Topics in Applied Math: Logic and Foundations of Mathematics

Part 1. Equational theory

Kazuyuki Tanaka

BIMSA

September 17, 2025

Outline of the Course

1. This is an introductory graduate-level course in **mathematical logic**, emphasizing on **foundations of mathematic**.
2. Each week, there are two lectures, on Wednesday and Friday. During the lectures, I will assign some homework problems, and collect homeworks at the beginning of the 4n+1-th lectures. At the end of the course, instead of homework due the 25th lecture, I will give a set of little harder problems for the final report.
3. TA (Mr. Kai Duo) is in charge of our WeChat group. He will handle homeworks as well as questions and comments via WeChat.
4. Lecture slides will be uploaded somewhere later.

Education

- ⋆ Institute of Science Tokyo (Tokyo Inst Tech)
  Information Science, Bachelor and Master
- ⋆ University of California, Berkeley
  Mathematics, Ph.D.
  (Advisor: Leo Harrington)

Teaching Jobs

- ⋆ Assistant Prof., Inst. of Science Tokyo
  (visiting Penn State)
- ⋆ Associate Prof., Tohoku Univ.
  (visiting Oxford)
- ⋆ 1997 $\sim$ 2022, Professor, Tohoku University.
  I supervised 15 doctoral/50 master students.
- ⋆ 2022 $\sim$ now, Professor, BIMSA.

Introducing myself

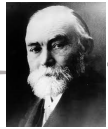
Speciality

Mathematical logic, especially definabilty and computability theory. Among others, I have contributed to second-order arithmetic and reverse mathematics.
See https://sendailogic.com/tanaka/.


Boole


De Morgan

Mathematics of logic


Frege

Predicate logic

Logic of mathematics


Bolzano


Cantor

Set theory, theory of real numbers


Dedekind


Peano

Theory of natural numbers

Second half of the 19th century

Foundations of mathematics


Hilbert

Type theory


Russell

Beginning of the 20th century


Hilbert

Foundations of mathematics


Gödel


Turing

Recursion theory / Computability theory

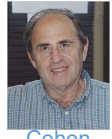

Gentzen

Proof theory


Tarski

Model theory


Gödel


Cohen

Set theory

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) Free algebras and Birkhoff's theorem
- Sep. 24, (3) Boolean algebras
- Sep. 26, (4) Computable functions and general recursive functions

Today's topics

1. Equational Theory
2. Algebraic structures

§1. Introduction to Equation Theory

- In part 1, we study mathematical theories that are characterized by axioms in the form of equations ($=$).
- The class of models of such a theory has some intriguing properties (e.g., it is closed under the Cartesian product).
- The Birkhoff completeness theorem and the equational class theorems are two major results, which will also be extended to more general theories involving logical symbols in the following parts of this course.
- In this part, we also discuss Boolean algebra as a typical equational theory. At last, we introduce general recursive functions as another application of equational theory.

- To begin with, we look at an equational theory of groups in order to observe how a mathematician proves. Among various ways to describe the theory of groups, we adopt the following equational axioms.

Definition 1.1

Group theory $\mathrm{G_p}$ consists of the following three axioms.

$$\begin{array}{lrcll} \mathrm{G1}: & (x \cdot y) \cdot z & = & x \cdot (y \cdot z) & \text{(associativity)} \\ \mathrm{G2}: & \mathsf{e} \cdot x & = & x & \text{(left identity)} \\ \mathrm{G3}: & x^{-1} \cdot x & = & \mathsf{e} & \text{(left inverse)} \end{array}$$

where x, y and z are variables, e is a constant, and $^{-1}$ represents a unary function.

- Consider a structure $\mathfrak{G} = (\mathbf{G}, *, \tilde{}, e)$, where $\mathbf{G}$ is a non-empty set, $*$ a binary function, $\tilde{}$ a unary function on $\mathbf{G}$, and e an element of $\mathbf{G}$.
- $\mathfrak{G}$ is called a **model** of $\mathrm{G_p}$, or simply **group**, if by interpreting the symbols $\cdot$, $^{-1}$, e of $\mathrm{G_p}$ as $*$, $\tilde{}$, e on $\mathbf{G}$, the three equalities hold for any assignment of an element of $\mathbf{G}$ to each variable.

