Definability in a Structure

Suppose we want to study the real field, $(\mathbb{R}; 0, 1, +, \cdot)$, consisting of the set $\mathbb{R}$ of real numbers, together with the distinguished elements 0 and 1 and the two operations of addition and multiplication. We can consider the real field as a structure

$$\mathfrak{R} = (\mathbb{R}; 0, 1, +, \cdot)$$

where the language (with equality) has constant symbols **0** and **1** and two-place function symbols $+$ and $\cdot$.

Although we have not included an ordering symbol $<$ in the language, we still have a way to say "$x \geq 0$." Because *in this structure*, the nonnegative elements are exactly the elements with square roots. That is, the formula $\exists\, \mathbf{v}_2\; x = \mathbf{v}_2 \cdot \mathbf{v}_2$ is satisfied in the structure $\mathfrak{R}$ whenever x is assigned a nonnegative number, and only then:

$$\models_{\mathfrak{R}} \exists\, \mathbf{v}_2\;\mathbf{v}_1 = \mathbf{v}_2 \cdot \mathbf{v}_2\, [\![a]\!] \iff a \geq 0.$$

Because of this fact, we will say that the interval $[0, \infty)$ is *definable* in $\mathfrak{R}$, and that the formula $\exists\, \mathbf{v}_2\; \mathbf{v}_1 = \mathbf{v}_2 \cdot \mathbf{v}_2$ defines it.

Moreover, the ordering relation on the reals, i.e., the binary relation

$$\{\langle a, b\rangle \in \mathbb{R} \times \mathbb{R} \mid a \leq b\},$$

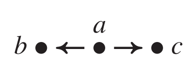
is defined in the structure $\mathfrak{R}$ by the formula expressing "$\mathbf{v}_1 \leq \mathbf{v}_2$":

$$\exists \mathbf{v}_3\; \mathbf{v}_2 = \mathbf{v}_1 + \mathbf{v}_3 \cdot \mathbf{v}_3.$$

For a smaller example, take the directed graph

$$\mathfrak{A} = (\{a, b, c\}; \{\langle a, b\rangle, \langle a, c\rangle\})$$

where the language has parameters $\forall$ and E:



Then in $\mathfrak{A}$, the set $\{b, c\}$ (the range of the relation $E^{\mathfrak{A}}$) is defined by the formula $\exists\, \mathbf{v}_2\; E\mathbf{v}_2\mathbf{v}_1$. In contrast, the set $\{b\}$ is *not* definable in $\mathfrak{A}$. This is because there is no definable property in this structure that would separate b and c; the proof of this fact will utilize the homomorphism theorem, to be proved later in this section.

We now want to set forth precisely this concept of definability of a subset of the universe or of a relation on the universe. Consider a structure $\mathfrak{A}$ and a formula φ whose free variables are among $\mathbf{v}_1, \ldots, \mathbf{v}_k$. Then we can construct the k-ary relation on $|\mathfrak{A}|$

$$\{\langle a_1, \ldots, a_k\rangle \mid \models_{\mathfrak{A}} \varphi[\![a_1, \ldots, a_k]\!]\}.$$

Call this the k-ary relation φ *defines* in $\mathfrak{A}$. In general, a k-ary relation on $|\mathfrak{A}|$ is said to be *definable* in $\mathfrak{A}$ iff there is a formula (whose free variables are among $\mathbf{v}_1, \ldots, \mathbf{v}_k$) that defines it there.

Example. Assume that we have a part of the language for number theory, specifically that our language has the parameters $\forall$, $\mathbf{0}$, $\mathbf{S}$, $+$, and $\cdot$. Let $\mathfrak{N}$ be the intended structure:

$|\mathfrak{N}| = \mathbb{N}$, the set of natural numbers.
$\mathbf{0}^{\mathfrak{N}} = 0$, the number 0.
$\mathbf{S}^{\mathfrak{N}}$, $+^{\mathfrak{N}}$, and $\cdot^{\mathfrak{N}}$ are S, $+$, and $\cdot$, the functions of successor, addition, and multiplication.

