Topics in Applied Math: Logic and Foundations of Mathematics

Part 1. Equational theory

Kazuyuki Tanaka

BIMSA

September 19, 2025

Logic and Foundations

- **Part 1. Equational theory**
- **Part 2. First order theory**
- **Part 3. Basic Model theory**
- **Part 4. First order arithmetic and incompleteness theorems**
- **Part 5. Models of first-order arithmetic**
- **Part 6. Second order arithmetic and reverse mathematics**

Part 1. Schedule

- Sep. 17, (1) Formal systems of equations
- Sep. 19, (2) Birkhoff's theorems and Boolean algebras
- Sep. 24, (3) Boolean algebras (continued) and propositional logic
- Sep. 26, (4) Computable functions and general recursive functions

Recap: Syntax of Algebra

An **algebraic language** is a list of function symbols $\mathcal{L} = (\mathtt{f}_0, \mathtt{f}_1, \dots)$,
where each $\mathtt{f}_i$ stands for an m_i-ary function. Then, m_i is called the **arity** of $\mathtt{f}_i$ and the list $\rho = (m_0, m_1, \dots)$ is called the **similarity type** of $\mathcal{L}$.

The **terms** in an algebraic language $\mathcal{L}$ are defined inductively as follows.

1. Variables $x, y, z, \dots$ are terms.
2. If $t_0, \dots, t_{n-1}$ are terms, and $\mathtt{f}$ is an n-ary function symbol in $\mathcal{L}$, so is $\mathtt{f}(t_0, \dots, t_{n-1})$.

A 0-ary function symbol is also called a **constant**. A constant is a term by itself.

For two terms s, t, the symbol string $s = t$ is called an **equation**. A set of equations is called an **(equational) theory**.

Example: Group theory $\mathrm{G_p}$ is formalized in an algebraic language $\mathcal{L} = (\cdot,\ ^{-1}, \mathtt{e})$.
A symbol string such as $x^{-1} \cdot x$ is a term, and $x^{-1} \cdot x = e$ is an equation.
$\mathrm{G_p}$ can be regarded as a set $\{(x \cdot y) \cdot z = x \cdot (y \cdot z),\ \mathtt{e} \cdot x = x,\ x^{-1} \cdot x = \mathtt{e}\}$.

Recap: Deduction System

Definition 1.3

The **deduction system** of equational theory T consists of the following axioms and inference rules:

(1) The equations belonging to T are axioms.

(2) Equations of the form $t = t$ (refl) are axioms.

(3) The following four diagrams are inference rules

$$\frac{s = t}{t = s}\ (\mathrm{sym}), \qquad \frac{s = t \quad t = u}{s = u}\ (\mathrm{trans}),$$

$$\frac{s(x) = t(x)}{s(u) = t(u)}\ (\mathrm{sub}), \qquad \frac{s_1 = t_1 \ \ldots \ s_n = t_n}{\mathtt{f}(s_1, \ldots, s_n) = \mathtt{f}(t_1, \ldots, t_n)}\ (\mathrm{comp}).$$

each of which expresses that the lower formula holds when the upper holds. Here, s, t, s_i, t_i, $u (1 \leq i \leq n)$ are terms, x is a variable, and $\mathtt{f}$ is any function symbol in T.

Recap: Proof Trees

Definition 1.4

A **proof tree** (or **proof**) in equational theory T is defined inductively as follows:

1. An equation as an axiom is a proof tree by itself.
2. If P_i is a proof tree for $s_i = t_i$ $(1 \leq i \leq n)$, and

$$\frac{s_1 = t_1 \ \ldots \ s_n = t_n}{s = t}$$

is an inference rule, then

$$\frac{P_1 \ \ldots \ P_n}{s = t}$$

is a proof tree for $s = t$.

If $s = t$ has a proof tree in T, we write

$$T \vdash s = t,$$

where $\vdash$ is read as "turnstile".

Recap: Examples of proof trees

We work in equational theory $\mathrm{G_p}$ unless otherwise noted. We write xy in short for $x \cdot y$.

Example 1-1: A proof tree P_1 for $(x^{-1}x)x^{-1} = x^{-1}$

$$\dfrac{\dfrac{x^{-1}x = \mathsf{e} \quad x^{-1} = x^{-1}}{(x^{-1}x)x^{-1} = \mathsf{e}x^{-1}}\ (\mathrm{comp}) \qquad \dfrac{\mathsf{e}x = x}{\mathsf{e}x^{-1} = x^{-1}}\ (\mathrm{sub})}{(x^{-1}x)x^{-1} = x^{-1}}\ (\mathrm{trans}).$$

Example 1-2: A proof tree P_2 for $x^{-1}(xx^{-1}) = (x^{-1}x)x^{-1}$

$$\dfrac{\dfrac{(xy)z = x(yz)}{(x^{-1}x)x^{-1} = x^{-1}(xx^{-1})}\ (\mathrm{sub}) \times 3\mathrm{times}}{x^{-1}(xx^{-1}) = (x^{-1}x)x^{-1}}\ (\mathrm{sym})$$

Recap: Algebraic structures

Definition 2.2

- An **algebraic structure** $\mathfrak{A}$ in a language $\mathcal{L} = (\mathtt{f}_0, \mathtt{f}_1, \dots)$ (or simply **$\mathcal{L}$-algebra**) consists of a non-empty set A and a list of m_i-ary functions $\mathtt{f}_i^{\mathfrak{A}} : A^{m_i} \to A$, that is,

$$\mathfrak{A} = (A, \mathtt{f}_0^{\mathfrak{A}}, \mathtt{f}_1^{\mathfrak{A}}, \dots).$$

- We say that A is the **domain** or **universe** of $\mathfrak{A}$, denoted by $|\mathfrak{A}|$.
- For a 0-ary function symbol or constant c, $\mathtt{c}^{\mathfrak{A}}$ is an element of A.

