Cambridge University Press
978-1-107-16388-1 — An Invitation to Model Theory
Jonathan Kirby
Excerpt
More Information

Part I

Languages and Structures

In this first part of the book, we introduce the basic methods from predicate logic which underpin the rest of the book. Mathematical objects are formalised as L-structures, and statements about these structures are formalised in the notions of L-terms and L-formulas. We introduce the central notion of a definable set, a subset of an L-structure which is defined by an L-formula. A key notion in mathematical logic is that of a recursive definition, and both the notions of L-terms and L-formulas give examples of that. These recursive definitions give rise to methods of proof by induction. Throughout this part, these proofs by induction are used prove preservation theorems, most importantly the preservation of definable sets by automorphisms of a structure. From this result we get a method to show that certain subsets of a structure are *not* definable, an essential tool which we will later exploit in the programme of characterising the definable sets of a structure.

1
Structures

In different mathematical contexts, familiar mathematical objects may actually have different meanings. For example a reference to the integers $\mathbb{Z}$ in group theory is likely to mean the infinite cyclic group, whereas in number theory it is likely to mean $\mathbb{Z}$ as a ring. In model theory, when we specify a structure, we have to be precise about such things. The integers as an additive group will be written as $\mathbb{Z}_{\text{adgp}} = \langle \mathbb{Z}; +, -, 0 \rangle$, and $\mathbb{Z}$ as a ring will be written as $\mathbb{Z}_{\text{ring}} = \langle \mathbb{Z}; +, \cdot, -, 0, 1 \rangle$. The integers are also used to index the years in a calendar, and an appropriate structure for that purpose is $\mathbb{Z}_< = \langle \mathbb{Z}; < \rangle$, because it is not very meaningful to add or multiply calendar years, but the order is important. In general, we capture these ideas with the notions of a language, L, and an L-structure.

1.1 *L*-structures

Definition 1.1 A *language* L is specified by the following (sometimes called the *vocabulary* or *signature* of L):

(i) a set of *relation symbols*,
(ii) a set of *function symbols*,
(iii) a set of *constant symbols*, and
(iv) for each relation and function symbol, a positive natural number called its *arity*.

Definition 1.2 An *L-structure* $\mathcal{A}$ consists of a set A called the *domain* of the structure, together with *interpretations* of the symbols from L:

(i) for each relation symbol R of L, of arity n, a subset $R^{\mathcal{A}}$ of A^n,
(ii) for each function symbol f of L, of arity n, a function $f^{\mathcal{A}} : A^n \to A$, and
(iii) for each constant symbol c of L an element $c^{\mathcal{A}} \in A$.

Example 1.3 The language of rings $L_{\text{ring}} = \langle +, \cdot, -, 0, 1 \rangle$, where $+$ and $\cdot$ are function symbols of arity 2 (we say they are *binary* function symbols), $-$ is a function symbol of arity 1 (a *unary* function symbol for negation rather than the binary function of subtraction), and 0 and 1 are constant symbols. $\mathbb{Z}_{\text{ring}}$ is the L_{ring}-structure with domain the set $\mathbb{Z}$ of integers. We interpret the symbols $+$, $\cdot$, and $-$ as the usual functions of addition, multiplication, and negation of integers and the constant symbols 0 and 1 are interpreted as the usual zero and one. We can write this as $\mathbb{Z}_{\text{ring}} = \langle \mathbb{Z}; +^{\mathbb{Z}}, \cdot^{\mathbb{Z}}, -^{\mathbb{Z}}, 0^{\mathbb{Z}}, 1^{\mathbb{Z}} \rangle$ if for example we want to distinguish the symbol $+$ from its interpretation $+^{\mathbb{Z}}$ as a function from $\mathbb{Z}^2$ to $\mathbb{Z}$. This distinction can be important in mathematical logic. For example we also have the L_{ring}-structure $\mathbb{R}_{\text{ring}}$ with domain the set of real numbers $\mathbb{R}$, and the function $+^{\mathbb{R}} : \mathbb{R}^2 \to \mathbb{R}$ is not the same function as $+^{\mathbb{Z}} : \mathbb{Z}^2 \to \mathbb{Z}$. However, usually no ambiguity arises, and we just write $+$ for the symbol and for its interpretations in different structures.