In one equation,

$$\mathfrak{N} = (\mathbb{N}; 0, S, +, \cdot).$$

Some relations on $\mathbb{N}$ are definable in $\mathfrak{N}$ and some are not. One way to show that some are not definable is to use the fact that there are uncountably many relations on $\mathbb{N}$ but only countably many possible defining formulas. (There is, however, an inherent difficulty in giving a specific example. After all, if something is undefinable, then it is hard to say exactly what it is! Later we will get to see a specific example, the set of Gödel numbers of sentences true in $\mathfrak{N}$; see Section 3.5.)

1. The ordering relation $\{\langle m, n\rangle \mid m < n\}$ is defined in $\mathfrak{N}$ by the formula

$$\exists\, \mathbf{v}_3\ \mathbf{v}_1 + \mathbf{S}\mathbf{v}_3 = \mathbf{v}_2.$$

2. For any natural number n, $\{n\}$ is definable. For example, $\{2\}$ is defined by the equation

$$\mathbf{v}_1 = \mathbf{SS0}.$$

Because of this we say that n is a *definable element* in $\mathfrak{N}$.

3. The set of primes is definable in $\mathfrak{N}$. We could use the formula

$$\mathbf{1} < \mathbf{v}_1 \land \forall\, \mathbf{v}_2\, \forall\, \mathbf{v}_3 (\mathbf{v}_1 = \mathbf{v}_2 \cdot \mathbf{v}_3 \to \mathbf{v}_2 = \mathbf{1} \lor \mathbf{v}_3 = \mathbf{1})$$

if we had parameters $\mathbf{1}$ and $<$ for 1 and $<$. But since $\{1\}$ and $<$ are definable in $\mathfrak{N}$, it is really quite unnecessary to add parameters for them; we can simply use their definitions instead. Thus the set of primes is definable by

$$\exists\, \mathbf{v}_3\, \mathbf{S0} + \mathbf{S}\mathbf{v}_3 = \mathbf{v}_1 \land \forall\, \mathbf{v}_2\, \forall\, \mathbf{v}_3\ (\mathbf{v}_1 = \mathbf{v}_2 \cdot \mathbf{v}_3 \to \mathbf{v}_2 = \mathbf{S0} \lor \mathbf{v}_3 = \mathbf{S0}).$$

4. Exponentiation, $\{\langle m, n, p\rangle \mid p = m^n\}$ is also definable in $\mathfrak{N}$. This is by no means obvious; we will give a proof later (in Section 3.8) using the Chinese remainder theorem.

In fact, we will argue later that any decidable relation on $\mathbb{N}$ is definable in $\mathfrak{N}$, as is any effectively enumerable relation and a great many others. To some extent the complexity of a definable relation can be measured by the complexity of the simplest defining formula. This idea will come up again at the end of Section 3.5.

Definability of a Class of Structures

Many a mathematics class, on its first day, begins with the instructor saying something like one of the following:

1. "A *graph* is defined to consist of a nonempty set V together with a set E such that. . . ."
2. "A *group* is defined to consist of a nonempty set G together with a binary operation $\circ$ satisfying the axioms. . . ."
3. "An *ordered field* is defined to consist of a nonempty set F together with two binary operations $+$ and $\cdot$ and a binary relation $<$ satisfying the axioms. . . ."
4. "A *vector space* is defined to consist of a nonempty set V together with a binary operation $+$ and, for each real number r, an operation called scalar multiplication such that. . . ."

We want to abstract from this situation. In each case, the objects of study (the graphs, the groups, and so forth) are *structures* for a suitable language. Moreover, they are required to satisfy a certain set Σ of sentences (referred to as "axioms"). The course in question then studies the models of the set Σ of axioms — or at least some of the models.

For a set Σ of sentences, let Mod Σ be the class of all models of Σ, i.e., the class of all structures for the language in which every member of Σ is true. For a single sentence τ we write simply "Mod τ" instead of "Mod $\{\tau\}$." (The reader familiar with axiomatic set theory will notice that Mod Σ, if nonempty, is a proper class; i.e., it is too large to be a set.)

A class $\mathcal{K}$ of structures for our language is an *elementary class* (EC) iff $\mathcal{K} = \text{Mod } \tau$ for some sentence τ. $\mathcal{K}$ is an *elementary class in the wider sense* (EC_Δ) iff $\mathcal{K} = \text{Mod } \Sigma$ for some set Σ of sentences. (The adjective "elementary" is employed as a synonym for "first-order.")