- If an equation α holds in a structure $\mathfrak{M}$, we write $\mathfrak{M} \models \alpha$. If all the equations in theory T holds, we also write $\mathfrak{M} \models T$, and we say that $\mathfrak{M}$ is a **model** of T. Here $\models$ is read as "double turnstile".

- If an equation α holds for all models of a theory T, α is said to be a **consequence** of T or σ is **valid** in T, written as $T \models \sigma$

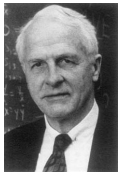
Birkhoff's theorems

- For an equational theory T, the following holds.

Birkhoff's completeness theorem (1935)

$$T \models s = t \Leftrightarrow T \vdash s = t.$$

- $T \models s = t \Leftarrow T \vdash s = t$ (the soundness of T) is easy. Let $\mathfrak{M}$ be any model of T. Then we can show by induction that all equations appearing in a proof tree for $T \vdash s = t$ holds in $\mathfrak{M}$. Especially the bottom $s = t$ holds in $\mathfrak{M}$.
- To show the contrapositive, we first assume $T \not\vdash s = t$, and construct a structure $\mathfrak{M}$ such that $\mathfrak{M} \models T$ and $\mathfrak{M} \not\models s = t$. Such a structure is obtained as the "free algebra" generated by the variables appearing in s, t.



Garrett Birkhoff

Variety theorem

A class $\mathcal{K}$ of structures is characterized by an equational theory $\Leftrightarrow$ $\mathcal{K}$ is closed under
- subalgebras,
- homomorphisms,
- Cartesian products.

Today's topics

1. Birkhoff's completeness theorem and variety theorem
2. Boolean Algebra

§3. Birkhoff's completeness theorem and variety theorem

- Today, we are going to prove Birkhoff's completeness theorem and equational class (variety) theorem.
- Fix an algebraic language $\mathcal{L}$. Unless otherwise stated, we only consider algebraic structures in this language.

Definition 3.1

An algebra $\mathfrak{B}$ is said to be a **subalgebra** of an algebra $\mathfrak{A}$ (denote $\mathfrak{B} \subseteq \mathfrak{A}$) if $|\mathfrak{B}| \subseteq |\mathfrak{A}|$ and for each function symbol $\mathtt{f} \in \mathcal{L}$ and $b_0, \ldots, b_{n-1} \in |\mathfrak{B}|$,

$$\mathtt{f}^{\mathfrak{A}}(b_0, \ldots, b_{n-1}) = \mathtt{f}^{\mathfrak{B}}(b_0, \ldots, b_{n-1}).$$

Definition 3.2

Let $\mathfrak{A}$ be an algebra and $X \subseteq |\mathfrak{A}|$. An algebra $\mathfrak{B}$ is the subalgebra **generated** by X if it is the smallest subalgebra of $\mathfrak{A}$ containing X.

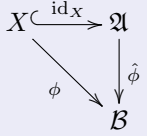
Example 7

Let $\mathfrak{A} = (\mathbb{Z}, +, -, 0)$ be a group and $X \subseteq \mathbb{Z}$. The elements of the subalgebra generated by X are the numbers expressed as $n_1x_1 + n_2x_2 + \cdots + n_kx_k\,(x_i \in X, n_i \in \mathbb{Z})$.
In particular, the subalgebra generated by $X = \{2\}$ is the group $(E, +, -, 0)$, where E is the set of even numbers.

Definition 3.3

Let $\mathcal{K}$ be a class of $\mathcal{L}$-algebras. Let $\mathfrak{A} \in \mathcal{K}$ and $X \subseteq |\mathfrak{A}|$.
We say that $\mathfrak{A}$ is a **free $\mathcal{K}$-algebra** generated by X if

1. $\mathfrak{A}$ is generated by X
2. Every map $\phi : X \to |\mathfrak{B}|$ with $\mathfrak{B} \in \mathcal{K}$ can be uniquely extended to a homomorphism $\hat{\phi} : \mathfrak{A} \to \mathfrak{B}$.



Example 8

Let $\mathcal{K}$ be a class of groups. The group $\mathfrak{A} = (\mathbb{Z}, +, -, 0)$ is the free $\mathcal{K}$-algebra (the free group) generated by $X = \{1\}$. Indeed, for a group $\mathfrak{G} = (\mathbf{G}, *, {}^{\sim}, e)$ and a homomorphism ϕ defined by

$$\phi(1) = g \in \mathbf{G},$$

then we have a unique homomorphism $\hat{\phi} : \mathfrak{A} \to \mathfrak{B}$ such that

$$\hat{\phi}(n) = g^n.$$

where g^n is obtained by multiplying g n-times with $*$ if $n > 0$, and multiplying $g^{\sim}$ n-times with $*$ if $n < 0$. When $n = 0$, it is defined as $g^n = e$.

Lemma 3.4

Let $\mathfrak{A}$ and $\mathfrak{B}$ are free $\mathcal{K}$-algebras generated by X and Y, respectively. If X and Y have the same cardinality, then we have $\mathfrak{A} \cong \mathfrak{B}$.

Proof. Since X and Y have the same cardinality, we have a bijection $\phi : X \to Y$. Since $\mathfrak{A}$, $\mathfrak{B}$ are free $\mathcal{L}$-algebras, maps ϕ, ϕ^{-1} are uniquely extended to homomorphisms,

$$\hat{\phi} : \mathfrak{A} \to \mathfrak{B}, \ \widehat{\phi^{-1}} : \mathfrak{B} \to \mathfrak{A}.$$

Then, $\widehat{\phi^{-1}}\hat{\phi}$ is a homomorphism from $\mathfrak{A}$ to $\mathfrak{A}$, which is an extension of $\mathrm{id}_X = \phi^{-1}\phi$. By the uniqueness of the extension, we have

$$\widehat{\phi^{-1}}\hat{\phi} = \mathrm{id}_A.$$

Similarly, we have

$$\hat{\phi}\widehat{\phi^{-1}} = \mathrm{id}_B.$$

Thus $\mathfrak{A} \cong \mathfrak{B}$. (see also Problem 5). □

Problem 7 (Homework # 2)

Let $\mathcal{L} = \{\mathtt{g}_1, \mathtt{g}_2, \mathtt{h}\}$. We define the set of equations E as follows.

$$E = \{\mathtt{h}(\mathtt{g}_1(x), \mathtt{g}_2(x)) = x,\ \mathtt{g}_1(\mathtt{h}(x, y)) = x,\ \mathtt{g}_2(\mathtt{h}(x, y)) = y\}$$

Let $\mathcal{K}$ be $\mathrm{Mod}(E)$, the class of models of E. Show that all finitely generated free $\mathcal{K}$-algebras are isomorphic.

