Chapter 6

Structures with Two Binary Operations

In the last two lectures we investigated groupoids, semigroups, and groups as examples of a set with one binary operation. Now, we will be interested in structures that consist of a nonempty set together with two binary operations, as fields, lattices and Boolean algebras.

6.1 Rings and Fields

Consider the set of all real numbers $\mathbb{R}$. On $\mathbb{R}$, two binary operations are defined: addition $+$ and multiplication $\cdot$. We know that $(\mathbb{R}, +, 0)$ is a commutative group, $(\mathbb{R}, \cdot, 1)$ a commutative monoid. Moreover, for the operations the distributivity laws hold: For all $a, b, c \in \mathbb{R}$ it holds that

$$a\,(b+c) = a\,b + a\,c \quad \text{and} \quad (b+c)\,a = b\,a + c\,a.$$

Another example: Consider the set of all square matrices M_n of order n. We can add two matrices, we can multiply two matrices. In fact, $(M_n, +, O)$ (O is the zero matrix) is a commutative group, $(M_n.\cdot, E)$ (E is the identity matrix) is a monoid. And moreover the operations $+$ and $\cdot$ satisfy the distributivity laws.

Two examples above do not have the same properties; indeed, $(M_n, \cdot, E)$ is not commutative, in $(\mathbb{R}, \cdot, 1)$ every number $x \neq 0$ has its inverse, whereas only regular matrices are invertible in $(M_n, +, \cdot)$. The following notions capture such differences.

6.1.1 A (Commutative) Ring with Identity.

Definition. A nonempty set M together with two binary operations $+$ and $\cdot$ is called a *ring with identity* if $(M, +, 0)$ is a commutative group, $(M, \cdot, 1)$ is a monoid and two distributive laws hold

$$a \cdot (b+c) = a \cdot b + a \cdot c \quad \text{and} \quad (b+c) \cdot a = b \cdot a + c \cdot a$$

for every $a, b, c \in M$.

If moreover the multiplication $\cdot$ is commutative then the ring is called a *commutative ring with identity.* □

Convention. We will denote a ring with identity by $(M, +, \cdot)$, where $M \neq \emptyset$. Further, we denote the neutral element of the commutative group $(M, +)$ as 0, and the neutral element of $(M, \cdot)$ by 1. Moreover, $-a$ is the opposite (inverse) element to a in $(M, +, 0)$, and a^{-1} the inverse of a in $(M, \cdot, 1)$ if it exists.

Remark. Notice, that in any ring with identity we have $0 \cdot a = 0 = a \cdot 0$ and $(-a) \cdot b = a \cdot (-b) = -ab$.

6.1.2 Examples of Rings.

1. $(\mathbb{R}, +, \cdot)$ where $\mathbb{R}$ is the set of all real numbers with addition $+$ and multiplication $\cdot$ forms a commutative ring with identity.
2. $(M_n, +, \cdot)$ where M_n is the set of all real square matrices of order n, $+$ is the matrix addition and $\cdot$ is the matrix multiplication forms a ring with identity which is **not commutative** (note that multiplication of matrices is not commutative).
3. $(\mathbb{Z}, +, \cdot)$ where $\mathbb{Z}$ is the set of all integers together with addition and multiplication forms a commutative ring with identity.
4. $(\mathbb{Z}_n, +, \cdot)$ where $+$ and $\cdot$ are operations in $\mathbb{Z}_n$ forms a commutative ring with identity where the class containing 1 is the identity element. This ring has got n elements.

6.1.3 Zero Divisors. There are rings with identity where we can obtain 0 even if we multiply two nonzero elements. We give two such examples.

1. Consider the product of the two following nonzero matrices:

$$\begin{pmatrix} 2 & 2 \\ 3 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

2. In $(\mathbb{Z}_6, \cdot, 1)$ we have $2 \cdot 3 = 0$ and $2 \neq 0 \neq 3$.

On the other hand, no product of two nonzero real numbers (or integers) equals 0. This motivates the following notion.

