# XP33CHM Lecture notes

Dominika Burešová, Mirko Navara, Pavel Pták, Jan Ševic

17th January 2025

## 1 Notes on sets

It stands to reason that if there is an **injection** $f\colon K \to M$ then card $K$ **should not** be bigger than card $M$. Let $\mathbb{Q}$ be the set of all rational numbers and $\mathbb{N} = \{1, 2, \ldots, n, \ldots\}$ be the set of all natural numbers. The set $\mathbb{Q}$ seems bigger than $\mathbb{N}$...

**Proposition 1.1.** *There is an injection* $f\colon \mathbb{Q} \to \mathbb{N}$.

*Proof.* $f(a/b) = 2^a \cdot 3^b$. Check that $f$ is injective. We have to show that if $a/b \neq c/b$ then $f(a/b) \neq f(c/b)$. Indeed, if $a = c$ then it is clear. If $a \neq c$ then $f(a/b) = 2^a \cdot 3^b$ and $f(c/d) = 2^c \cdot 3^d$. Suppose that $a > c$. If $2^a \cdot 3^b = 2^c \cdot 3^d \implies 2^{a-c} \cdot 3^b = 3^d$. Then one side is even and one side is odd. This is absurd.
By an analogous idea, we can find an injective mapping $g : \mathbb{Q}^n \to \mathbb{N}$. So, in other words, a finite Cartesian product of countable sets is countable (Bourbaki method). □

**Proposition 1.2.** *Let us denote by* $\exp S$ *the set of all subsets of* $S$. *Then* $\operatorname{card} \exp S > \operatorname{card} S$.

*Proof.* Let us prove it by contradiction. Suppose that $\operatorname{card} \exp S = \operatorname{card} S$. Then there is an injection $f\colon \exp S \to S$. This implies that there is a surjection $g\colon S \to \exp S$. Consider the following set $T = \{x \in S \mid x \notin g(x)\}$. Since $g$ is onto $\exp S$, there is some $y$, $y \in S$, such that $g(y) = T$. If $y \in g(y)$ then by the definition $y \notin g(y)$. If $y \notin g(y)$, then $y \in g(y)$. A contradiction. □

So we have proved something out of nothing...?! Bizarre.

## 2 Partially ordered sets (posets) and quantum logics

### 2.1 Partial ordering

**Definition 2.1.** *Suppose that* $M$ *is a set. The relation* $\leq$ *on* $M$ *is said to be a* ***partial ordering*** *if* $(a, b, c \in M)$:

1. $\leq$ *is reflexive:* $a \leq a$,
2. $\leq$ *is antisymmetric:* $a \leq b, b \leq a \implies a = b$,
3. $\leq$ *is transitive:* $a \leq b, b \leq c \implies a \leq c$.

**Note 2.2.** $\leq$ *is said to be* ***linear*** *if for any pair* $a, b \in M$ *it holds* $a \leq b$ *or* $b \leq a$. *So in this case any pair* $a, b \in M$ *is comparable.*

**Examples 2.3.**

- *The standard ordering on real numbers* $(\mathbb{R}, \leq)$,
- $(\mathbb{R}^n, \leq)$ *coordinatewisely (note that this ordering is not linear),*
- $(\exp S, \subseteq)$, $\leq$ *is given by inclusion,* $A \leq B \iff A \subseteq B$ *(subset).*

**Definition 2.4.** $(M, \leq)$ *is said to be a* ***lattice*** *if any pair* $a, b \in M$ *has a supremum (a least upper bound) and an infimum (a greatest lower bound).*

**Definition 2.5.** *Let* $(M, \leq)$ *be a poset with* $0$ *and* $1$, $0$ *is the smallest element,* $1$ *is the greatest. Let* $'$ *be an operation on* $(M, \leq)$ *such that* $'\colon M \to M$ *and* $'$ *satisfies the following* $3$ *conditions:*

1. $a \leq b \implies b' \leq a'$,

2. $a'' = a$,

3. $a \vee a' = 1$, $a \wedge a' = 0$.

*Then* $(M, \leq, ', 0, 1)$ *is said to be an* ***orthocomplemented poset***.

The same definition applies for lattices as well.

### 2.2 Ordered structures

We want to study the structures called **quantum logics**. They are associated to the events of quantum experiments. The following axioms are relevant.
Let $(M, \leq, ', 0, 1)$ be an orthocomplemented poset (respectively an orthocomplemented lattice). We say that $(M, \leq, ', 0, 1)$ is

**a)** **orthomodular** if (for $a, b, c \in M$) we have $a \leq b \implies b = a \vee (b \wedge a')$; this structure is called a **quantum logic**.

**b)** **modular** if we have $a \geq b \implies a \wedge (b \vee c) = b \vee (a \wedge c)$.

**c)** **distributive** if $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ ; this structure is called **Boolean**.

Obviously, **c)** $\implies$ **b)** $\implies$ **a)**.

**Definition 2.6.** *Let $M$ be a set of an even number of elements. Let us consider all subsets of $M$ with an even number of elements. Let us denote it as $M_{even}$. It is easy to see that $M_{even}$ is an orthomodular poset.*

**Example 2.7.** $(M, \leq, ', \emptyset, \{1, 2, 3, 4\})$, *where* $M = \{1, 2, 3, 4\}_{even} = \{\emptyset, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{1, 2, 3, 4\}\}$; $\leq$ *is the inclusion,* $'$ *is forming a complement in* $\{1, 2, 3, 4\}$.

**Examples 2.8.**

- $M = \{1, 2, 3, 4\}_{even}$ *is an orthomodular lattice.*
- $M = \{1, 2, 3, 4, 5, 6\}_{even}$ *is an orthomodular poset but obviously not a lattice.*
- $\exp S$ *is Boolean.*

An important example in theoretical physics and elsewhere is the following classics.