Now, we will see a concrete construction of free algebras.

Let X be a set of variables. Let $\mathrm{Term}(X)$ be the set of $\mathcal{L}$-terms whose variables are all contained in X.

We define an $\mathcal{L}$-algebra $\mathcal{T}(X) = (\mathrm{Term}(X), \mathtt{f}_0^{\mathcal{T}(X)}, \mathtt{f}_1^{\mathcal{T}(X)}, \dots)$, called a **term algebra**, as follows: for each function symbol $\mathtt{f}$ in $\mathcal{L}$,

$$\mathtt{f}^{\mathcal{T}(X)}(t_0, \dots, t_{n-1}) = \mathtt{f}(t_0, \dots, t_{n-1}).$$

Here, the right-hand side $\mathtt{f}(t_0, \dots, t_{n-1})$ is a term as a symbol string.

Lemma 3.5

If a class of $\mathcal{L}$-algebra $\mathcal{K}$ contains $\mathcal{T}(X)$, then $\mathcal{T}(X)$ is a free $\mathcal{K}$-algebra generated by X.

Proof.

- Obviously, $\mathcal{T}(X)$ is an $\mathcal{L}$-algebra generated by X.
  So, we only need to check condition 2 of the definition of free algebra.
- Let $\mathfrak{B} \in \mathcal{K}$ and $\phi : X \to |\mathfrak{B}|$ be a morphism.
  Then we define a homomorphism $\hat{\phi} : \mathcal{T}(X) \to \mathfrak{B}$ inductively as follows:
  1. $\hat{\phi}(x) = \phi(x)$ for $x \in X$.
  2. $\hat{\phi}(\mathtt{f}(t_0, \ldots, t_{n-1})) = \mathtt{f}^{\mathfrak{B}}(\hat{\phi}(t_0), \ldots, \hat{\phi}(t_{n-1}))$.
- Then, it is clear that $\hat{\phi}$ is a homomorphism extending ϕ.
- In addition, since any homomorphism always satisfies the above equation, it is easy to see the uniqueness.

Definition 3.6

Let $\mathfrak{A}$ an algebra and $s, t \in \mathrm{Term}(X)$. We say that the equation $s = t$ **holds** in $\mathfrak{A}$ if for every homomorphism $\phi : \mathcal{T}(X) \to \mathfrak{A}$, we have $\phi(s) = \phi(t)$. Then we denote this by

$$\mathfrak{A} \models \mathbf{s = t}.$$

A homomorphism $\phi : \mathcal{T}(X) \to \mathfrak{A}$ can be viewed as an evaluation function of terms. The value of a term s is uniquely obtained from the values $\phi(\vec{x})$ of variables $\vec{x}$ in s.

Thus, $\mathfrak{A} \models s = t$ means that two terms s, t always have the same value on $\mathfrak{A}$ whichever elements of $|\mathfrak{A}|$ are assigned to the variables.

Definition 3.7

Let E be a set of equations on $\mathrm{Term}(X)$. If $\mathfrak{A} \models \alpha$ holds for all $\alpha \in E$, we write

$$\mathfrak{A} \models \mathbf{E}.$$

Moreover, we adopt the following notation:

$$\mathrm{Mod}(\mathbf{E}) = \{\mathfrak{A} \in \mathcal{K} : \mathfrak{A} \models E\},$$
$$\mathbf{E} \models \alpha \Leftrightarrow \text{ for all } \mathfrak{A} \in \mathrm{Mod}(E),\ \mathfrak{A} \models \alpha.$$

In the last lecture, we introduce a formal derivation system of equations.
If we can formally derive $s = t$ from the equational theory E, we denote this by

$$\mathbf{E} \vdash \mathbf{s} = \mathbf{t}$$

We are going to prove the following completeness theorem.

$$E \models s = t \Leftrightarrow E \vdash s = t.$$

Birkhoff's completeness theorem: $E \models s = t \Leftrightarrow E \vdash s = t$.

Proof. $\Leftarrow$ is easy to show.

- Suppose $E \vdash s = t$ and take a proof tree P for this.
- Let $\mathfrak{M}$ be a model of E. Since the equations at the top levels of the proof tree P are either the axiom of E or $t = t$, they naturally hold in $\mathfrak{M}$.
- If the premises (upper equations) of each inference rule in Definition 1.3 (3) hold in $\mathfrak{M}$, then clearly the conclusion (lower equation) also holds.
- Therefore, by induction, all equations in the proof tree of E hold in $\mathfrak{M}$.
- In particular, the bottom equation $s = t$ holds in $\mathfrak{M}$.

$\Rightarrow$ will be shown after defining the following relation $\equiv_E$ and proving some lemmas.

Definition 3.8

Let E be a set of equations on $\mathrm{Term}(X)$, and let $\equiv_E$ be a relation on $\mathrm{Term}(X)$ defined by

$$s \equiv_E t \Leftrightarrow E \vdash s = t.$$

Lemma 3.9

Let E be a set of equations on $\mathrm{Term}(X)$, and let $\equiv_E$ be the relation defined in Definition 3.8. Then, the following hold:

1. $\equiv_E$ is a congruence relation.
2. For any homomorphism $\phi : \mathcal{T}(X) \to \mathcal{T}(X)$, $\quad s \equiv_E t \Rightarrow \phi(s) \equiv_E \phi(t)$.
3. For any homomorphism $\phi : \mathcal{T}(X) \to \mathcal{T}(X)/\equiv_E$, there exists $\psi : \mathcal{T}(X) \to \mathcal{T}(X)$ s.t.

$$\phi = \pi_{\equiv_E} \circ \psi.$$

Note. A relation $\equiv$ that satisfies the lemma is called an **invariant congruence relation**.