- In general, when a sentence σ holds in a structure $\mathfrak{M}$ (in other words, σ is true in $\mathfrak{M}$), we write $\mathfrak{M} \models \sigma$.
- A set T of sentences (logical formulas or axioms) is called a **theory**. If all the sentences $\sigma \in T$ hold in $\mathfrak{M}$, we say that $\mathfrak{M}$ is a **model** of T or T has a model $\mathfrak{M}$, denote $\mathfrak{M} \models T$. Here $\models$ is read as "double turnstile".
- If a sentence σ holds for all models of a theory T, σ is called a **consequence** of T or σ is **valid** in T, written as $T \models \sigma$
- We take a look at the following theorem and proof, as an example of an argument for a consequence of group theory $\mathrm{G_p}$.

Theorem 1.2

$\mathrm{G_p} \models x \cdot x^{-1} = \mathsf{e}$ [right inverse]

Proof.
Let $\mathfrak{G} = (\mathbf{G}, *, {}^{\sim}, e)$ be an arbitrary group. Pick any element a of $\mathbf{G}$. We claim $a * a^{\sim} = e$.
First, we show $a = e$ if $a * a = a$. Multiply by $a^{\sim}$, on both sides of $a * a = a$, we have $a^{\sim} * (a * a) = a^{\sim} * a$. The left-hand side of this is

$$\begin{array}{rcll} a^{\sim} * (a * a) & = & (a^{\sim} * a) * a & \text{(by G1)} \\ & = & e * a & \text{(by G3)} \\ & = & a & \text{(by G2)} \end{array}$$

Since the right-hand side $a^{\sim} * a$ is equal to e from G3, we obtain $a = e$.
Now, we have

$$\begin{array}{rcll} (a * a^{\sim}) * (a * a^{\sim}) & = & a * (a^{\sim} * (a * a^{\sim})) & \text{(by G1)} \\ & = & a * ((a^{\sim} * a) * a^{\sim}) & \text{(by G1)} \\ & = & a * (e * a^{\sim}) & \text{(by G3)} \\ & = & a * a^{\sim} & \text{(by G2)} \end{array}$$

Hence, $a * a^{\sim} = e$. □

Definition 1 (revisited)

Group theory $\mathrm{G_p}$ consists of the following three axioms.

$$\begin{array}{lrcl} \mathsf{G1}: & (x \cdot y) \cdot z & = & x \cdot (y \cdot z) \\ \mathsf{G2}: & \mathsf{e} \cdot x & = & x \\ \mathsf{G3}: & x^{-1} \cdot x & = & \mathsf{e} \end{array}$$

Problem 1

$\mathrm{G_p} \models x \cdot \mathsf{e} = x$ [right identity].

Problem 2

Let $\mathrm{G'_p}$ be a theory obtained by replacing G3 [left inverse] in $\mathrm{G_p}$ with

$$x \cdot x^{-1} = \mathsf{e} \quad \text{[right inverse]}.$$

Prove that G3 does not hold in $\mathrm{G'_p}$, i.e.,

$$\mathrm{G'_p} \not\models x^{-1} \cdot x = \mathsf{e}.$$

- The proof of Theorem 1.2 in Page 10 is an ordinary argument in mathematics.
- However, if you think twice, it is not at all obvious to take an arbitrary group $\mathbf{G}$ and select an arbitrary element a to discuss it.
- Can we say that the claim is true if there exists a right inverse in the groups one can imagine or people have found until today?
- However, we should notice that once we have fixed a group $\mathbf{G}$ and its arbitrary element a, the rest is a simple transformation of formulas.
- The transformation is obtained by starting from the axioms of $\mathrm{G_p}$ and applying the rules of equality.
- Indeed, it doesn't really matter which group you would choose to handle. Any structure that satisfies the axioms will work out even if you cannot imagine it.

Formal system of an equational theory

- Let us now introduce a formal system of equations. We will give the general definition of a language, a term, etc. later.
- Here, we may consider a **language** as a set of mathematical symbols such as $\cdot$, $^{-1}$, and e in group theory.
- A string consisting of these symbols and variables with parentheses, is called a **term** if it is properly combined to denote an element of a given structure.
- Then, for two terms s, t, the symbol string $s = t$ is called an **equation**.
- A set of equations is called a **theory**.
- A deductive system, which derives the consequences of a theory T, is defined in the next page.

Definition 1.3

Let T be a theory of equations. An **equational theory** of T consists of the following axioms and (inference) rules.