**Theorem 2.9.** *Let $P$ be a finite-dimensional linear space. Let $L(P)$ be the lattice of all linear subspaces of $P$. Let $\leq$ be given by inclusion and $': L(P) \to L(P)$ be given by the orthogonal complement. Then $(L(P), \subseteq, ', \{\vec{0}\}, P)$ is a modular lattice.*

*Proof.* $L(P)$ is a lattice, $A \wedge B = A \cap B$ (the intersection of two linear subspaces is a linear subspace), $A \vee B = \text{Span}(A \cup B)$. Suppose $A, B, C \in L(P)$. We are to show $B \subseteq A \implies A \wedge (B \vee C) = B \vee (A \wedge C)$. Obviously, $B \vee (A \wedge C) \subseteq A \wedge (B \vee C)$.
Now we have to verify the second inclusion. Let $x \in A \wedge (B \vee C)$ and we have to show that $x \in B \vee (A \wedge C)$. So $x \in A$ and $x \in (B \vee C)$. Thus there exists $b \in B, c \in C$ with $x = b + c$. Therefore $c = x - b$ which means that $c \in (A \vee B) = A$. Since we already know that $c \in C$ we see that $c \in (A \wedge C)$. So $x \in B \vee (A \wedge C)$. This is what we wanted to show. □

# 3 Boolean algebra

Let us recall that $\vee$ denotes supremum and $\wedge$ denotes infimum. We know that Boolean algebra is distributive (unlike general quantum logics). A simple illustrating example of a non-distributive poset is $4_{\text{even}}$. (Take $a = \{1, 2\}$, $b = \{2, 3\}$ $c = \{3, 4\}$. We have $a \wedge (b \vee c) = a \wedge \{1, 2, 3, 4\} = a$. However, $(a \wedge b) \vee (a \wedge c) = \emptyset \vee \emptyset = \emptyset$.)

**Note 3.1.** *Observe that the equation that defines distributivity:*

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

*implies the dual equation:*

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

**Note 3.2.** *The lattice* $\exp S$ *of all subsets of* $S$ *is distributive (* $\leq$ *is the inclusion on* $\exp S$ *– recall that by our convention* $A \leq B$ *means* $A \subseteq B$*, the improper inclusion "smaller than or equal to"). Also, the finite-cofinite subsets of* $S$ *form a distributive lattice.*

The following deep theorem belongs to the foundations of modern mathematics. Prior to the formulation, recall that we say that two Boolean algebras $B_1, B_2$ are (Boolean) isomorphic if there is an isomorphism $i\colon B_1 \to B_2$, i.e., a bijection that preserves operations $\vee$, $\wedge$ and $'$. If $B_1$ is isomorphic with $B_2$ we allow ourselves to say "$B_1$ is $B_2$".

**Theorem 3.3** (**Stone's Theorem**)**.** *Let* $B_1$ *be a Boolean algebra. Then there is a set-representable Boolean algebra* $B_2 = (S, \mathcal{B})$ *such that* $B_1$ *is isomorphic to* $B_2$*. (We sometimes write* $(S, \mathcal{B})$ *instead of* $\mathcal{B}$ *when we need to refer to the underlying set* $S$*. The set* $S$ *is obviously not unique. Note also that the "abstract" operations* $\vee$*,* $\wedge$*, and* $'$ *of* $B_1$ *are transformed to the set operations* $\cup$*,* $\cap$*, and the set-theoretical complementation in* $S$*.)*

This theorem is **highly nontrivial** and more detailed explanation including a proof will be provided later. At this moment we will present some of its applications. Now let us formulate one of its applications that is structurally important and its proof becomes trivial once one is aware of Stone's Theorem. Prior to that, let us recall a definition of local finiteness.

**Definition 3.4.** *Standardly, a subset of an orthomodular poset is said to be an* ***orthomodular subposet*** *if it is an orthomodular poset itself (with the operations inherrited from the bigger orthomodular poset).*

**Definition 3.5.** *An orthomodular poset* $(L, \leq, 0, 1)$ *is said to be* ***locally finite*** *if, for each finite subset* $F$ *of* $L$*, the smallest orthomodular subposet of* $(L, \leq, 0, 1)$ *that contains* $F$ *is finite.*

Typically, $(L, \leq, 0, 1)$ is not locally finite. But...

**Theorem 3.6.** *Each Boolean algebra is locally finite.*

*Proof.* Let $B$ be a Boolean algebra. By Stone's Theorem, we can view $B$ as a collection of subsets of a set, $S$, and understand the operations set-theoretically. Let $F = \{A_1, A_2, \ldots, A_n\}$ be a finite collection of elements of $B$. Consider the elements $A_1^{i_1} \cap A_2^{i_2} \cap \ldots \cap A_n^{i_n}$, where each $i_j$ $(j \leq n)$ is either 1 or $-1$ and we define $A_j^1 = A_j$, $A_j^{-1} = A_j' = S \setminus A_j$. It is easy to check (draw a figure) that in the way described above we obtain $2^n$ elements $A_1^{i_1} \cap A_2^{i_2} \cap \ldots \cap A_n^{i_n}$ of $B$ that are pairwisely disjoint and their union is $S$. Hence the smallest Boolean subalgebra of $B$ that contains $F$ must consist of disjoint unions of some families of these $2^n$ sets and therefore its cardinality is at most $2^{2^n}$. The proof is complete. □

# 4 Stone's Theorem

## 4.1 Representation of a finite Boolean algebra

When an engineer is asked what a Boolean algebra is, he usually replies "zeros and ones". We shall not laugh at him because, technically, this response is not wrong ☺.

**Theorem 4.1.** *Every finite Boolean algebra is Boolean isomorphic to a Boolean algebra of all subsets of a finite set.*

In simple words, a finite Boolean algebra is a system of all subsets of a finite set (with operations $\cup, \cap, '$). Indeed, if we take the atoms (the smallest non-zero elements) of the algebra, the presence of distributivity gives us that the atoms are generators of the Boolean algebra. Obviously, the algebra must be (isomorphic) to $\exp\{1, 2 \ldots n\}$ ($n$ means the number of atoms). However, we know that every subset is determined by a characteristic function on a finite set. Hence, a finite sequence of 0's and 1's.

- $\emptyset \to$ all 0,
- $X \to$ all 1,
- $\mathrm{mod}_2 \to \triangle = \mathrm{XOR}$.

This was easy. No Stone's Theorem was needed. All is done by simple observations.