Definition. An element of a ring $(M, +, \cdot)$ is called a *zero divisor* if $a \neq 0$ and there exists $b \neq 0$ such that $a \cdot b = 0$. □

If a is a zero divisor in a ring $(M, +, \cdot)$ with identity then a is not invertible in $(M, \cdot, 1)$. Indeed, if a^{-1} exists then from $a \cdot b = 0$ we immediately get

$$b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0.$$

So if a is invertible then from $a \cdot b = 0$ it follows that $b = 0$.

Let us mention that a ring with identity without zero divisors is called an *integral domain.*

6.1.4 A Field. A commutative ring with identity where every nonzero element is invertible (hence, with the similar properties as real numbers) is called a *field.* More precisely:

Definition. A commutative ring with identity is called a *field* if every nonzero element of M is invertible in $(M, \cdot, 1)$, and if $0 \neq 1$. □

Let us note that the condition $0 \neq 1$ only means that every field must have at least two elements, namely 0 and 1. So we exlude the "trivial" commutative ring having just one element 0. (In this ring $(\{0\}, +)$ is the same as $(\{0\}, \cdot)$.)

It is not difficult to see that $(\mathbb{Z}_2, +, \cdot)$ is a field with exactly two elements 0 and 1.

Examples.

a) $(\mathbb{R}, +, \cdot)$ is a field.
b) $(\mathbb{Z}_p, +, \cdot)$ where p is a prime number is a field.
c) $(\mathbb{Q}, +, \cdot)$ where $\mathbb{Q}$ is the set of all rational numbers is a field.
d) $(\mathbb{C}, +, \cdot)$ where $\mathbb{C}$ is the set of all complex numbers is a field.
e) $(M_n, +, \cdot)$, $n > 1$, **is not** a field because only regular matrices are invertible.
f) $(\mathbb{Z}_n, +, \cdot)$ where n is composite number **is not** a field, indeed, every divisor $i \neq 1$ of n is not invertible.

6.1.5 Remark. In the course of linear algebra one works with vector spaces, matrices, etc. Scalars there are taken from the field of real numbers or the field of complex numbers. This is not necessary; linear algebra can be built over *any* field (commutative ring with identity does not suffice). There are only small differences; for example, if we study vector spaces over a finite field with k elements, then any vector space of dimension n has only k^n elements. Similarly, there are only finitely many solutions of a system of linear equtions over a field with k elements.

We know that $(\mathbb{Z}_p, +, \cdot)$, p a prime, is an example of a finite field. These are not the only one examples. It can be shown that for any prime p and integer $k \geq 1$ there is a field with p^k elements (which is in some sense unique). Moreover, there are no finite fields with other number of elements. The construction of fields with p^k elements for $k > 1$ is beyond the scope of this course.

6.1.6 The Group of Invertible Elements of a Finite Field. Let $(F, +, \cdot)$ be a finite field. Then we know that $F \setminus \{0\}$ forms a group, the group of invertible elements of $(F, \cdot, 1)$. It can be proved that the group $(F^\star, \cdot, 1)$ is always cyclic. In other words, it has a generating element a (here called a primitive element) such that every non-zero element of F is a power of a. So once we know the correspondence between non-zero elements and a^i, multiplication and cancellation becomes rather easy. The proof of the following proposition is beyond the scope of the course.

Theorem. Let $(F, +, \cdot)$ be a finite field. Then the group of invertible elements of the monoid $(F, \cdot, 1)$ is a cyclic group. □

6.2 Boolean Algebras

There is an other type of structures with two binary operations than rings and fields — lattices and their special case Boolean algebras. First, let us recall some facts known from the set theory.

Properties of Subsets. Consider a nonempty set U and the set of all its subsets $\mathcal{P}(U)$. Let $\cap$ denote the intersection of sets, and $\cup$ the union of sets. Then for every sets $A, B, C \subseteq U$ we have

1. $A \cap (B \cap C) = (A \cap B) \cap C$, $A \cup (B \cup C) = (A \cup B) \cup C$ (associative law).
2. $A \cap B = B \cap A$, $A \cup B = B \cup A$ (commutative law).
3. $A \cap A = A$, $A \cup A = A$.
4. $A \cap (B \cup A) = A$, $A \cup (B \cap A) = A$.

