and $m > n$. Let $\Sigma = \cup_{n=0}^{\infty} \mathcal{F}_n$. □

1.5. **Rings.**

Definition 1.9. A **ring** is an ordered quadruple

$$(R, \alpha, 0, \mu)$$

such that $(R, \alpha, 0)$ is an Abelian group, μ is a associative binary operation on R which is **distributive over** α, by which we mean that

$$\mu(a, \alpha(b, c)) = \alpha(\mu(a, b), \mu(a, c)) \quad \text{and} \quad \mu(\alpha(a, b), c) = \alpha(\mu(a, c), \mu(b, c))$$

whenever $a, b, c \in R$.

It is customary to say "R is a ring" instead of "$(R, \alpha, \mu, 0)$ is a ring". If $a, b \in R$ we write

$$a + b \text{ for } \alpha(a, b) \text{ and } ab \text{ for } \mu(a, b).$$

Distributivity then amounts to

$$a(b + c) = ab + ac \quad \text{and} \quad (a + b)c = ac + bc \quad \text{whenever } a, b, c \in R.$$

We say the ring R is **commutative** if

$$ab = ba \quad \text{whenever } a, b \in R.$$

We say R is a ring with identity if there is $1 \in R$ such that

$$1a = a = a1 \quad \text{whenever } a \in R.$$

We say the nonzero element a of the commutative ring R is a **divisor** of the element $c \in R$ if there is there is $b \in R$ such that $c = ab$.

We say D is an **integral domain** if R is a commutative ring with identity and 0 has no divisors.

Definition 1.10. An **ordering** for the ring R is a subset P of R such that

(i) for each $a \in R$ exactly one of the following holds:

$$a \in P, \quad a = 0, \quad -a \in P;$$

(ii) $a + b \in P$ and $ab \in P$ whenever $a, b \in P$;

If the R is a commutative ring R with identity which has an ordering then R is an integral domain. We say $a \in R$ is **positive** if $a \in P$ and we say a is **negative** if $-a \in P$.

Suppose P is an ordering for R. One easily verifies that

$$<= \{(a, b) : b - a \in P\}$$

is a linear ordering of R

1.6. **Fields.**

Definition 1.11. A **field** is an ordered quintuple

$$(F, \alpha, 0, \mu, 1)$$

such that $(F, \alpha, 0, \mu)$ is a ring and $(F \sim \{0\}, \mu|(F \sim \{0\} \times F \sim \{0\}), 1)$ is an Abelian group. This last condition amounts to saying that μ is commutative and that any $x \in F \sim \{0\}$ has an inverse with respect to μ.

1.6.1. *The field of quotients of an integral domain.* Suppose D is an integral domain. One easily verifies that

$$q = \{((a, b), (c, d)) \in (R \times R \sim \{0\})^2 : ad = bc\}$$

is an equivalence relation on $R \times (R \sim \{0\})$. whenever $(a, b) \in R \times (R \sim \{0\})$ we let

$$\frac{a}{b}$$

be the equivalence class of (a, b). It is a simple exercise which we leave to the reader to verify that there are unique binary operations α and μ on $\frac{D}{q}$ such that

$$\alpha(\frac{a}{b}, \frac{c}{d}) = \frac{ad + bc}{bd} \quad \text{and} \quad \mu(\frac{a}{b}, \frac{c}{d}) = \frac{ac}{bd} \quad \text{whenever } (a, b), (c, d)) \in R \times (R \sim \{0\})$$

and that

$$(\frac{D}{q}, \alpha, \frac{0}{1}, \mu, \frac{1}{1})$$

is a field. Moreover, if P is the set of positive elements of an ordering of D then

$$\frac{P}{d} = \{\frac{a}{b} : a, b \in P\}$$

is an ordering of $\frac{D}{q}$.