## 4.2 Representation of (infinite) Boolean algebra

However, the world of infinite mathematics is much more complicated and scary ☹ and the Stone's Theorem must cope with it. There is to be **a lot** of preparatory work and strategical remarks.
One has further to analyze orthocomplemented lattices, the distributive lattices and ideals on them as well as the extensions of ideals. The harvest of the analysis conveys the following moral: **There are no other Boolean algebras than those that are set-representable!**

**Definition 4.2.** *Let $L = (X, \wedge, \vee, 0, 1)$ ($\wedge, \vee$ are binary operations) be an algebra such that for $a, b, c \in X$ we have:*

1. $a \wedge a = a$, $a \vee a = a$ *(idempotence),*
2. $a \wedge b = b \wedge a$, $a \vee b = b \vee a$ *(commutativity),*
3. $(a \wedge b) \wedge c = a \wedge (b \wedge c)$, $(a \vee b) \vee c = a \vee (b \vee c)$ *(associativity),*
4. $a \wedge (a \vee b) = a$, $a \vee (a \wedge b) = a$ *(absorption).*

*Thus this is a universal algebraic definition of a lattice. By defining an ordering, it will become equivalent with a lattice in terms of ordering. We will set $a \leq b$, precisely when $a \wedge b = a$, equivalently $a \vee b = b$.*

**Definition 4.3.** *An **orthocomplemented lattice** is a lattice $L = (X, \wedge, \vee, ', 0, 1)$ enriched with a unary operation (**orthocomplementation**) $': X \to X$ and axioms that apply to that operation:*

1. $a \wedge a' = 0$, $a \vee a' = 1$,
2. $a \leq b \implies b' \leq a'$,
3. $a'' = a$.

Let us now recall a definition of distributivity.

**Definition 4.4.** *Let $(L, \leq)$ be a lattice. Let $\wedge, \vee$ be lattice operations given by $\leq$. Lattice $(L, \leq)$ is called **distributive** if $\forall a, b, c \in L$ the following conditions (known as distributive laws) hold:*

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

Note that we showed in Note 3.1 that condition 1 implies condition 2.
Recall the notion of a set-representable Boolean algebra. Now we will recall characterization of set-representable Boolean algebra.

**Theorem 4.5** (**A characterization of set-representable Boolean algebra**)**.** *Let $S$ be a set and $\exp(S)$ be the set of all subsets of $S$. Let $\mathcal{S} \subseteq \exp(S)$ be a system of subsets that has a Boolean structure. It means that:*

1. $\mathcal{S}$ *contains* $\emptyset$,
2. $A \in \mathcal{S} \implies S \setminus A \in \mathcal{S}$ *(closedness under complement),*
3. $A, B \in \mathcal{S} \implies A \cap B$ *(closedness under intersection).*

*Vice versa if a system $\mathcal{S} \subseteq S$ satisfies conditions 1., 2., 3. the system $\mathcal{S}$ is a Boolean algebra.*

Now we can state that no other Boolean algebras than the set-representable ones with operations $\cap, \cup, ', \emptyset, S$ exist. Well, almost. We only need to prove it first ☺.

### 4.2.1 Preparatory work

Numerous auxiliary lemmas will be stated and proved. This is a technical part ☹ of the proof of Stone's Theorem.

**Lemma 4.6.** *Let $B$ be a Boolean algebra. For $a, b \in B$ we have $a \wedge b = 0 \iff a \leq b'$.*

*Proof.* $\implies$**:** $a \wedge b = 0 \implies (a \wedge b) \vee b' = b'$. The left side: $(a \wedge b) \vee b' = b' \vee (a \wedge b)$ (by commutativity) $= (b' \vee a) \wedge (b' \vee b)$ (by distributivity) $= b' \vee a$. Hence $b' \vee a = b'$ which means that $b' \geq a$.
$\impliedby$**:** $a \leq b' \implies a \wedge b \leq b' \wedge b \implies a \wedge b \leq 0 \implies a \wedge b = 0$. □

**Consequence 4.7.** $a \leq b \iff a \wedge b' = 0$*. Indeed,* $a \wedge b' = 0 \iff a \leq (b')' \iff a \leq b$.

**Definition 4.8** (**Ideal**)**.** *Let $B$ be a Boolean algebra. $I \subseteq B$, $I \neq \emptyset$ is called an* ***ideal*** *(in $B$) if it has the following properties:*

1. $a \in I$, $b \leq a \implies b \in I$ *(Intuitively, it is a segment. With every element it contains everything below.)*
2. $a, b \in I \implies a \vee b \in I$ *(closedness under suprema).*
3. $1 \notin I$.

**Definition 4.9** (**Prime ideal**)**.** *We call an ideal $I$ a* ***prime ideal*** *if $\forall a \in B$ either $a \in I$ or $a' \in I$.*

**Example 4.10.** *Let $B = \exp \mathbb{N}$ and let $I$ be the set of all finite subsets of $\mathbb{N}$. Then $I$ is an ideal. However, $I$* ***is not*** *a prime ideal.*

**Definition 4.11** (**Two-valued state**)**.** *Let $B$ be a Boolean algebra. A mapping $s \colon B \to \{0, 1\}$ is a two-valued state if $\forall a, b \in B$ we have:*

1. $s(1) = 1$,
2. $a \wedge b = 0 \implies s(a) + s(b) = s(a \vee b)$.

This is a fundament of mathematical logic!

**Lemma 4.12** (**Correspondence of the prime ideals with two-values states**)**.** *Let $B$ be a Boolean algebra. Then $I \subseteq B$ is a prime ideal in $B \iff I = \{a \mid s(a) = 0\}$ for some two-valued state $s$ on $B$.*

*Proof.* Left as an exercise. Hint: verify the axioms of a state. □

**Lemma 4.13.** *Let $B$ be a Boolean algebra. Let $s$ be a two-valued state. Then:*

1. $s(a \wedge b) = 1$ *if and only if* $\big(s(a) = 1$ *and* $s(b) = 1\big)$,
2. $s(a \vee b) = 1$ *if and only if* $\big(s(a) = 1$ *or* $s(b) = 1\big)$.