- (1) Any equation in T is an axiom. (2) $t = t$ is a reflexivity axiom for each term t.
- $\dfrac{s = t}{t = s}\ (\mathrm{sym})$ expresses a symmetricity rule.
- $\dfrac{s = t \quad t = u}{s = u}\ (\mathrm{trans})$ expresses a transitivity rule.
- $\dfrac{s(x) = t(x)}{s(u) = t(u)}\ (\mathrm{sub})$ is a substitution rule for replacing all occurrences of variable x with a term u.
- $\dfrac{s_1 = t_1 \ \ldots \ s_n = t_n}{\mathtt{f}(s_1, \ldots, s_n) = \mathtt{f}(t_1, \ldots, t_n)}\ (\mathrm{comp})$ guarantees that equality is preserved by function composition. E.g, in group theory, $s_1 = t_1, s_2 = t_2 \Rightarrow s_1 \cdot s_2 = t_1 \cdot t_2$, and $s = t \Rightarrow s^{-\mathbf{1}} = t^{-\mathbf{1}}$.

Definition 1.4

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

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

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

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".

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 $(x^{-1}x)x^{-1} = x^{-1}$

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

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

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

Example 1-3: A proof tree for $(xx^{-1})(xx^{-1}) = (xx^{-1})$

Let P_3 be a proof tree for $(xx^{-1})(xx^{-1}) = x(x^{-1}(xx^{-1}))$ (easily constructed by G1). The following is a proof tree for $(xx^{-1})(xx^{-1}) = (xx^{-1})$.

$$\dfrac{P_3 \quad \dfrac{x = x \quad \dfrac{P_2 \quad P_1}{x^{-1}(xx^{-1}) = x^{-1}}\,(\text{trans})}{x(x^{-1}(xx^{-1})) = xx^{-1}}\,(\text{comp})}{(xx^{-1})(xx^{-1}) = (xx^{-1})}\,(\text{trans})$$

Problem 3

Using the examples above, construct a proof tree for $\mathrm{G_p} \vdash xx^{-1} = \mathsf{e}$.

Problem 4

Construct a proof tree for $\mathrm{G_p} \vdash x\mathsf{e} = x$.

Homework Problem 1

Consider an equation system consisting of binary operator symbol $\cdot$ and c, d, e as constants.

1. For a theory $T = \{c \cdot x = x, x \cdot d = x\}$, construct a proof tree for $T \vdash c = d$.
2. For a theory $T' = \{c \cdot x = x, e \cdot x = x, x \cdot d = x\}$, construct a proof tree for $T' \vdash c = e$.
3. Prove that $c = e$ does not hold in some model of $T'' = \{(x \cdot y) \cdot z = x \cdot (y \cdot z), c \cdot x = x, e \cdot x = x\}$.

Birkhoff's completeness theorem

- For an equational theory T, the following relationship holds.

Birkhoff's completeness theorem (1935)

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

Garrett Birkhoff

In other words, "$s = t$ is a consequece of theory T ($T \models s = t$)" can be completely captured by a finite diagram of a proof tree for $s = t$.

- It can be regarded as a special case of **Gödel's completeness theorem** (1930), which asserts that mathematical arguments in first-order logic can be completely formalized.

Kurt Gödel

Birkhoff's completeness theorem

- We will prove Birkhoff's completeness theorem next time, but we here explain the brief idea of the proof.
- $T \models s = t \Leftarrow T \vdash s = t$ (the soundness of T) is easier. 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 $\mathfrak{M}$.
- However, $\Rightarrow$ is not easy. To show the contrapositive, we first assume $T \not\vdash s = t$, and construct a structure $\mathfrak{M}$ such that

$$\mathfrak{M} \models T \text{ and } \mathfrak{M} \not\models s = t.$$

Such a structure is obtained as the "free algebra" generated by the variables appearing in s, t. Before introducing it, we first review the basic concepts of general algebra.

§2. Algebraic languages and structures

Definition 2.1

An **algebraic language** is a list of function symbols

$$\mathcal{L} = (\mathtt{f}_0, \mathtt{f}_1, \dots),$$

where each $\mathtt{f}_i$ is associated with a natural number m_i, called its **arity**, that is, $\mathtt{f}_i$ stands for an m_i-ary function. A 0-ary function symbol is also regarded as a **constant**.
$\rho = (m_0, m_1, \dots)$ is called the **similarity type** of $\mathcal{L}$.

Note that there may be infinitely many (possibly uncountably many) symbols in an algebraic language $\mathcal{L}$.