Proof.

- (1) can be proved directly from the definition of derivation system.
- For (2), first note that the value of $\phi(s)$ is uniquely determined by the values of variables $\vec{x}$ in s (cf. the remark on P.16). For example, when $\phi(x) = u$ (where $x \in X$), $\phi(s(x)) = s(u)$. Thus, $s(x) = t(x) \Rightarrow s(u) = t(u)$ is nothing but the substitution rule.
- (3) is also obvious. For each $x \in X$, take an element t_x of the equivalence class $\phi(x)$, and define ψ as a homomorphism extending $x \mapsto t_x$.

Lemma 3.10

$\mathcal{T}(X)/\equiv_E$ is the free $\mathrm{Mod}(E)$-algebra generated by $\pi_{\equiv_E}(X)$.

Note. The lemma also holds for any invariant congruence $\equiv$.

Proof.

Claim 1. $\mathcal{T}(X)/\equiv_E \in \mathrm{Mod}(E)$

- To show the claim, let $s = t$ be any equation in E and $\phi : \mathcal{T}(X) \to \mathcal{T}(X)/\equiv_E$ be any homomorphism. Then, it is sufficient to show $\phi(s) = \phi(t)$.
- By Lemma 3.9 (3), there exists $\psi : \mathcal{T}(X) \to \mathcal{T}(X)$ such that $\phi = \pi_{\equiv_E} \circ \psi$.
- Since $s \equiv_E t$, again by Lemma 3.9 (2), $\psi(s) \equiv_E \psi(t)$.
- Then, from the definition of $\pi_{\equiv_E}$ and $\phi = \pi_{\equiv_E} \circ \psi$, we have $\phi(s) = \phi(t)$.

Also, since $\mathcal{T}(X)$ is generated by X, $\mathcal{T}(X)/\equiv_E$ is also generated by $\pi_{\equiv_E}(X)$.
This is because if $\pi_{\equiv_E}(X)$ generates a proper subalgebra of $\mathcal{T}(X)/\equiv_E$, then taking the inverse image of $\pi_{\equiv}$, X generates a proper subalgebra of $\mathcal{T}(X)$.

Proof.(continued)

Claim 2. $\mathcal{T}(X)/\equiv_E$ is a free $\mathrm{Mod}(E)$-algebra.

- We take any $\mathfrak{A} \models E$ and $\phi : X/\equiv_E \to |\mathfrak{A}|$.
- Let $\psi = \phi \circ \pi_{\equiv_E}$. Since $\mathcal{T}(X)$ is free, $\psi : X \to |\mathfrak{A}|$ can be extended to a homomorphism $\hat{\psi} : \mathcal{T}(X) \to \mathfrak{A}$.
- If $s \equiv_E t$, then since $\mathfrak{A} \models E$, we have $\mathfrak{A} \models s = t$ (i.e., $\hat{\psi}(s) = \hat{\psi}(t)$).
- By the homomorphism theorem, there exists $\hat{\phi} : \mathcal{T}(X)/\equiv_E \to \mathfrak{A}$ s.t. $\hat{\psi} = \hat{\phi} \circ \pi_{\equiv_E}$.
- Clearly $\hat{\phi}$ is a homomorphism extending ϕ, and the uniqueness of $\hat{\psi}$ implies the uniqueness of $\hat{\phi}$. □

We are now ready to prove

Theorem 3.11 (Birkhoff completeness theorem)

$$E \models \alpha \Leftrightarrow E \vdash \alpha.$$

Proof.

- $\Leftarrow$ has already been shown.
- To prove $\Rightarrow$, let $E \models s = t$.
  Since $\mathcal{T}(X)/\equiv_E \in \mathrm{Mod}(E)$, we have $\mathcal{T}(X)/\equiv_E \models s = t$.
  Then for any homomorphism $\phi : \mathcal{T}(X) \to \mathcal{T}(X)/\equiv_E$, we have $\phi(s) = \phi(t)$.
  In particular, letting $\phi = \pi_{\equiv_E}$, we have $s \equiv_E t$.
  Hence $E \vdash s = t$.

Birkhoff's variety theorem

Definition 3.12

If a set $\mathcal{K}$ of $\mathcal{L}$-algebras is said to be an **equational class** (or **variety**) if it is characterized by a set E of equations, that is

$$\mathcal{K} = \mathrm{Mod}(E).$$

Theorem 3.13 (Birkhoff's variety theorem)

$\mathcal{K}$ is an equational class $\Leftrightarrow$ $\mathcal{K}$ is closed under subalgebras, homomorphisms, and Cartesian products.

- Note that "closed under homomorphism" means that for any algebra $\mathfrak{A} \in \mathcal{K}$ and homomorphism $\phi : \mathfrak{A} \to \mathfrak{B}$ ($\mathfrak{B}$ does not necessarily belong to $\mathcal{K}$), the subalgebra of $\mathfrak{B}$ as the range of ϕ belongs to $\mathcal{K}$.
- "Closed under Cartesian product" means that the Cartesian product of algebras $\mathfrak{A}_i$ in $\mathcal{K}$ belongs again to $\mathcal{K}$. (General definitions will be given in part 3 of this course).

Proof.

To show $\Rightarrow$

- It is clear since an equation that holds in an algebraic structure also holds in its subalgebras and homomorphic images.
- The equality that holds for each $\mathfrak{A}_i$ also holds for the Cartesian product $\prod \mathfrak{A}_i$.