6.2.1 A Lattice. The example above motivates the notion of a lattice. It will be a nonempty set together with two operations that will satisfy the above four properties. More precisely:

Definition. A *lattice* consists of a nonempty set M together with two binary operations on M; one is *meet* $\wedge$ and the other is *join* $\vee$ which satisfy the following four conditions

1. $A \wedge (B \wedge C) = (A \wedge B) \wedge C$, $A \vee (B \vee C) = (A \vee B) \vee C$ (associative law).
2. $A \wedge B = B \wedge A$, $A \vee B = B \vee A$ (commutative law).
3. $A \wedge A = A$, $A \vee A = A$.
4. $A \wedge (B \vee A) = A$, $A \vee (B \wedge A) = A$.

□

Hence, $(\mathcal{P}(U), \cap, \cup)$ is an example of a lattice.

Lemma. In every lattice we have

$$a \wedge b = a \quad \text{if and only if} \quad a \vee b = b.$$

□

Justification. Assume that $a \wedge b = a$. Then $b = b \vee (a \wedge b)$ (property 4); hence, $b = b \vee a$ because $a \wedge b = a$.

Similarly, assume that $a \vee b = b$. Then $a = a \wedge (b \vee a) = a \wedge (a \vee b) = a \wedge b$ because $a \vee b = b$. □

6.2.2 Partial Order on a Lattice. On $\mathcal{P}(U)$ we have not only two operations (union and intersection) but we have a partial order $\subseteq$ at the same time (for the definition of a partial order see **??**). The following proposition states that in **any** lattice we can define a partial order, so any lattice is a poset. (Note that the opposite implication does not hold, there are posets which are not lattices.)

Proposition. Given a lattice $(M, \wedge, \vee)$. Define a relation $\sqsubseteq$ on M by:

$$a \sqsubseteq b \ \text{ if and only if } a \wedge b = a \ (\text{iff } a \vee b = b).$$

Then the relation $\sqsubseteq$ on a lattice $(M, \wedge, \vee)$ is reflexive, antisymmetric, and transitive; i.e. it is a partial order on M (and $(M, \sqsubseteq)$ is a poset). □

Justification. Let $(M, \wedge, \vee)$ be a lattice. Because for every element $a \in M$ we have $a \wedge a = a$, it holds that $a \sqsubseteq a$. In other words, the relation $\sqsubseteq$ is reflexive.

Assume that for some $a, b \in M$ it holds that $a \sqsubseteq b$ and $b \sqsubseteq a$. Then the first fact means that $a \wedge b = a$ and the second one $b \wedge a = b$. Since $a \wedge b = b \wedge a$, we get $a = b$, and the relation is antisymmetric.

Assume that for some $a, b, c \in M$ it holds that $a \sqsubseteq b$ and $b \sqsubseteq c$. Then $a \wedge b = a$ and $b \wedge c = b$. Hence

$$a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a.$$

Therefore $a \sqsubseteq c$ and the relation is transitive. □

For the lattice $(\mathcal{P}(U), \cap, \cup)$ the partial order $\sqsubseteq$ is the relation "to be a subset", i.e. $A \sqsubseteq B$ if and only if $A \subseteq B$.

6.2.3 Remark. The operations $\wedge$ and $\vee$ are sometimes called an *infimum* and a *supremum*. This is because in the poset $(M, \sqsubseteq)$ the element $a \wedge b$ is the greatest lower bound and $a \vee b$ is the smallest upper bound of the set $\{a, b\}$.

6.2.4 The Smallest Element 0, and the Greatest Element 1.

Definition. Given a lattice $(M, \wedge, \vee)$. An element $\mathbf{0}$ for which

$$\mathbf{0} \wedge a = \mathbf{0}, \ \ \mathbf{0} \vee a = a \quad \text{for every } a \in M.$$

is called the *smallest element* of $(M, \wedge, \vee)$.