Example 1.4 We write $L_< = \langle < \rangle$, where $<$ is a binary relation symbol. Then $\mathbb{Z}_<$ is the $L_<$-structure with domain the set $\mathbb{Z}$ of integers, and the symbol $<$ is interpreted as the set of pairs $\left\{(a, b) \in \mathbb{Z}^2 \mid a < b\right\}$. As above, we could write this set as $<^{\mathbb{Z}}$, but usually we will not.

Examples 1.5 Many other languages can be built as variations on these two languages:

(i) $L_{\text{gp}} = \langle \cdot, (-)^{-1}, 1 \rangle$ is the language of groups. Again, $\cdot$ is a binary function symbol, $(-)^{-1}$ is a unary function symbol representing the multiplicative inverse function $x \mapsto x^{-1}$, and 1 is a constant symbol.

(ii) $L_{\text{adgp}} = \langle +, -, 0 \rangle$ is the language of groups written additively. It is a *sub-language* of L_{ring}, because every symbol in L_{adgp} is also in L_{ring} (with the same arity). We also say that L_{ring} is an *expansion* of the language L_{adgp}.

(iii) $L_{\text{o-ring}} = \langle +, \cdot, -, 0, 1, < \rangle$ is the language of ordered rings, consisting of $L_{\text{ring}} \cup L_<$.

(iv) A common language in which to consider the natural numbers is the language of semirings, $L_{\text{s-ring}} = \langle +, \cdot, 0, 1 \rangle$. We will always use the convention that 0 is a natural number.

(v) The language of monoids is $L_{\text{mon}} = \langle \cdot, 1 \rangle$ and the language of additive monoids is $L_{\text{admon}} = \langle +, 0 \rangle$.

Most of the structures we will consider as examples have a domain with a commonly used notation such as $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{R}$, and the functions, relations, and constants we consider will be those in the above languages. In this case we name the structure by putting the name of the language as a subscript, for example $\mathbb{Z}_{\text{ring}}$, $\mathbb{R}_{\text{o-ring}}$, $\mathbb{Q}_{<}$, $\mathbb{N}_{\text{s-ring}}$.

We can also specify structures directly, which is useful for creating simpler examples. In this case we will often use a caligraphic letter for the name of the structure and the corresponding Roman letter for the name of its domain, so $\mathcal{A}$ would be the name of a structure with domain A. This convention of using different notation for the name of a structure and its domain is useful when the same set is the domain of different structures. However, where no confusion is likely to arise, we will sometimes follow the common mathematical practice of using the same notation for both.

Example 1.6 Take the language $L = \langle R, f, c \rangle$, where R is a ternary relation symbol, f is a unary function symbol, and c is a constant symbol. We can define an L-structure $\mathcal{A}$ with domain $A = \{0, 1, 2, 3, 4\}$, by specifying the interpretation of the symbols as $f^{\mathcal{A}}(x) = x+1 \mod 5$, $R^{\mathcal{A}} = \left\{(x, y, z) \in A^3 \;\middle|\; \text{exactly two of } x, y \text{ and } z \text{ are equal}\right\}$ and $c^{\mathcal{A}} = 3$.

Remark 1.7 The key idea from mathematical logic here is that the symbols of the vocabulary of a language L are separate from their interpretations in a structure. It follows that the symbols do not have to be interpreted by their usual meanings. For example we can make the set $\mathbb{N}$ into an L_{gp}-structure by interpreting the symbol $\cdot$ as addition and $(-)^{-1}$ as the identity function, so $x^{-1} = x$ for all $x \in \mathbb{N}$, and interpreting the constant symbol 1 as the number 2. However, this is perverse, and if we want an unusual interpretation, we will choose to use a different symbol.