To show $\Leftarrow$

- Let $\mathcal{K}$ be closed under subalgebras, homomorphisms, and Cartesian products.
- Let X be an infinite set of variables. We define the following set of equations in $\mathrm{Term}(X)$ as follows:

$$E = \{s = t : \text{for any } \mathfrak{A} \in \mathcal{K}, \mathfrak{A} \models s = t\}.$$

- Our aim is to show $\mathrm{Mod}(E) = \mathcal{K}$.
- $\mathrm{Mod}(E) \supseteq \mathcal{K}$ is obvious. Hence, we will prove the following by two steps.

Claim. $\mathrm{Mod}(E) \subseteq \mathcal{K}$.

The idea of the poof: For any $\mathfrak{A} \in \mathrm{Mod}(E)$, it suffices to construct a homomorphism from $\mathfrak{C} \in \mathcal{K}$ onto $\mathfrak{A}$.

Suppose $\mathfrak{A} \in \mathrm{Mod}(E)$. Take a set Y of variables and a surjection $\chi : Y \to |\mathfrak{A}|$. This can be extended to an epimorphism (surjective homom.) $\hat{\chi} : \mathcal{T}(Y) \to \mathfrak{A}$.
By suitable replacement of variables, any equation in Y can be regarded as an equation in X. (Then it is plausible to consider $\mathcal{T}(Y)/E$. In fact, this will be a desired algebra $\mathfrak{C}$.)
Now, we are going to construct $\mathfrak{C}$ more rigorously so that we can see $\mathfrak{C} \in \mathcal{K}$.
For any $\mathfrak{B} \in \mathcal{K}$ and any homomorphism $\phi : \mathcal{T}(Y) \to \mathfrak{B}$, we define a congruence relation $\approx_\phi$ on $\mathcal{T}(Y)$ such that

$$s \approx_\phi t \Leftrightarrow \phi(s) = \phi(t)$$

By the homomorphism theorem, we have

$$\phi(\mathcal{T}(Y)) \simeq \mathcal{T}(Y)/\approx_\phi$$

Since the left-hand side is a subalgebra of $\mathfrak{B} \in \mathcal{K}$, by assumption we have $\mathcal{T}(Y)/\approx_\phi \in \mathcal{K}$.

We write $\mathcal{D}$ for the set of congruence relations on $\mathcal{T}(Y)$ expressed as $\approx_\phi$ for some homomorphism ϕ.

Since $\mathcal{K}$ is closed under Cartesian products, we have

$$\prod_{\approx \in \mathcal{D}} (\mathcal{T}(Y)/\approx) \in \mathcal{K}.$$

With a homom. $\pi_{\approx} : \mathcal{T}(Y) \to \mathcal{T}(Y)/\approx$ for each $\approx \in \mathcal{D}$, we can naturally define a homom.

$$\psi : \mathcal{T}(Y) \to \prod_{\approx \in \mathcal{D}} (\mathcal{T}(Y)/\approx).$$

Since $\mathcal{T}(Y)/\approx_\psi$ is isomorphic to a subalgebra of $\prod_{\approx \in \mathcal{D}} (\mathcal{T}(Y)/\approx)$, it also belongs to $\mathcal{K}$. Here, we have: $s \approx_\psi t \Leftrightarrow \psi(s) = \psi(t) \Leftrightarrow$ for each $\approx \in \mathcal{D}$ $s \approx t \Leftrightarrow$ for all ϕ $\phi(s) = \phi(t) \Leftrightarrow$ for all $\mathfrak{B} \in \mathcal{K}$, $\mathfrak{B} \models s = t \Leftrightarrow s = t \in E$ (with suitable replacement of variables). Thus, $\mathcal{T}(Y)/\approx_\psi$ is a desired algebra $\mathfrak{C}$.

Finally, by the corollary to the homomorphism theorem, we have an epimorphism

$$\hat{\chi}_{\approx_\psi} : \mathcal{T}(Y)/\approx_\psi \to \mathfrak{A}.$$

Since $\mathcal{K}$ is closed under homomorphism on $\mathcal{T}(Y)/\approx_\psi \in \mathcal{K}$, we have $\mathfrak{A} \in \mathcal{K}$. □

Non-equational class

- Since the axiom system of the group given in last lecture consists only of equations, the class of all groups is considered to form an equality class.
- However, groups can also be characterized in other ways. For example, we may define a group $(G, \bullet)$ as a pair of set and a binary operation on it, satisfying

$$(x \bullet y) \bullet z = x \bullet (y \bullet z) \text{ and there exists } w \text{ such that}$$
$$\text{for any } x \ (w \bullet x = x \text{ and } \exists y (y \bullet x = w))$$

- The group according to this definition is not an equational class. In fact, $(\mathbb{N}, +)$ is a subalgebra of the group $(\mathbb{Z}, +)$, but it is not a group.
- Abelian groups, rings, R-modules, lattices, Boolean algebras can be treated as equational classes with sufficient operators.
- But integral domains (commutative rings with no zero factors other than 0) and fields cannot be axiomatized only with equations, no matter how many operators are added. For example, the Cartesian product $\mathfrak{Z} \times \mathfrak{Z}$ of the integral domain $\mathfrak{Z} = (\mathbb{Z}, +, \bullet \cdot, 0, 1)$ is not an integral domain (note: $(0,1) \bullet (1,0) = (0,0)$).

A simple extension of equational theory

- Consider a language including relational symbols $\mathtt{R}_1, \mathtt{R}_2, \ldots$ besides function symbols.
- An expression of the form $s = t$ or $\mathtt{R}(t_1, \ldots, t_n)$ is called an **atomic formula**. We will give a deduction system that handles atomic formulas.