An element $\mathbf{1}$ for which

$$\mathbf{1} \wedge a = a, \ \ \mathbf{1} \vee a = \mathbf{1} \quad \text{for every } a \in M.$$

is called the *greatest element* of $(M, \wedge, \vee)$. □

Note that for $\mathbf{0}$ and any $a \in M$ we have $\mathbf{0} \sqsubseteq a$ for every $a \in M$; analogously, $a \sqsubseteq \mathbf{1}$ for every $a \in M$. Therefore, $\mathbf{0}$ is really the smallest element and $\mathbf{1}$ the greatest element of the poset $(M, \sqsubseteq)$.

6.2.5 Distributive Lattices. In $(\mathcal{P}(U), \cap, \cup)$ there are other laws that hold, two distributive laws are among them. On the other hand there are lattices where distributivity laws do not hold.

Definition. A lattice $(M, \wedge, \vee)$ is called a *distributive lattice* if it satisfies the distributive laws: For every elements $a, b, c \in M$ it holds that

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c), \;\; a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

□

It can be shown that if one of the distributivity laws holds so does the other one. Indeed, let us show e.g. that $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ for **every** $a, b, c \in M$ implies $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

Let us calculate:

$$(a \vee b) \wedge (a \vee c) = ((a \vee b) \wedge a) \vee ((a \vee b) \wedge c).$$

we used the first distributivity law for $(a \vee b)$, a, and c. Further,

$$((a \vee b) \wedge a) \vee ((a \vee b) \wedge c) = a \vee ((a \vee b) \wedge c) = a \vee (c \wedge (a \vee b)).$$

We used the absorption law 4, and commutativity. Now, the first distributivity law yields

$$a \vee (c \wedge (a \vee b)) = a \vee ((c \wedge a) \vee (c \wedge b)) = (a \vee (c \wedge a)) \vee (c \wedge b) = a \vee (b \wedge c).$$

as required.

Moreover, it is not difficult to see that in any lattice we have

$$(a \wedge b) \vee (a \wedge c) \sqsubseteq a \wedge (b \vee c), \;\; a \vee (b \wedge c) \sqsubseteq (a \vee b) \wedge (a \vee c).$$

6.2.6 Complements in Distributive Lattices. Another notion known from sets is a complement of a set A, i.e. the set of all those elements which do not belong to A.

Definition. Given a distributive lattice $(M, \wedge, \vee)$ with the smallest element $\mathbf{0}$ and the greatest element $\mathbf{1}$. We say that an element b is a *complement of* a, if

$$a \wedge b = \mathbf{0}, \;\text{ and }\; a \vee b = \mathbf{1}. \tag{6.1}$$

The complement of a is denoted by $\overline{a}$. □

The notation from the above definition is justified by the following proposition.

Proposition. Let $(M, \wedge, \vee)$ be a distributive lattice. Then if for $a, b, c \in M$ we have

$$a \vee b = a \vee c \quad \text{and} \quad a \wedge b = a \wedge c$$

then $b = c$.

Specially, if a has a complement, then the complement is unique. □

Justification. Assume that $a \vee b = a \vee c$ and $a \wedge b = a \wedge c$. Let us compute

$$b = (b \vee a) \wedge b = (a \vee b) \wedge b = (a \vee c) \wedge b = (a \wedge b) \vee (c \wedge b) = (a \wedge c) \vee (c \wedge b) =$$

$$= (c \wedge a) \vee (c \wedge b) = c \vee (a \wedge b) = c \vee (a \wedge c) = c,$$

as stated. □

Remark. Let us mention that a complement can be defined also in lattices that are not distributive; only one element can have more that one complement in lattices that are not distributive.

6.2.7 Boolean Algebras. Definition. A *Boolean algebra* is a distributive lattice with the smallest element $\mathbf{0}$ and the greatest element $\mathbf{1}$ in which every element has its complement. □

Proposition. Let $(B, \wedge, \vee)$ be a Boolean algebra with the smallest element $\mathbf{0}$, the greatest element $\mathbf{1}$, and the complement . Then for every elements $a, b, c \in B$ it holds that

1. $\overline{\mathbf{0}} = \mathbf{1}$, $\overline{\mathbf{1}} = \mathbf{0}$.
2. $\overline{a \wedge b} = \overline{a} \vee \overline{b}$, $\overline{a \vee b} = \overline{a} \wedge \overline{b}$.
3. $\overline{\overline{a}} = a$.