Examples

1. Assume that the language has equality and the two parameters $\forall$ and E, where E is a two-place predicate symbol. Then a *graph* is a structure for this language $\mathfrak{A} = (V; E^{\mathfrak{A}})$ consisting of a nonempty set V of objects called *vertices* (or *nodes*), and an *edge relation* $E^{\mathfrak{A}}$ that is symmetric (if $uE^{\mathfrak{A}}v$ then $vE^{\mathfrak{A}}u$) and irreflexive (never $vE^{\mathfrak{A}}v$). The axiom stating that the edge relation is symmetric and irreflexive can be translated by the sentence

$$\forall x(\neg xEx \wedge \forall y(xEy \rightarrow yEx)).$$

So the class of all graphs is an elementary class. For *directed graphs* or *digraphs*, the assumption of symmetry is dropped. And if one wants to allow "loops" then the assumption of irreflexivity is dropped. But perhaps the instructor then explains that the course will study only *finite* graphs. Is the class of all finite graphs an elementary class? No, we will prove later that it is not, not even in the wider sense.

2. Assume that the language has equality and the parameters $\forall$ and P, where P is a two-place predicate symbol. As before, a structure $(A; R)$ for the language consists of a nonempty set A together with a binary relation R on A. $(A; R)$ is called an *ordered set* iff R is transitive and satisfies the trichotomy condition (which states that for any a and b in A, exactly one of $\langle a, b\rangle \in R$, $a = b$, $\langle b, a\rangle \in R$ holds). Because these conditions can be translated into a sentence of the formal language, the class of nonempty ordered sets is an elementary class. It is, in fact, Mod τ, where τ is the conjunction of the three sentences

$$\forall x \forall y \forall z(xPy \rightarrow yPz \rightarrow xPz);$$
$$\forall x \forall y(xPy \vee x = y \vee yPx);$$
$$\forall x \forall y(xPy \rightarrow \neg yPx).$$

The next two examples assume that the reader has had some contact with algebra.

3. Assume that the language has $=$ and the parameters $\forall$ and $\circ$, where $\circ$ is a two-place function symbol. The class of all groups is an elementary class, being the class of all models of the conjunction of the group axioms:

$$\forall x \forall y \forall z\,(x \circ y) \circ z = x \circ (y \circ z);$$
$$\forall x \forall y \exists z\, x \circ z = y;$$
$$\forall x \forall y \exists z\, z \circ x = y.$$

The class of all infinite groups is EC_Δ. To see this, let

$$\lambda_2 = \exists x \exists y\, x \neq y,$$
$$\lambda_3 = \exists x \exists y \exists z(x \neq y \wedge x \neq z \wedge y \neq z),$$
$$\ldots.$$

Thus λ_n translates, "There are at least n things." Then the group axioms together with $\{\lambda_2, \lambda_3, \ldots\}$ form a set Σ for which Mod Σ is exactly the class of infinite groups. We will eventually (in Section 2.6) be able to show that the class of infinite groups is not EC.

4. Assume that the language has equality and the parameters $\forall, \mathbf{0}, \mathbf{1}, +, \cdot$. Fields can be regarded as structures for this language.

The class of all fields is an elementary class. The class of fields of characteristic zero is EC_Δ. It is not EC, a fact which will follow from the compactness theorem for first-order logic (Section 2.6 again).

Homomorphisms[1]

In courses about graphs or groups or vector spaces, one usually encounters the concept of what it means for two of the structures in question, $\mathfrak{A}$ and $\mathfrak{B}$, to be *isomorphic*: Roughly speaking, there must be a one-to-one correspondence between their universes $|\mathfrak{A}|$ and $|\mathfrak{B}|$ that "preserves" the operations and relations.

It is then explained that two isomorphic structures, although not identical, must have all the same mathematical properties. We want to define here the isomorphism concept in a general setting, and to show that two isomorphic structures must satisfy exactly the same sentences.