*Proof.* 1. $\impliedby$**:** As $a \vee b \geq a$, $s(a \vee b) \geq s(a) = 1$ and $s\big((a \wedge b)'\big) = 0$. By De-Morgan law, we know that $s\big((a \wedge b)'\big) = s(a' \vee b') = 0$. And therefore $s(a') = 0$ and $s(b') = 0$. The rest is obvious. 1. $\implies$**:** Triv. 2. $\implies$**:** $s(a \vee b) = s(a) + s(a' \wedge b)$. If $s(a) = 0$, $s(a' \wedge b)$ must be 1. However, $s(a' \wedge b) \leq s(b)$. Hence $s(b) = 1$. 2. $\impliedby$**:** Triv. □

### 4.2.2 Putting pieces together

Now we will move to the most important part ☺ of the proof by proving Weaker Stone's Lemma and Stronger Stone's Lemma. The proof is very interesting and heavily based on Zorn's Lemma. (We call a set in a poset a **chain** if it is linearly ordered, i.e., every two elements $a, b$ are comparable, $a \leq b$ or $b \leq a$.)

**Lemma 4.14** (**Zorn's Lemma**)**.** *Let $M$ be a poset such that for each chain $R$ in $M$ we have:*

$$\exists a \in M \ \forall b \in R : b \leq a\,.$$

*Then :*

$$\forall b \in M \ \exists c \in M : b \leq c, \ \ c \text{ is maximal in } M\,.$$

*Intuitively, each element of $M$ is dominated by a maximal element.*

**Lemma 4.15** (**Weaker Stone's Lemma**). *Let $B$ be a Boolean algebra, $a \in B$, $a \neq 1$. Then there exists prime ideal $I$ with $a \in I$.*

*Proof.* We consider $I_a = \{x \in B \mid x \leq a\}$. We take the set $J$ of all ideals in $B$ that contain $a$ and not 1. This is non-empty as it contains $I_a$. We will order $J$ by inclusion and get a poset $(J, \leq)$. The question is if this poset has a maximal element. We need to check the assumptions of Zorn's Lemma. Each chain of such ideals has an upper bound in $J$, its union (it is obviously an ideal that contains $a$, and does not contain 1). Therefore, $J$ has a maximal element. Let us denote it by $I$. We want to prove that $I$ is a prime ideal. Suppose for a contradiction that $I$ (that is the maximal element of $J$) is **not** a prime ideal. Then $\exists b \in B$ such that $b \notin I$ and $b' \notin I$. Let us consider $I_b = \{x \in B \mid x \leq b\}$. Now we consider $\tilde{I} = \{x \in B \mid x \leq (u \vee v), u \in I, v \in I_b\}$. The question is if $\tilde{I}$ is an ideal in $J$. We will proceed from the easiest to the most difficult. $\tilde{I}$ contains $I$, so it contains $a$. $\tilde{I}$ is a union of segments; thus, with each $u \in \tilde{I}$, it contains all elements below it. Let us check the closedness under the formation of suprema. Let $x, y \in \tilde{I}$. Then $x \leq u_1 \vee v_1$, $y \leq u_2 \vee v_2$ for some $u_1, u_2 \in I$, $v_1, v_2 \in I_b$, and

$$x \vee y \leq (u_1 \vee v_1) \vee (u_2 \vee v_2) \,.$$

So (as it follows from commutativity and associativity)

$$x \vee y \leq (u_1 \vee u_2) \vee (v_1 \vee v_2) \,.$$

$I$ and $I_b$ are ideals, so they are closed under the formation of suprema, $u_1 \vee u_2 \in I$, $v_1 \vee v_2 \in I_b$, and $x \vee y \in \tilde{I}$. Now we have to verify that $\tilde{I}$ does not contain 1. Suppose for a contradiction that $1 \in \tilde{I}$. Then $1 \leq u \vee v$, moreover, $1 = u \vee v$, for some $v \in I_b$, therefore $v \leq b$ and so $1 = u \vee b$. Trick: $b' = b' \wedge 1$. So $b' = b' \wedge (u \vee b)$. We get $b' = (b' \wedge u) \vee (b' \wedge b)$ (from distributivity). Hence we have $b' = b' \wedge u$. That is $b' \leq u$. However, $u \in I$, $I$ is an ideal, so everything $\leq u$ is in $I$. However, $b' \notin I$. We got a contradiction with maximality. □

**Lemma 4.16** (**Stronger Stone's Lemma**). *Let $B$ be a Boolean algebra, let $a, b \in B$ be non-comparable. Then there exists a two-valued state $s$ such that $s(a) = 1$ and $s(b) = 0$.*

*Proof.* We know by Lemma 4.6 that if $a, b$ are non-comparable, then $a \wedge b' \neq 0$. We come to the complement $(a \wedge b')' \neq 1$. We apply Weaker Stone's Lemma. So we know that there exists a prime ideal that contains $(a \wedge b')'$. We will use the correspondence of prime ideals with two-values states and we get $s\big((a \wedge b')'\big) = 0$. So $s(a \wedge b') = 1$. However, with the use of Lemma 4.13, this is possible if and only if $s(a) = 1$ and $s(b') = 1$. Therefore $s(a) = 1$ and $s(b) = 0$. □

## Stone continued.

Let us summarize our results so far. We have proved that a Boolean algebra always has "a lot" of two-valued states (a lot of prime ideals), as many as to distinguish non-comparable elements. This allows us to think of a representation. Recall that if $B = (S, \Delta)$ is a Boolean algebra—actually $\Delta \subseteq \exp(S)$ is the Boolean algebra but often we want to refer to the underlying set $S$ as well, so we require that $\Delta$ is closed under the formation of the operations $\cap$, $\cup$ and $'$.
Now, let us get back to Theorem 4.5.