□

Justification. 1. follows from the fact that $\mathbf{0} \wedge \mathbf{1} = \mathbf{0}$ and $\mathbf{0} \vee \mathbf{1} = \mathbf{1}$.

2. It is an easy calculation. We show the first identity. We have

$$(a \wedge b) \wedge (\overline{a} \vee \overline{b}) = ((a \wedge b) \wedge \overline{a}) \vee ((a \wedge b) \wedge \overline{b}) = (\mathbf{0} \wedge b) \vee (a \wedge \mathbf{0}) = \mathbf{0}.$$

We used distributivity, associativity, commutativity and the fact that $a \wedge \overline{a} = \mathbf{0}$.

Similarly,

$$(a \wedge b) \vee (\overline{a} \vee \overline{b}) = (a \vee (\overline{a} \vee \overline{b}) \wedge (b \vee (\overline{a} \vee \overline{b})) = (\mathbf{1} \vee \overline{b}) \wedge (\mathbf{1} \vee \overline{a}) = \mathbf{1}.$$

We used distributivity, associativity, commutativity and the fact that $a \vee \overline{a} = \mathbf{1}$.

3. Indeed, a is the element for which $\overline{a} \vee a = \mathbf{0}$ and $\overline{a} \wedge a = \mathbf{1}$. □

Remark. We know that $\mathcal{P}(U)$ with the operations $\cap$ and $\cup$, where $\mathbf{0} = \emptyset$, $\mathbf{1} = U$ and $\overline{A} = \{x \in U \,|\, x \notin A\}$ forms a Boolean algebra. There are other Boolean algebras. We will end this chapter with description of all finite Boolean algebras. The one used mostly is the smallest one (and sometimes called "the Boolean algebra").

6.2.8 Boolean algebra B_2. The smallest Boolean algebra has 2 elements, 0 and 1 and operations are defined by:

Let $B_2 = \{0, 1\}$. Define

1. $\wedge$ is the logical product, i.e. $i \wedge j = \min\{i, j\}$,
2. $\vee$ is the logical addition, i.e. $i \vee j = \max\{i, j\}$,
3. $\mathbf{0} = 0$, $\mathbf{1} = 1$, and
4. $\overline{0} = 1$, $\overline{1} = 0$.

It is straightforward to verify all the properties that a Boolean algebra has.

6.2.9 Finite Boolean Algebras. For any $n = 2^k$ there is a Boolean algebra with n elements. It is the following one:

Denote by B_n the set of all k-tuples of 0 and 1, i.e.

$$B_n = \{(a_1, a_2, \dots, a_k) \mid a_i \in \{0, 1\}\}.$$

Define

1. $(a_1, a_2, \dots, a_k) \wedge (b_1, b_2, \dots, b_k) = (a_1 \wedge b_1, a_2 \wedge b_2, \dots, a_k \wedge b_k)$,
2. $(a_1, a_2, \dots, a_k) \vee (b_1, b_2, \dots, b_k) = (a_1 \vee b_1, a_2 \vee b_2, \dots, a_k \vee b_k)$,
3. $\mathbf{0} = (0, 0, \dots, 0)$, $\mathbf{1} = (1, 1, \dots, 1)$,
4. $\overline{(a_1, a_2, \dots, a_k)} = (\overline{a_1}, \overline{a_2}, \dots, \overline{a_k})$.

Then B together with the above operations forms a Boolean algebra with $n = 2^k$ elements.

Notice that B_n can be viewed as the set of characteristic functions of subsets of $U = \{1, 2, \dots, k\}$. On the other hand, you can look at B_n as a cartesian product of k copies of B_2 where operations are coordinatewise.

It can be proved that the Boolean algebras above are unique up to renaming elements (i.e. up to an isomorphism) and that there are no other finite Boolean algebras.