Algebraic structures

Definition 2.2

- An **algebraic structure** $\mathfrak{A}$ in a language $\mathcal{L} = (\mathtt{f}_0, \mathtt{f}_1, \dots)$ (or simply an **$\mathcal{L}$-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.

Example

- A group $\mathfrak{G}$ is an algebraic structure $(\mathbf{G}, *, {}^{\sim}, e)$ in an algebraic language $\mathcal{L} = (\cdot, {}^{-1}, \mathtt{e})$.
- Then $\cdot^{\mathfrak{G}}$ is a binary function $*$, $({}^{-1})^{\mathfrak{G}}$ is a unary function ${}^{\sim}$, and $\mathtt{e}^{\mathfrak{G}}$ is a 0-ary function e. Therefore, the similarity type of $\mathcal{L}$ is $(2, 1, 0)$.

Terms

Definition 2.3

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

1. Variables $x, y, z, \ldots$ are terms.
2. If $t_0, \ldots, t_{n-1}$ are terms and $\mathtt{f}$ is an n-ary fuction symbol in $\mathcal{L}$, then $\mathtt{f}(t_0, \ldots, t_{n-1})$ is also a term.

- In particular, constants (0-ary function symbols) are terms.
- A term t including some variables (e.g., x, y) are often written as $t(x, y)$.
- The term obtained from a term $t(x)$ by replacing all variables x appearing in it with a term s is expressed as $t(s)$.
- By convention, a binary function $\mathtt{f}(x, y)$ is also expressed as $x\mathtt{f}y$, e.g., $+(x, y)$ is written as $x + y$.

Homomorphisms and isomorphisms

We fix an algebraic language $\mathcal{L}$. We will only consider algebraic structures in this language unless otherwise stated.

Definition 2.4

Let $\mathfrak{A}$, $\mathfrak{B}$ be $\mathcal{L}$-algebras. A morphism $\phi : \mathfrak{A} \to \mathfrak{B}$ is a **homomorphism** if for each n-ary function symbol $\mathtt{f}$ in $\mathcal{L}$, and for any $a_0, \ldots, a_{n-1} \in |\mathfrak{A}|$,

$$\phi(\mathtt{f}^{\mathfrak{A}}(a_0, \ldots, a_{n-1})) = \mathtt{f}^{\mathfrak{B}}(\phi(a_0), \ldots, \phi(a_{n-1})).$$

Moreover, ϕ is said to be an **isomorphism** if ϕ is bijective.
If there exists an isomorphism $\phi : \mathfrak{A} \to \mathfrak{B}$, then we say that $\mathfrak{A}$ and $\mathfrak{B}$ are **isomorphic**, denoted by

$$\mathfrak{A} \cong \mathfrak{B}.$$

Example 3

Consider a group $\mathfrak{A} = (\mathbb{Z}, +, -, 0)$ and a group $\mathfrak{B} = (\mathbb{R}^+, \cdot, 1/x, 1)$ where $\mathbb{R}^+ = \{r \in \mathbb{R} \mid r > 0\}$. Then there is a homomorphism $\phi : \mathfrak{A} \to \mathfrak{B}$ defined by

$$\phi(n) = 2^n.$$

In particular, we have $\phi(m + n) = \phi(m) \cdot \phi(n)$.
Furthermore, $\mathfrak{M} = (M, \cdot, 1/x, 1)$ with $M = \{2^n : n \in \mathbb{Z}\}$ is also a group, and we have $\mathfrak{A} \cong \mathfrak{M}$.

Problem 5

Prove that $\mathfrak{A}$ and $\mathfrak{B}$ are isomorphic iff there exist two homomorphisms $\phi : \mathfrak{A} \to \mathfrak{B}$ and $\psi : \mathfrak{B} \to \mathfrak{A}$ such that their composite functions $\psi \circ \phi$ and $\phi \circ \psi$ are both identity maps (id_A and id_B).