*Proof.* Let $S_2(B) =$ the set of all two-valued states on $B$. Let us consider the mapping

$$i : B \to \exp(S) \text{ where } i(a) = \{s \in S_2(B) \mid s(a) = 1\} \,.$$

We have to prove that $i$ is a Boolean isomorphism, i.e.

$$\begin{aligned} i(a \cap b) &= i(a) \cap i(b) \\ i(a \cup b) &= i(a) \cup i(b) \\ i(a') &= S \setminus i(a) \\ i(0) &= \emptyset \\ i(1) &= S \end{aligned}$$

Only the first two conditions are non-trivial. Let us prove the first one.
Obviously, if $s(a \cap b) = 1$ then $s(a) = s(b) = 1$. Vice versa, let $s(a) = 1$ and $s(b) = 1$. We have to show that $s(a \cap b) = 1$. This is equivalent to $s(a' \cup b') = 0$ (we use de Morgan law $(a \cap b)' = a' \cup b'$ and $s(a') = s(b') = 0$). But then $s(a' \cup b') = s(a') \cup s(b' \cap a') = 0 + 0 = 0$. Hence $s(a' \cup b') = 0$ and therefore $s(a \cap b) = 1$. □

Once again the moral of the story: Boolean algebras are set-representable. If $B$ is a Boolean algebra then take for $S$ the set $S_2(B)$ and for $\Delta$ the subsets of $S$ of the form $\{s \in S_2(B) \mid s(a) = 1\}$. Formally, $\Delta = \{M \subseteq S_2(B) \mid \exists a \in B : M = \{s \in S_2(B) \mid s(a) = 1\}\}$. The considerations above give us a proof. (Note that quantum logics need not be set-representable, since they need not have two-valued states (R. Greechie), e.g., $S_2(L(R^3)) = \emptyset$, Bell 1964, Kochen & Specker 1966.)

## Some lattice peculiarities

**Definition 4.17.** *Let $(L, \leq)$ be a lattice. Then $(L, \leq)$ is said to be*

1. *$\sigma$-complete if $\bigvee_{i \in \mathbb{N}} a_i$ exists in $L$ for any sequence $a_i$, $i \in \mathbb{N}$ (so any sequence of elements in $L$ has a supremum).*
2. *complete if $\bigvee_{i \in J} a_i$ exists in $L$ for any set $J \subseteq L$ (so $\bigvee_{i \in J} a_i$ exists in $L$ for an arbitrary set $J$).*

**Example 4.18.** *Let $S$ be an arbitrary infinite set and $L$ be a family of all finite subsets of $S$, $\subseteq$ being the inclusion. Then $(L, \subseteq)$ is not $\sigma$-complete. Similarly, if $S$ is uncountable and $L$ is the family of all countable subsets, then $L$ is not complete.*
*The lattice of all Borel sets of the real numbers (in $\mathbb{R}$) is not complete.*

**Theorem 4.19** (Tarski Fixed Point)**.** *Let $(L, \leq)$ be a complete lattice. Let $f : (L, \leq) \to (L, \leq)$ be an order-preserving mapping ($x \leq y \Rightarrow f(x) \leq f(y)$). Then $f$ has a fixed point ($\exists a \in L$ with $f(a) = a$).*

*Proof.* Let us set $S = \{x \in L \mid x \leq f(x)\}$. Then $S \neq \emptyset$ ($0 \in S$). Let us write $a = \sup S$. Then $\forall x \in S : x \leq f(x) \leq f(a)$. It implies $f(a) \leq f(f(a))$ and so $f(a) \in S$. We see that $f(a) \leq \sup S$ and therefore $f(a) = a$. □

**Note.** Davis 1985 – also vice versa: if each order-preserving mapping has a fixed point then the lattice is complete.

**Theorem 4.20** (Cantor-Bernstein)**.** *Suppose that $B, C$ are sets and suppose that $f : B \to C$, $g : C \to B$ are injective mappings. Then there is a bijection $i : B \to C$. (In other words, if $\operatorname{card} B \leq \operatorname{card} C$ and $\operatorname{card} C \leq \operatorname{card} B$, then $\operatorname{card} B = \operatorname{card} C$.)*

*Proof.* We will apply Theorem 4.19. Take the mapping $h : \exp(B) \to \exp(B)$

$$h(X) = B \setminus g(C \setminus f(X)).$$

To satisfy the assumptions of Tarski fixed point theorem, observe that $\exp B$ is complete and $h$ is order-preserving. Hence $h$ has a fixed point, $X_0$.
Thus $h(X_0) = X_0$. We can check that if we set

$$i(x) = f(x) \text{ provided } x \in X_0,$$
$$i(x) = g^{-1}(x) \text{ provided } x \in X \setminus X_0;$$

then we find that $i : B \to C$ is a bijection. □

**Theorem 4.21** (McNeille completion)**.** *Let $(L, \leq)$ be a poset. Then there is a completion of $(L, \leq)$. In other words, we can construct a complete $(\tilde{L}, \leq)$ such that there is an order embedding $i_{emb} : (L, \leq) \to (\tilde{L}, \leq)$. Moreover, there is such an embedding $i_{emb}$ that the following result is true: If $f : (L, \leq) \to (M, \leq)$ is an order-preserving mapping then $f$ can be extended in such a way that the extension $\tilde{f} : i_{emb}(L, \leq) \to i_{emb}(M, \leq)$ preserves infima and suprema.*

# 5 Elementary Proof of the Fundamental Theorem of Algebra

Let us prove a deep statement. Due to its importance, this result is known in the classical literature as the *Fundamental Theorem of Algebra*. Note that the first proof was given by K. F. Gauss (1777–1855) in 1799.
We will firstly state and prove auxiliary results and then we will put them together (similarly as we did in Section 4 ☺).

## 5.1 Preparatory work

**Lemma 5.1.** *Let $p \in \mathbb{C}[x]$ be a polynomial of degree at least one. Then*

$$\lim_{|z| \to +\infty} |p(z)| = +\infty$$

*(i.e., formally $\forall K \geq 0\ \exists r > 0\ \forall z \in \mathbb{C} : |z| > r \Rightarrow |p(z)| > K$).*

*Proof.* Let $p(z) = a_n z^n + \cdots + a_1 z + a_0$, where $n \geq 1$ and $a_n \neq 0$. Then

$$a_n z^n = p(z) - (a_{n-1} z^{n-1} + \cdots + a_1 z + a_0),$$

i.e.,

$$\begin{aligned} |a_n z^n| &= |p(z) - (a_{n-1} z^{n-1} + \cdots + a_1 z + a_0)| \\ &\leq |p(z)| + |a_{n-1} z^{n-1}| + \cdots + |a_1 z| + |a_0|. \end{aligned}$$

Thus

$$\begin{aligned} |p(z)| &\geq |a_n z^n| - |a_{n-1} z^{n-1}| - \cdots - |a_1 z| - |a_0| \\ &= |z|^n \left( |a_n| - |a_{n-1}| \frac{1}{|z|} - \cdots - |a_1| \frac{1}{|z|^{n-1}} - |a_0| \frac{1}{|z|^n} \right). \end{aligned}$$