Definition 3.14

Let T be a set of atomic formulas. A deduction system for T consists of the following:
(1) Atomic formulas belonging to T and equations of the form $t = t$ are axioms.
(2) The following five diagrams are inference rules.

$$\frac{s = t}{t = s} \qquad \frac{s = t \quad t = u}{s = u}$$

$$\frac{s(x) = t(x)}{s(u) = t(u)} \qquad \frac{s_1 = t_1 \ \ldots \ s_n = t_n}{\mathtt{f}(s_1, \ldots, s_n) = \mathtt{f}(t_1, \ldots, t_n)}$$

$$\frac{s_1 = t_1 \ \ldots \ s_n = t_n \quad \mathtt{R}(s_1, \ldots, s_n)}{\mathtt{R}(t_1, \ldots, t_n)}$$

where, s, t, s_i, t_i, u are terms, x is a variable, $\mathtt{f}$ is a function symbol, and $\mathtt{R}$ is a relation symbol.

- A proof tree for this system is defined in the same way as for an equational theory, and if an atomic formula σ has a proof tree, we write $T \vdash \sigma$.
- The concept of models of T and $T \models \sigma$ can be naturally defined by extending structures to involve interpretations of relational symbols.
- For this extended theory, the same assertions as Birkhoff's completeness theorem and variety theorem hold.

§4. Boolean Algebras

- In the mid-19th century, British mathematician G. Boole attempted to clarify Aristotle's logic by treating logical relations algebraically.
- This was the beginning of Boolean algebra, but in modern times it is often subsumed under the more general concepts of "order" and "lattice" and treated as equational theory.

Definition 4.1

- If a binary relation $\leq$ on a nonempty set X satisfies **reflection** ($x \leq x$), **antisymmetry** (if $x \leq y$ and $y \leq x$, then $x = y$), as well as **transitivity** (if $x \leq y$ and $y \leq z$, then $x \leq z$) is satisfied, then $(X, \leq)$ is called a **(partial) order**.
- If an order $(X, \leq)$ additionally satisfies **comparability** ($x \leq y$ or $y \leq x$), then it is called a **total order** or **linear order**.

Example 9

$n|m$ on the natural numbers $\mathbb{N}^+$ excluding 0 represents the relation "n divides m" or "m is a multiple of n". Then, $(\mathbb{N}^+, |)$ is a partial order.

Let $(X, \leq)$ be a partial order. Suppose that for any a, $b \in X$, $\sup\{a, b\}$ and $\inf\{a, b\}$ exist in X, denoted by $a \vee b$ and $a \wedge b$, respectively.
Note: $\sup A$ is the minimum upper bound (supremum) of A, that is, the smallest value of b such that $a \leq b$ for all $a \in A$. Similarly, $\inf A$ is the maximum lower bound (infimum) of A.

Example 10

In the partial order $(\mathbb{N}^+, |)$, $\sup\{x, y\}$ is the greatest common divisor (gcd) of x and y, $\inf\{x, y\}$ is the least common multiple (lcm) of x and y.

Definition 4.2

Theory of **lattice** consists of the following eight equations. A model of lattice theory $(L, \vee, \wedge)$ is called a **lattice**.

L1 :	$x \vee x = x,\ x \wedge x = x$	[Idempotence]
L2 :	$x \vee y = y \vee x,\ x \wedge y = y \wedge x$	[Commutativity]
L3 :	$x \vee (y \vee z) = (x \vee y) \vee z,\ x \wedge (y \wedge z) = (x \wedge y) \wedge z$	[Associativity]
L4 :	$(x \vee y) \wedge x = x,\ (x \wedge y) \vee x = x$	[Absorption]

Example 11

$(\mathbb{N}^+, \mathrm{gcd}, \mathrm{lcm})$ is a lattice.

Conversely, for a given lattice $(L, \vee, \wedge)$, if a relation $x \leq y$ is defined as follows

$$x \leq y \Leftrightarrow x \wedge y = x (\Leftrightarrow x \vee y = y)$$

then it is a partial order on L. In this case, the lattice operations $\vee, \wedge$ are the same as $\sup$ and $\inf$ regarding this partial order.

Note. We show $x \wedge y = x \Leftrightarrow x \vee y = y$. $\Leftarrow$ can be derived by substituting $y := x \vee y$ to the left side and using lattice axioms L2 and L4. Similarly for $\Rightarrow$.

Now, Boolean algebra is defined as an equational theory as follows.

Definition 4.3

The theory of **Boolean algebra** (BA) is defined in language $\mathcal{L}_{\mathrm{B}} = \{\vee, \wedge, \neg, 0, 1\}$ with the following axioms.

1. All the lattice axioms and the following distributive law:

$$(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z), \quad (x \wedge y) \vee z = (x \vee z) \wedge (y \vee z).$$

2. $x \vee 0 = x, \quad x \vee (\neg x) = 1, \quad x \wedge 1 = x, \quad x \wedge (\neg x) = 0.$

A model of theory BA is called a **Boolean algebra**.

In the definition of Boolean algebra, (1) can be reduced to only L2 and distributive laws. This will be shown in problem 9 after the duality theorem.

Lemma 4.4 (Uniqueness of complement)

If $x \vee y = 1$ and $x \wedge y = 0$, then $y = \neg x$.

Proof. Assume $x \vee y = 1$ and $x \wedge y = 0$. Apply the distributive law at $=^{(*)}$ to obtain the desired equation as follows.

$$\begin{aligned} y &= y \vee 0 = y \vee (x \wedge \neg x) =^{(*)} (y \vee x) \wedge (y \vee \neg x) = (x \vee y) \wedge (y \vee \neg x) \\ &= 1 \wedge (y \vee \neg x) = (x \vee \neg x) \wedge (y \vee \neg x) =^{(*)} (x \wedge y) \vee \neg x = 0 \vee \neg x = \neg x. \end{aligned}$$

□

- **Remark**. In the formal deduction system of equations, "a premise σ implies a conclusion δ" means that if σ holds with any substitution for all variables then δ also holds with any substitution for all variables.
  In contrast, the lemma should be interpreted as "for all x, y, if ($x \vee y = 1$ and $x \wedge y = 0$, then $y = \neg x$)". To state it strictly, we need first-order logic for the argument.