Definition 2.5

Let $\mathfrak{A}$ be an algebra and $\equiv$ be a binary relation on $|\mathfrak{A}|$. Then we say that $\equiv$ is a **congruence relation** on $\mathfrak{A}$ if $\equiv$ is an equivalence relation on $|A|$ (i.e., satisfying reflexivity, transitivity, and symmetricity) and for every functional symbol $\mathtt{f} \in \mathcal{L}$, and for any $a_0, \cdots, a_{n-1}, b_0, \cdots, b_{n-1} \in A$, we have

$$a_0 \equiv b_0, \ldots, a_{n-1} \equiv b_{n-1} \Rightarrow \mathtt{f}^{\mathfrak{A}}(a_0, \ldots, a_{n-1}) \equiv \mathtt{f}^{\mathfrak{A}}(b_0, \ldots, b_{n-1}).$$

Example 4

Let $\mathfrak{Z} = (\mathbb{Z}, +, \cdot, -, 0, 1)$ be a ring of integers. We define $m \equiv_3 n \Leftrightarrow$ "$m - n$ is a multiple of 3". To prove $\equiv_3$ is a congruence relation, we will show that if $m \equiv_3 n$ and $m' \equiv_3 n'$, then $m + m' \equiv_3 n + n'$ and $m \cdot m' \equiv_3 n \cdot n'$ and $-m \equiv_3 -n$.

Problem 6

Let $\mathfrak{H}$ be a normal subgroup of the group $\mathfrak{G}$ (for any $g \in |\mathfrak{G}|$ and $h \in |\mathfrak{H}|$, $ghg^{\sim} \in |\mathfrak{H}|$). Let $g_1 \equiv_H g_2 \Leftrightarrow g_1 g_2{}^{\sim} \in |\mathfrak{H}|$. Show that $\equiv_H$ is a congruence relation.

- Given an equivalence relation $\equiv$ on a set A and an element $a \in A$, a subset of A defined as
$$\{x \in A : x \equiv a\}$$
is called the **equivalent class** or **residue class** of a, denoted by $[a]$. A class of all equivalence classes is denoted by $A/\equiv$.

- Then, we can make an algebra $\mathfrak{A}/\equiv$ with domain $|\mathfrak{A}|/\equiv$ when $\equiv$ is a congruence relation on $\mathfrak{A}$.

Definition 2.6

Give a congruence relation $\equiv$ on an $\mathcal{L}$-algebra $\mathfrak{A}$. Each n-ary function symbol $\mathtt{f}$ in $\mathcal{L}$ is interpretated on $|\mathfrak{A}|/\equiv$ as follows: for all $a_0, \ldots, a_{n-1} \in |\mathfrak{A}|$,

$$\mathtt{f}^{\mathfrak{A}/\equiv}([a_0], \ldots, [a_{n-1}]) = [\mathtt{f}^{\mathfrak{A}}(a_0, \ldots, a_{n-1})].$$

The algebra $\mathfrak{A}/\equiv$ thus defined is called the **factor algebra** or **quotient algebra** of $\mathfrak{A}$ by $\equiv$.

In the above definition, the value of $\mathtt{f}^{\mathfrak{A}/\equiv}$ is (uniquely) determined by the fact that $\equiv$ is the congruence relation. That is, if $[a_0] = [a'_0], \ldots, [a_{n-1}] = [a'_{n-1}]$, then we have

$$[\mathtt{f}^{\mathfrak{A}}(a_0, \ldots, a_{n-1})] = [\mathtt{f}^{\mathfrak{A}}(a'_0, \ldots, a'_{n-1})].$$

Example 5

Consider the congruence relation in Example 3.
To make $\mathfrak{Z}/\equiv_3$, we first have $\mathbb{Z}/\equiv_3 = \{[0], [1], [2]\}$.
Then the operations on $\mathfrak{Z}/\equiv_3$ are defined as follows:
$[m] +^{\mathfrak{Z}/\equiv_3} [n] = [m+n]$, $[m] \cdot^{\mathfrak{Z}/\equiv_3} [n] = [m \cdot n]$, $-^{\mathfrak{Z}/\equiv_3}[m] = [-m]$, $0^{\mathfrak{Z}/\equiv_3} = [0]$, $1^{\mathfrak{Z}/\equiv_3} = [1]$.

Example 6

Let $\mathfrak{H}$ be a normal subgroup of the group $\mathfrak{G}$, then $\mathfrak{G}/\equiv_H$ is the usual residue group $\mathfrak{G}/\mathfrak{H}$. (see also Problem 6)

Lemma 2.7

If $\equiv$ is a congruence relation on an algebra $\mathfrak{A}$, then $\pi : \mathfrak{A} \to \mathfrak{A}/\equiv$ defined by $\pi(a) = [a]$ is a homomorphism.