As $|z| \to +\infty$, we have $|z|^n \to +\infty$ and

$$\left( |a_n| - |a_{n-1}| \frac{1}{|z|} - \cdots - |a_0| \frac{1}{|z|^n} \right) \to |a_n|.$$

From this, the statement follows. □

**Theorem 5.2.** *Let $p(x) \in \mathbb{C}[x]$ be a polynomial of degree at least one. Then the function $z \mapsto |p(z)|$ has an absolute minimum on $\mathbb{C}$.*

*Proof.* Let $p(z) = a_n z^n + \cdots + a_1 z + a_0$, $n \geq 1$, $a_n \neq 0$. Take the value $|p(0)| = |a_0|$. Then according to Lemma 5.1 there exists $r > 0$ such that for $z \in \mathbb{C}$, $|z| > r$ implies $|p(z)| > |p(0)|$. Let $S_r = \{z \in \mathbb{C} \mid |z| \leq r\}$. Then $S_r$ is a compact set, and therefore the function $z \mapsto |p(z)|$ (which is continuous on $\mathbb{C}$, and thus also on $S_r$) attains its minimum on it. Let this be at point $z_0$. Then at point $z_0$ the function $|p|$ has an absolute minimum:

1. if $z \in S_r$, then obviously $|p(z_0)| \leq |p(z)|$,
2. if $z \in \mathbb{C} \setminus S_r$, then $|z| > r$, and thus $|p(z)| > |p(0)| \geq |p(z_0)|$, since $0 \in S_r$.

□

**Theorem 5.3.** *Let $p(x) \in \mathbb{C}[x]$ be a polynomial of degree at least one and let $p(z_0) \neq 0$ hold at point $z_0 \in \mathbb{C}$. Then the function $z \mapsto |p(z)|$ does not have a local minimum at point $z_0$.*
*More specifically: There exists $\xi \in \mathbb{C}$ (direction of descent) such that for every sufficiently small $t > 0$ it holds:*

$$|p(z_0 + t\xi)| < |p(z_0)|$$

*(that is $\exists \xi \in \mathbb{C}\ \exists \varepsilon > 0\ \forall t \in (0, \varepsilon) : |p(z_0 + t\xi)| < |p(z_0)|$).*

*Proof.* Let $b_0 = p(z_0) \neq 0$. The polynomial $p(z) - b_0$ has the root $z_0$. Let $m \geq 1$ denote its multiplicity. There therefore exists polynomial $q(x) \in \mathbb{C}[x]$, such that $p(z) - b_0 = (z - z_0)^m q(z)$, where $\deg(q) \geq 0$, $q(z_0) \neq 0$. Let $b_1 = q(z_0)$. Choose $\xi \in \mathbb{C}$, $t \in \mathbb{R}$, and let's calculate the value $p(z_0 + t\xi)$:

$$\begin{aligned} p(z_0 + t\xi) &= b_0 + (t\xi)^m q(z_0 + t\xi) = b_0 + t^m \xi^m [q(z_0 + t\xi) - b_1 + b_1] \\ &= b_0 + t^m \xi^m b_1 + t^m \xi^m [q(z_0 + t\xi) - b_1]. \end{aligned}$$

Let $r(t) = q(z_0 + t\xi) - b_1$. Then $r(t)$ is a polynomial without absolute term. There exists therefore $K > 0$ such that

$$\forall t \in [0, 1] : |r(t)| \leq Kt.$$

(Proof: Let $r(t) = b_s t^s + \cdots + b_1 t = t(b_s t^{s-1} + \cdots + b_1)$. Then for $t \in [0, 1]$ holds

$$|r(t)| = |t| \, |b_s t^{s-1} + \cdots + b_1| \le |t| \, (|b_s| + \cdots + |b_1|).$$

Now it suffices to set $K = |b_s| + \cdots + |b_1|$.)
For any $t \in \mathbb{R}$ we see that:

$$p(z_0 + t\xi) = b_0 + t^m \xi^m b_1 + t^m \xi^m r(t) = b_0 \left(1 + t^m \xi^m \frac{b_1}{b_0} + t^m \xi^m \frac{1}{b_0} r(t)\right),$$
$$\text{i.e.} \quad |p(z_0 + t\xi)| = |b_0| \, |1 + t^m \xi^m \frac{b_1}{b_0} + t^m \xi^m \frac{1}{b_0} r(t)|.$$

About the last absolute value, we want to prove that for sufficiently small $t > 0$ it is $< 1$.
If we were to use the formula $|a + b + c| \le |a| + |b| + |c|$, we would not prove it. We must therefore separate two terms "not to add together" and the remaining term "separate". Since we already have an estimate for $|r(t)|$, we will "separate" the term $t^m \xi^m \frac{1}{b_0} r(t)$. For $t \in (0, 1)$, it holds:

$$\begin{aligned}|p(z_0 + t\xi)| &\le |b_0| \left(|1 + t^m \xi^m \frac{b_1}{b_0}| + |t^m \xi^m \frac{1}{b_0} r(t)|\right) \\ &\le |b_0| \left(|1 + t^m \xi^m \frac{b_1}{b_0}| + t^m \, |\xi^m \frac{1}{b_0}| \, K\right).\end{aligned}$$

If now the product $\xi^m \frac{b_1}{b_0}$ will be a real number, then for sufficiently small $t$

$$|1 + t^m \xi^m \frac{b_1}{b_0}| = 1 + t^m \xi^m \frac{b_1}{b_0}.$$

Then will be

$$|p(z_0 + t\xi)| \le |b_0| \left(1 + t^m \xi^m \frac{b_1}{b_0} + t^{m+1} |\xi^m| \frac{1}{|b_0|} K\right).$$

We now want that for every sufficiently small $t > 0$ would be

$$1 + t^m \xi^m \frac{b_1}{b_0} + t^{m+1} \, |\xi^m| \, \frac{1}{|b_0|} K < 1,$$

i.e. that

$$\xi^m \frac{b_1}{b_0} + t \, |\xi^m| \, \frac{1}{|b_0|} K < 0.$$

This will happen when $\xi^m \frac{b_1}{b_0} < 0$; for example when $\xi^m \frac{b_1}{b_0} = -1$, i.e. when $\xi^m = -\frac{b_0}{b_1}$. □