Given a mathematical problem you are trying to solve, or a statement you want to understand, it is often a good exercise to work out what structure the statement might be about. For example, the fundamental theorem of arithmetic states that every positive integer can be written as a product of primes in a unique way (up to reordering). An appropriate structure would have domain the set $\mathbb{N}^+$ of positive integers and needs to have the multiplication function; 1 is a special case as the empty product, which is relevant to single out, so we can regard the fundamental theorem of arithmetic as a statement about the structure $\mathbb{N}^+_{\text{mon}} = \langle \mathbb{N}^+; \cdot, 1 \rangle$. To actually prove the theorem, we might need more than that, for example the order to do induction on and also addition.

1.2 Expansions and Reducts

When considering different structures with the same domain, there are two useful pieces of terminology.

Definition 1.8 Let L be a language and L^+ another language such that $L \subseteq L^+$, that is, every symbol of L is also a symbol of L^+. Let $\mathcal{A}^+$ be an L^+-structure with domain A. Then the *reduct* of $\mathcal{A}^+$ to L is the L-structure $\mathcal{A}$ with domain A, and every symbol of L interpreted in $\mathcal{A}$ exactly as in $\mathcal{A}^+$. We also say that $\mathcal{A}^+$ is an *expansion* of $\mathcal{A}$ to the language L^+.

For example $\mathbb{R}_{\text{adgp}} = \langle \mathbb{R}; +, -, 0 \rangle$ is a reduct of $\mathbb{R}_{\text{ring}} = \langle \mathbb{R}; +, -, \cdot, 0, 1 \rangle$, which in turn is a reduct of $\mathbb{R}_{\text{o-ring}} = \langle \mathbb{R}; +, -, \cdot, 0, 1, < \rangle$.

1.3 Embeddings and Automorphisms

Definition 1.9 Let $\mathcal{A}$ and $\mathcal{B}$ be L-structures. An *embedding* of L-structures from $\mathcal{A}$ to $\mathcal{B}$ is an injective function $A \xrightarrow{\pi} B$ such that:

(i) for all relation symbols R of L, and all $a_1, \ldots, a_n \in A$,

$$(a_1, \ldots, a_n) \in R^{\mathcal{A}} \text{ iff } (\pi(a_1), \ldots, \pi(a_n)) \in R^{\mathcal{B}},$$

(ii) for all function symbols f of L, and all $a_1, \ldots, a_n \in A$,

$$\pi(f^{\mathcal{A}}(a_1, \ldots, a_n)) = f^{\mathcal{B}}(\pi(a_1), \ldots, \pi(a_n)), \quad \text{and}$$

(iii) for all constant symbols c of L, $\pi(c^{\mathcal{A}}) = c^{\mathcal{B}}$.

For any L-structure $\mathcal{A}$, the identity function 1_A on A is a embedding of $\mathcal{A}$ into itself. An embedding $\mathcal{A} \xrightarrow{\pi} \mathcal{B}$ is an *isomorphism* iff there is an embedding $\mathcal{B} \xrightarrow{\sigma} \mathcal{A}$ such that the composite $\pi \circ \sigma$ is the identity on $\mathcal{B}$ and the composite $\sigma \circ \pi$ is the identity on $\mathcal{A}$. We write π^{-1} for σ, as usual, and call it the inverse of π. An isomorphism from $\mathcal{A}$ to itself is called an *automorphism* of $\mathcal{A}$.

Examples 1.10 We have the obvious inclusion functions $\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$, which take a number to itself. These inclusion functions give us embeddings of L_{ring}-structures

$$\mathbb{Z}_{\text{ring}} \hookrightarrow \mathbb{Q}_{\text{ring}} \hookrightarrow \mathbb{R}_{\text{ring}} \hookrightarrow \mathbb{C}_{\text{ring}}.$$

Definition 1.11 If we have an embedding $\mathcal{A} \longrightarrow \mathcal{B}$ where the function is an inclusion of the domain of $\mathcal{A}$ as a subset of the domain of $\mathcal{B}$ then we say that $\mathcal{A}$ is a *substructure* of $\mathcal{B}$, and that $\mathcal{B}$ is an *extension* of $\mathcal{A}$.