By the definition of residue algebra, the proof of the lemma should be clear.
In the following, we represent this homomorphism π as $\pi_{\equiv}$.

Lemma 2.8

Let $\mathfrak{A}$, $\mathfrak{B}$ be $\mathcal{L}$-algebras and $\phi : \mathfrak{A} \to \mathfrak{B}$ be a homomorphism. If we define a binary relation $\equiv$ on A as

$$a \equiv b \Leftrightarrow \phi(a) = \phi(b),$$

then $\equiv$ is a congruence relation on $\mathfrak{A}$.

Proof.
It is clear that $\equiv$ is an equivalence relation. To show the preservation property of $\mathtt{f}$, suppose $a_0 \equiv b_0, \ldots, a_{n-1} \equiv b_{n-1}$. Then,

$$\begin{array}{rcll} \phi(\mathtt{f}^{\mathfrak{A}}(a_0, \ldots, a_{n-1})) & = & \mathtt{f}^{\mathfrak{B}}(\phi(a_0), \ldots, \phi(a_{n-1})) & (\phi \text{ is a homomorphism}) \\ & = & \mathtt{f}^{\mathfrak{B}}(\phi(b_0), \ldots, \phi(b_{n-1})) & (\text{by assumption } a_i \equiv b_i) \\ & = & \phi(\mathtt{f}^{\mathfrak{A}}(b_0, \ldots, b_{n-1})) & (\phi \text{ is a homomorphism}). \end{array}$$

Therefore, we have

$$\mathtt{f}^{\mathfrak{A}}(a_0, \ldots, a_{n-1}) \equiv \mathtt{f}^{\mathfrak{A}}(b_0, \ldots, b_{n-1}).$$

□

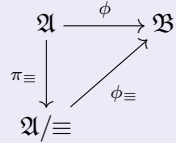
Homomorphism theorem

Theorem 2.9 (Homomorphism theorem)

Let $\phi : \mathfrak{A} \to \mathfrak{B}$ be a surjective homomorphism. Let $\equiv$ be the congruence relation on $\mathfrak{A}$ defined in the above lemma, that is,

$$a \equiv b \Leftrightarrow \phi(a) = \phi(b).$$

Then there exists an isomorphism $\phi_{\equiv} : \mathfrak{A}/\equiv \to \mathfrak{B}$ such that $\phi = \phi_{\equiv} \circ \pi_{\equiv}$.



Proof.

- We define $\phi_{\equiv}$ as $\phi_{\equiv}([a]) = \phi(a)$ for $[a] \in |\mathfrak{A}/\equiv|$,
- If $[a] = [b]$, by definition we have $a \equiv b$, and thus $\phi(a) = \phi(b)$. The converse is also true. Hence $\phi_{\equiv}$ is injective.
- Since ϕ is surjective, so is $\phi_{\equiv}$.
- Finally, we claim that $\phi_{\equiv}$ is a homomorphism.

$$
\begin{array}{lcll}
\phi_{\equiv}(\mathtt{f}^{\mathfrak{A}/\equiv}([a_0], \ldots, [a_{n-1}])) & = & \phi_{\equiv}([\mathtt{f}^{\mathfrak{A}}(a_0, \ldots, a_{n-1})]) & \text{(def. of factor algebra)} \\
& = & \phi(\mathtt{f}^{\mathfrak{A}}(a_0, \ldots, a_{n-1})) & \text{(definition of } \phi_{\equiv}\text{)} \\
& = & \mathtt{f}^{\mathfrak{B}}(\phi(a_0), \ldots, \phi(a_{n-1})) & (\phi \text{ is a homomorphism}) \\
& = & \mathtt{f}^{\mathfrak{B}}(\phi_{\equiv}([a_0]), \ldots, \phi_{\equiv}([a_{n-1}])) & \text{(definition of } \phi_{\equiv}\text{)}.
\end{array}
$$

□

The following corollary can be proved in almost the same way as the homomorphism theorem.

Corollary 2.10

Let $\phi : \mathfrak{A} \to \mathfrak{B}$ be a homomorphism and $\equiv$ be a congruence relation on $\mathfrak{A}$ such that

$$a \equiv b \Rightarrow \phi(a) = \phi(b).$$

Then there exists a homomorphism $\phi_{\equiv} : \mathfrak{A}/\equiv \to \mathfrak{B}$ such that $\phi = \phi_{\equiv} \circ \pi_{\equiv}$.

Thank you for your attention!