### 5.2 Putting pieces together

**Corollary 5.4** (Fundemental Theorem of Algebra)**.** *Let $p(x) \in \mathbb{C}[x]$ be a polynomial of degree at least one. Then $p$ has at least a root in the field $\mathbb{C}$.*

*Proof.* According to Theorem 5.2, the function $|p|$ attains its absolute minimum at some point $z_0 \in \mathbb{C}$. At this point $z_0$ then according to Theorem 5.3, it must be $p(z_0) = 0$. □

**Corollary 5.5.** *Every polynomial of degree $n$ has (including multiplicity) exactly $n$ roots.*

*Proof.* Simple induction argument using the previous corollary. □

## 6 Matrices

**Definition 6.1** (Transpose of a Matrix)**.** *Let $A = (a_{ij})$ be an $m \times n$ matrix over an arbitrary field. The* ***transpose*** *of $A$, denoted by $A^T$, is defined as the $n \times m$ matrix whose $(i, j)$-th entry is given by*

$$(A^T)_{ij} = a_{ji}.$$

**Definition 6.2** (Rank of a Matrix)**.** *Let $A$ be a matrix over a field (for instance, $\mathbb{R}$ or $\mathbb{C}$). The* ***rank*** *of $A$ is defined as the dimension of the vector space spanned by the rows of $A$ (referred to the* ***row space*** *of $A$, analogously we define a* ***column space*** *as a space that is spanned by columns of $A$). Thus, the rank of $A$ is the maximum number of linearly independent rows of $A$.*

**Theorem 6.3.** *For any matrix $A$, it holds that* $\operatorname{rank}(A) = \operatorname{rank}(A^T)$.

*Proof.* We will prove the inequality $\operatorname{rank}(A) \leq \operatorname{rank}(A^T)$. The opposite inequality will then follow from symmetry, since from it we immediately get

$$\operatorname{rank}(A^T) \leq \operatorname{rank}((A^T)^T) = \operatorname{rank}(A).$$

Let $r = \operatorname{rank}(A^T)$ be the maximum number of linearly independent *columns* in the matrix $A$. Take a basis of the column space, $\{c_1, c_2, \dots, c_r\}$. These vectors are linearly independent and generate all the columns of $A$. Thus, each column of $A$ can be expressed as a linear combination of the vectors $c_1, c_2, \dots, c_r$.
We use the fact that left multiplication by a matrix represents taking linear combinations of rows, while right multiplication corresponds to taking linear combinations of columns. Using the basis $\{c_1, c_2, \dots, c_r\}$, ($C$ is the matrix whose columns are the vectors $\{c_1, c_2, \dots, c_r\}$) we can write $A$ in the form $A = CR$, where the columns of $R$ are the coefficients of the respective linear combinations.
Viewing the equality $A = CR$ row-wise, we see that the rows of the matrix $R$ generate the row space of $A$. From this, it follows that

$$\operatorname{rank}(A) \leq \operatorname{rank}(R) \leq r = \operatorname{rank}(A^T).$$

□

Let us present another proof based on properties of scalar product (so, we assumed that the field in question has the scalar product).

*Proof.* Again, we prove $\operatorname{rank}(A) \leq \operatorname{rank}(A^T)$. Let $\{x_1, x_2, \dots, x_r\}$ be a basis of the *row* space of $A$ (here $r = \operatorname{rank}(A)$). Then $Ax_1, Ax_2, \dots, Ax_r$ lie in the column space of $A$.
We will show that the vectors $Ax_1, Ax_2, \dots, Ax_r$ are linearly independent. Suppose that, for some scalars $\alpha_1, \alpha_2, \dots, \alpha_r$,

$$\alpha_1 Ax_1 + \alpha_2 Ax_2 + \dots, + \alpha_r Ax_r = 0.$$

We are to show that all $\alpha_i$ are 0. Using linearity, our equation reads

$$A\left(\sum_{i=1}^{r} \alpha_i x_i\right) = 0.$$

If we write $v = \sum_{i=1}^{r} \alpha_i x_i$, we see that $v$ is orthogonal to all rows of $A$. As all $x_i$ were from the row space of $A$, so is $v$; it is orthogonal to the generators of this space, thus also to itself, $\langle v \mid v \rangle = 0$. From the properties of a scalar product, this implies $v = 0$. From the linear independence of the vectors $x_i$, we conclude that all $\alpha_i = 0$. Hence the vectors $A_{x_1}, A_{x_2} \dots A_{x_r}$ are linearly independent and we are done.

□

# 7 Fixed point theorem for contractive mappings in complete metric spaces

Now we will formulate and prove the famous Banach Fixed Point Theorem. The symbol $\exists!$ is a mathematical convention used instead of "there exists exactly one".

**Theorem 7.1** (Banach Fixed Point Theorem)**.** *Let $(X, d)$ be a complete metric space and let $g : (X, d) \to (X, d)$ be a contractive (hence automatically continuous) mapping*

$$\exists K, 0 < K < 1 \ \forall x, y \in X : d(g(x), g(y)) \leq K\, d(x, y)\,.$$

*Then $g$ has exactly one fixed point, i.e.,*

$$\exists!\, x \in X : g(x) = x\,.$$

*Proof.* Take any point $x_0 \in X$ and form a sequence $x_1 = g(x_0)$, $x_2 = g(x_1) = g^2(x_0), \ldots$, etc.
For $n \geq m$,

$$d(x_m, x_n) \leq K^m\, d(x_0, x_{n-m}) \leq K^m\, \frac{1 - K^{n-m}}{1 - K}\, d(x_0, x_1)\,.$$