Lemma 4.5 (Elimination of double negation)

$\neg\neg x = x$.

Proof. Apply the above lemma to $\neg x \vee x = 1$ and $\neg x \wedge x = 0$.

Theorem 4.6 (Duality theorem)

For an equation φ in $\mathcal{L}_{\mathrm{B}} = \{\vee, \wedge, \neg, 0, 1\}$, let $\tilde{\varphi}$ denote the equation (dual equation) obtained from φ by interchanging $\vee$ with $\wedge$ and 0 with 1. Then

$$\mathrm{BA} \vdash \varphi \Leftrightarrow \mathrm{BA} \vdash \tilde{\varphi}.$$

Proof. The dual formula $\tilde{\sigma}$ for each axiom σ of BA is also an axiom. Therefore, for a proof tree of theorem φ in BA, if we replace all expressions in the tree with dual expressions, we obtain a proof tree of $\tilde{\varphi}$. □

Problem 9, Homework # 3

In Defition 4.3, reduce (1) to only the commutative law and distributive law, and then prove the Idempotent, absorption law, and associative law.

Theorem 4.7 (De Morgan's law)

In BA, $\neg(x \vee y) = \neg x \wedge \neg y$, $\neg(x \wedge y) = \neg x \vee \neg y$ holds.

Proof They can be deduced from the following equations together with the uniqueness of the complement.

$$\begin{aligned}
(x \vee y) \vee (\neg x \wedge \neg y) &= [(x \vee y) \vee \neg x] \wedge [(x \vee y) \vee \neg y] \\
&= [(x \vee \neg x) \vee y] \wedge [x \vee (y \vee \neg y)] \\
&= (1 \vee y) \wedge (x \vee 1) = 1 \wedge 1 = 1. \\
(x \vee y) \wedge (\neg x \wedge \neg y) &= [x \wedge (\neg x \wedge \neg y)] \vee [y \wedge (\neg x \wedge \neg y] \\
&= [(x \wedge \neg x) \wedge \neg y] \vee [\neg x \wedge (y \wedge \neg y)] \\
&= (0 \wedge \neg y) \vee (\neg x \wedge 0) = 0 \vee 0 = 0.
\end{aligned}$$

Therefore, $\neg(x \vee y) = \neg x \wedge \neg y$. Also, $\neg(x \wedge y) = \neg x \vee \neg y$ follows from the duality theorem.

Example 12

Let X be any set and $\mathcal{P}(X)$ be the power set (all subsets) of X. Now, if $Y^c = X - Y$ for $Y \subseteq X$, then the power set algebra $\mathfrak{P}(X) = (\mathcal{P}(X), \cup, \cap, ^c, \varnothing, X)$ is a Boolean algebra. In particular, when X is a singleton $\{a\}$, $\mathcal{P}(X)$ is a trivial Boolean algebra, and isomorphic to $2 = (\{0, 1\}, \vee, \wedge, 0, 1)$.

Conversely, any finite Boolean algebra is isomorphic to a power set algebra, and more generally the following theorem holds. (The proof will be given in part 3)

Theorem 4.8 (Stone's representation theorem)

For any Boolean algebra $\mathfrak{B}$, there exists a set X, $\mathfrak{B}$ can be embedded in its power set algebra $\mathfrak{P}(X)$. Especially, if $\mathfrak{B}$ is finite, it is isomorphic to $\mathfrak{P}(X)$.

- By a Boolean expression $\varphi(x_1, x_2, \ldots, x_n)$, we denote a term of $\mathcal{L}_{\mathrm{B}}$ with only variables $\{x_1, x_2, \ldots, x_n\}$.
- A Boolean expression $\varphi(x_1, x_2, \ldots, x_n)$ defines a function $f_\varphi : \{0,1\}^n \to \{0,1\}$. Such functions are called **Boolean functions**.
- We want to show that any function $f : \{0,1\}^n \to \{0,1\}$ can be expressed as f_φ with some Boolean expression φ. Moreover, if two Boolean expressions φ and ψ define the same function $f_\varphi = f_\psi$, then $\varphi = \psi$ is a theorem of BA. These can be obtained from the normal form theorem for Boolean expressions.

Shannon's expansion (decomposition) theorem

Lemma 4.9 (Shannon's theorem)

$\mathrm{BA} \vdash \varphi(x_1, x_2, \ldots, x_n) \leftrightarrow (\varphi(0, x_2, \ldots, x_n) \wedge \neg x_1) \vee (\varphi(1, x_2, \ldots, x_n) \wedge x_1)$ [1].

Proof.

- Given a Boolean expression, we use de Morgan's laws and double negation elimination to push the negation symbols innermost so that each negation appears just before an variable. A Boolean expression in such a form is called a **negation normal form**.
- So, we may assume that a Boolean expression φ is in the negation normal form.
- Now, we prove the assertion of the lemma by induction on the number m of operators $\vee$ and $\wedge$ included in φ.

[1] This was already proved by Boole, but it is known as "Shannon's expansion (decomposition) theorem."

(i) In the case of $m = 0$.
φ is a variable or the negation of a variable.

- If φ is x_1, $(\varphi(0) \wedge \neg x_1) \vee (\varphi(1) \wedge x_1) = (0 \wedge \neg x_1) \vee (1 \wedge x_1) = x_1$.
- If φ is $\neg x_1$, $(\varphi(0) \wedge \neg x_1) \vee (\varphi(1) \wedge x_1) = (1 \wedge \neg x_1) \vee (0 \wedge x_1) = \neg x_1$.
- If φ is x_i or $\neg x_i (i \neq 1)$, no matter what is assigned to x_1, it is the same as φ, so $(\varphi \wedge \neg x_1) \vee (\varphi \wedge x_1) = \varphi \wedge (\neg x_1 \vee x_1) = \varphi$.