Example 1.12 The only automorphisms of $\mathbb{Z}_{\text{adgp}}$ are the identity and the map $x \mapsto -x$. To see this, note that if $\pi : \mathbb{Z} \to \mathbb{Z}$ is an L_{adgp}-embedding, then $\pi(0) = 0$, and if $\pi(1) = n$, then for any $m \in \mathbb{N}^+$, we have

$$\pi(m) = \pi(\underbrace{1 + \cdots + 1}_{m}) = \underbrace{\pi(1) + \cdots + \pi(1)}_{m} = mn.$$

Then also $\pi(-n) = -\pi(n) = -mn$. To have an inverse, π must be surjective, which implies $n = \pm 1$.

Exercises

1.1 Let $L = \langle f, c \rangle$ be a language with one unary function symbol and one constant symbol. Describe all the possible L-structures on the domain $\{1, 2\}$. How many of them are there up to isomorphism (which means counting isomorphic structures as the same)?

1.2 For each of the following statements, give a structure which they say something about.

(a) There is no largest integer.
(b) Every integer has an additive inverse.
(c) Square integers are always non-negative.
(d) Every complex number is the sum of a real number and i times a real number.
(e) The exponential function is strictly increasing on the real numbers.
(f) A real quadratic equation $ax^2 + bx + c = 0$ has real roots if and only if $b^2 - 4ac \geqslant 0$.
(g) Euler's identity $e^{i\pi} + 1 = 0$.

1.3 For each language L in Examples 1.5, say which of the sets from $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{R}$ is the domain of an L-structure with the symbols interpreted with their usual meanings. For example, there is no structure $\mathbb{N}_{\text{gp}}$ because $\mathbb{N}$ is not closed under multiplicative inverses. Which of your structures are expansions or reducts of each other? Which are extensions or substructures?

1.4 What are all the automorphisms of $\mathbb{Z}_<$?

1.5 Show that embeddings of $\mathbb{N}_<$ into $\mathbb{R}_<$ correspond to strictly increasing sequences of real numbers.

1.6 Show that an embedding of L-structures is an isomorphism if and only if it is surjective.

1.7 Explain what all the embeddings of $\mathbb{Z}_{\text{adgp}}$ into $\mathbb{R}_{\text{adgp}}$ are.

1.8 Find an automorphism π of the structure $\langle \mathbb{R}; < \rangle$ such that $\pi(0) = 1$ and $\pi(1) = 5$. Is your π also an automorphism of the structure $\langle \mathbb{R}; + \rangle$?

1.9 Find all the automorphisms of $\mathbb{Q}_{\text{adgp}}$.

1.10 Suppose that $\mathcal{A}^+$ is an expansion of $\mathcal{A}$ and π is an automorphism of $\mathcal{A}^+$. Show that π is also an automorphism of $\mathcal{A}$. Give an example to show that an automorphism of $\mathcal{A}$ may not be an automorphism of $\mathcal{A}^+$.

1.11 Let $\mathcal{A}$ be an L-structure. Show that the automorphisms of $\mathcal{A}$ form a group with the group operation being composition. We write this group as $\mathrm{Aut}(\mathcal{A})$.

1.12 In model theory, a *homomorphism* of L-structures $\mathcal{A} \xrightarrow{\pi} \mathcal{B}$ is a function $A \xrightarrow{\pi} B$ such that

(a) for all relation symbols R of L, and all $a_1, \ldots, a_n \in A$, if $(a_1, \ldots, a_n) \in R^{\mathcal{A}}$ then $(\pi(a_1), \ldots, \pi(a_n)) \in R^{\mathcal{B}}$,
(b) for all function symbols f of L, and all $a_1, \ldots, a_n \in A$, $\pi(f^{\mathcal{A}}(a_1, \ldots, a_n)) = f^{\mathcal{B}}(\pi(a_1), \ldots, \pi(a_n))$, and
(c) for all constant symbols c of L, $\pi(c^{\mathcal{A}}) = c^{\mathcal{B}}$.

Check that if $L = L_{\text{gp}}$ or $L = L_{\text{ring}}$, and $\mathcal{A}, \mathcal{B}$ are groups or rings, then L-homomorphisms are the same as group or ring homomorphisms. How do L-homomorphisms compare with, and how do they differ from, the notion of embedding of L-structures?