Since $0 < K < 1$, we have $K^m\, \frac{1-K^{n-m}}{1-K}\, d(x_0, x_1) \to 0$ for $n, m \to \infty$.
Thus the sequence $(x_n)_{n\in\mathbb{N}}$ is Cauchy in $(X, d)$.
Since $(X, d)$ is a complete metric space (let us recall that in complete metric spaces, Cauchy and convergent sequences coincide), we have $x_n \to x$. Then necessarily $g(x) = x$. The uniqueness of this fixed point follows from the fact that the mapping is contractive. Indeed, if $x, y$ are fixed points of $g$, we obtain

$$d(x, y) = d(g(x), g(y)) \leq K\, d(x, y)\,,$$

which can be satisfied only if $d(x, y) = 0$. □

The theorem above is as simple as ingenious. The proof is also constructive and effectively provides the precision of the approximation. It can be easily shown (do check it!) that at the beginning of the procedure at point $x_0$, the following relations determine the achieved precision in the $n$-th step of approximation:

$$d(x_n, x) \leq \frac{K}{1 - K}\, d(x_{n-1}, x_n)\,,$$
$$d(x_n, x) \leq \frac{K^n}{1 - K}\, d(x_0, x_1)\,.$$

The possibilities for applying the fixed point theorem have proven to be large. Some are so "folkloristic" that we don't even realize them (for example, numerical methods for solving systems of linear equations like the Jacobi method or Gauss–Seidel method have their theoretical basis in the fixed point theorem). Let's outline a typical application; we'll dedicate a special section to the third one (construction of fractals) later.

**Example 7.2.** *Let's approximately solve the equation $f(x) = x^3 + 2x - 1 = 0$.*
*Solution: Define $g(x) = x - \lambda f(x)$, where $\lambda \in \mathbb{R}, 0 < \lambda \leq 1$ (suitable $\lambda$ will be determined later). It's clear that $f(x) = 0$ if and only if $g(x) = x$. Since $f(0) = -1$ and $f(1) = 2$, it's evident by the Darboux property that $f(x)$ has a root in $(0, 1)$. By choosing suitable $\lambda \in \mathbb{R}$, we'll prepare the situation for applying Banach's Fixed Point Theorem. Let's apply the mean value theorem from differential calculus ($g$ has a continuous derivative):*

$$\frac{g(x) - g(y)}{x - y} = g'(c) \text{ at some point } c \in (0, 1).$$

*From this we get $|g(x) - g(y)| = |g'(c)|\,|x - y|$. Since $g'(x) = 1 - \lambda f'(x) = 1 - \lambda(3x^2 + 2)$ and since $2 \leq f'(x) \leq 5$ on $[0, 1]$, we get $1 - 5\lambda \leq g'(x) \leq 1 - 2\lambda$. We can choose, for example, $\lambda = \frac{1}{5}$ and then we have $|g(x) - g(y)| \leq \frac{3}{5}|x - y|$. It's clear that $g\colon [0, 1] \to [0, 1]$ is contractive and thus we can use the convergence procedure of the fixed point theorem. If we set $x_0 = 0$, we get*
*$x_1 = 0.2$, $x_2 = 0.318$, $x_3 = 0.385$, $x_4 = 0.419$, $x_5 = 0.437$, etc.*
*How good approximation have we already obtained? Let's use the comparison of $x_n$ and the ideal $x$ given in the previous paragraph:*

$$\frac{3}{5} \cdot \frac{5}{2} \cdot 0.018 = 0.027$$

*Thus we see that we have a solution with guaranteed precision $0.027$.*
*The exact solution obtained by Cardano method is*

$$\frac{(108 + 12\sqrt{177})^{\frac{1}{3}}}{6} - \frac{4}{(108 + 12\sqrt{177})^{\frac{1}{3}}} \doteq 0.453397\ldots$$

# 8 The Perron–Frobenius Theorem

**Theorem 8.1** (Brouwer)**.** *Let $B_n$ be a closed ball in $\mathbb{R}^n$ and $f : B_n \to B_n$ be a continuous mapping. Then $f$ has a fixed point (so there is a point $x$ in $B_n$ such that $f(x) = x$).*

The proof is not provided, for a sketch of the proof, see the lecture.

**Fact: Any simplex is homeomorphic with a ball of the same (topological) dimension** (it follows from Minkowski's theorem, see the lecture).

**Definition 8.2** (Homeomorphism)**.** *Let $S, T \subset \mathbb{R}^n$ and let $f : S \to T$ be both injective and surjective. The mapping $f$ is said to be a* ***homeomorphism*** *if both $f$ and $f^{-1}$ are continuous. Then $S$ and $T$ are said to be* ***homeomorphic****.*

**Consequence 8.3** (Perron–Frobenius)**.** *Let $A = (a_{ij})$ be an $n \times n$ matrix and let all of its entries be positive, i.e., $a_{ij} > 0$ for all $i, j \le n$. Then $A$ has a positive eigenvalue and the corresponding eigenvector has all positive components, i.e., there exists $\lambda > 0$ and a vector $v = (v_1, v_2, \dots, v_n) \in \mathbb{R}^n$ such that $v_i > 0$ for every $i \le n$ and $Av = \lambda v$.*

*Proof.* We look for an eigenvector in the positive cone $\{(x_1, \dots, x_n) \in \mathbb{R}^n \mid \forall i : x_i \ge 0\}$. Without loss of generality, we may restrict attention to unit eigenvectors in the norm $\|(x_1, \dots, x_n)\|_1 = \sum_{i=1}^n |x_i|$ and to the set $K = \{(x_1, \dots, x_n) \in \mathbb{R}^n \mid \sum_{i=1}^n x_i = 1, \forall i : x_i \ge 0\}$. It is an $(n-1)$-dimensional simplex, thus the Brouwer's Fixed Point Theorem is applicable.
We define the mapping $f \colon K \to \mathbb{R}^n$ by

$$f(x) = \frac{Ax}{\|Ax\|_1}\,.$$

For $x = (x_1, \dots, x_n) \in K$, all entries of the vector $Ax$ are positive (as convex combinations of positive values) and so is the denominator

$$\|Ax\|_1 = \sum_{i=1}^n \sum_{j=1}^n a_{ij} x_j\,,$$

thus the mapping $f$ is well-defined and continuous. Moreover, it maps $K$ into $K$, thus it has a fixed point in $K$, say $v \in \mathbb{R}^n$. We obtain

$$f(v) = \frac{Av}{\|Av\|_1} = v\,,$$

i.e., $Av = \|Av\|_1 v$, thus $\|Av\|_1 > 0$ is an eigenvalue and $v$ is a corresponding eigenvector in $K$ with all entries non-negative. They cannot be zero because all entries of $Av$ and of $f(v) = v$ are positive. □