(ii) In the case of $m > 0$.
Let φ be $\varphi_1 \vee \varphi_2$, and by induction hypothesis

$$\varphi_i = (\varphi_i(0) \wedge \neg x_1) \vee (\varphi_i(1) \wedge x_1) \ (i = 1, 2).$$

Then,

$$\begin{aligned} \varphi_1 \vee \varphi_2 &= [(\varphi_1(0) \wedge \neg x_1) \vee (\varphi_1(1) \wedge x_1)] \vee [(\varphi_2(0) \wedge \neg x_1) \vee (\varphi_2(1) \wedge x_1)] \\ &= [(\varphi_1(0) \vee \varphi_2(0)) \wedge \neg x_1] \vee [(\varphi_1(1) \vee \varphi_2(1)) \wedge x_1] \\ &= (\varphi(0) \wedge \neg x_1) \vee (\varphi(1) \wedge x_1). \end{aligned}$$

Similarly we can prove for $\varphi \equiv \varphi_1 \wedge \varphi_2$.

Notation. $\varphi_1 \vee \varphi_2 \vee \cdots \vee \varphi_n$ is also written as $\bigvee_{i=1,\ldots,n} \varphi_i$.
Furthermore, we set $x^b = x$ if $b = 1$ and $x^b = \neg x$ if $b = 0$.

Theorem 4.10 (Disjunctive normal form)

For a Boolean expression $\varphi(x_1, x_2, \ldots, x_n)$,

$$\begin{aligned} \mathrm{BA} \vdash \varphi(x_1, x_2, \ldots, x_n) &= \bigvee_{b_1,\ldots,b_n=0,1} \varphi(b_1, b_2, \ldots, b_n) \wedge x_1^{b_1} \wedge x_2^{b_2} \wedge \cdots \wedge x_n^{b_n} \\ &= \bigvee_{f_\varphi(b_1,\ldots,b_n)=1} x_1^{b_1} \wedge x_2^{b_2} \wedge \cdots \wedge x_n^{b_n}. \end{aligned}$$

If there is no $b_1, \ldots, b_n$ such that $f_\varphi(b_1, \ldots, b_n) = 1$, then we set the right-hand side $= 0$.

Proof By Shannon's theorem, we can prove this by induction on the number of variables. □

The rightmost expression in the last theorem is called the **disjunctive normal form** of φ. In addition, if we rewrite $\neg\sigma$ into the disjunctive normal form, then we can easily obtain a conjunctive normal form of σ by de Morgan's laws and double negation elimination.

Corollary 4.11

For any function $f : \{0,1\}^n \to \{0,1\}$, there exists a Boolean expression φ such that $f = f_\varphi$.

Proof. Obvious from the theorem □

Corollary 4.12

If two Boolean expressions φ and ψ define the same function $f_\varphi = f_\psi$, then $\mathrm{BA} \vdash \varphi = \psi$.

Proof. In the theorem, both disjunctive normal forms are the same. □

Corollary 4.13

The number of equivalence classes of Boolean expressions of n variables is 2^{2^n}.

Proof. The number of equivalence classes of a Boolean expression with n variable is equal to the number of the function $f : \{0,1\}^n \to \{0,1\}$, that is, 2^{2^n}. □

Finally, we introduce Boolean rings, which are essentially equivalent to Boolean algebras.

Definition 4.14

The theory CR of **commutative ring** consists of the following axioms, in the language $\mathcal{L}_{\mathrm{R}} = \{+, \cdot, -, 0, 1\}$.

$$x + 0 = x, \quad x + y = y + x, \quad x + (y + z) = (x + y) + z, \quad x + (-x) = 0,$$
$$x \cdot 1 = x, \quad x \cdot y = y \cdot x, \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z, \quad x \cdot (y + z) = (x \cdot y) + (x \cdot z).$$

A model of the theory CR is called a **commutative ring**.

In BA and CR, we usually assume $0 \neq 1$ as an axiom. But since we want to treat them as an equational theory, we treat a structure where $0 = 1$ as a special case.

Example 13

The structure of integers $\mathfrak{Z} = (\mathbb{Z}, +, \cdot, -, 0, 1)$ is a commutative ring.

Example 14

For a commutative ring $\mathfrak{A}$, the set of polynomials with variables $X_1, X_2, \ldots, X_n$ and coefficients in A also becomes a commutative ring, denote $\mathfrak{A}[X_1, X_2, \ldots, X_n]$.

Definition 4.15

The theory BR of **Boolean rings** is the theory CR plus the following axiom.

$$x^2 = x.$$

A model of the theory BR is called a **Boolean ring**.

We first show that $x + x = 0$ holds in BR.

$$x + x = (x + x)^2 = x^2 + x^2 + x^2 + x^2 = x + x + x + x.$$

By subtracting $x + x$ from both sides, we get $x + x = 0$. So, $+$ in a Boolean ring has a different property from $+$ in a Boolean algebra. However, both are mutually translatable as shown in the next theorem.

Theorem 4.16 (Stone's theorem)

(1) For any Boolean algebra $\mathfrak{B} = (B, \vee, \wedge, \neg, 0, 1)$, we set

$$x + y = (x \wedge (\neg y)) \vee ((\neg x) \wedge y), \quad x \bullet y = x \wedge y, \quad -x = x.$$

Then, $\mathfrak{B}^\circ = (B, +, \bullet, -, 0, 1)$ is a Boolean ring.

(2) For any Boolean ring $\mathfrak{R} = (R, +, \bullet, -, 0, 1)$, we set

$$x \vee y = x + y + x \bullet y, \quad x \wedge y = x \bullet y, \quad \neg x = 1 + x$$

and then $\mathfrak{R}^\circ = (R, \vee, \wedge, \neg, 0, 1)$ is a Boolean algebra.

(3) By (1) and (2), for a Boolean algebra $\mathfrak{B}$ and a Boolean ring $\mathfrak{R}$,

$$\mathfrak{B}^{\circ\circ} = \mathfrak{B},$$

$$\mathfrak{R}^{\circ\circ} = \mathfrak{R}.$$

Thank you for your attention!