Let $\mathfrak{A}$, $\mathfrak{B}$ be structures for the language. A *homomorphism* h of $\mathfrak{A}$ into $\mathfrak{B}$ is a function $h : |\mathfrak{A}| \to |\mathfrak{B}|$ with the properties:

(a) For each n-place predicate parameter P and each n-tuple $\langle a_1, \ldots, a_n \rangle$ of elements of $|\mathfrak{A}|$,

$$\langle a_1, \ldots, a_n \rangle \in P^{\mathfrak{A}} \quad \text{iff} \quad \langle h(a_1), \ldots, h(a_n) \rangle \in P^{\mathfrak{B}}.$$

(b) For each n-place function symbol f and each such n-tuple,

$$h(f^{\mathfrak{A}}(a_1, \ldots, a_n)) = f^{\mathfrak{B}}(h(a_1), \ldots, h(a_n)).$$

In the case of a constant symbol c this becomes

$$h(c^{\mathfrak{A}}) = c^{\mathfrak{B}}.$$

Conditions (a) and (b) are usually stated: "h preserves the relations and functions." (It must be admitted that some authors use a weakened version of condition (a); our homomorphisms are their "strong homomorphisms.")

If, in addition, h is one-to-one, it is then called an *isomorphism* (or an *isomorphic embedding*) of $\mathfrak{A}$ into $\mathfrak{B}$. If there is an isomorphism of $\mathfrak{A}$ onto $\mathfrak{B}$ (i.e., an isomorphism h for which $\operatorname{ran} h = |\mathfrak{B}|$), then $\mathfrak{A}$ and $\mathfrak{B}$ are said to be *isomorphic* (written $\mathfrak{A} \cong \mathfrak{B}$).

The reader has quite possibly encountered this concept before in special cases such as structures that are groups or fields.

[1] This topic can be postponed somewhat. But homomorphisms will be used in the proof of the completeness theorem (with equality). And we make use of the isomorphism concept, starting in Section 6 of Chapter 2.

Example. Assume that we have a language with the parameters $\forall$, $+$, and $\cdot$. Let $\mathfrak{A}$ be the structure $(\mathbb{N}; +, \cdot)$. We can define a function $h : \mathbb{N} \to \{e, o\}$ by

$$h(n) = \begin{cases} e & \text{if } n \text{ is even,} \\ o & \text{if } n \text{ is odd.} \end{cases}$$

Then h is a homomorphism of $\mathfrak{A}$ onto $\mathfrak{B}$, where $|\mathfrak{B}| = \{e, o\}$ and $+^{\mathfrak{B}}$, $\cdot^{\mathfrak{B}}$ are given by the following tables:

$+^{\mathfrak{B}}$	e	o
e	e	o
o	o	e

$\cdot^{\mathfrak{B}}$	e	o
e	e	e
o	e	o

It can then be verified that condition (b) of the definition is satisfied. For example, if a and b are both odd numbers, then $h(a+b) = e$ and $h(a) +^{\mathfrak{B}} h(b) = o +^{\mathfrak{B}} o = e$.

Example. Let $\mathbb{P}$ be the set of positive integers, let $<_P$ be the usual ordering relation on $\mathbb{P}$, and let $<_N$ be the usual ordering relation on $\mathbb{N}$. Then there is an isomorphism h from the structure $(\mathbb{P}; <_P)$ onto $(\mathbb{N}; <_N)$; we take $h(n) = n - 1$. Also the identity map $Id : \mathbb{P} \to \mathbb{N}$ is an isomorphism of $(\mathbb{P}; <_P)$ into $(\mathbb{N}; <_N)$. Because of this last fact, we say that $(\mathbb{P}; <_P)$ is a *substructure* of $(\mathbb{N}; <_N)$.

More generally consider two structures $\mathfrak{A}$ and $\mathfrak{B}$ for the language such that $|\mathfrak{A}| \subseteq |\mathfrak{B}|$. It is clear from the definition of homomorphism that the identity map from $|\mathfrak{A}|$ into $|\mathfrak{B}|$ is an isomorphism of $\mathfrak{A}$ into $\mathfrak{B}$ iff

(a) $P^{\mathfrak{A}}$ is the restriction of $P^{\mathfrak{B}}$ to $|\mathfrak{A}|$, for each predicate parameter P;

(b) $f^{\mathfrak{A}}$ is the restriction of $f^{\mathfrak{B}}$ to $|\mathfrak{A}|$, for each function symbol f, and $c^{\mathfrak{A}} = c^{\mathfrak{B}}$ for each constant symbol c.

If these conditions are met, then $\mathfrak{A}$ is said to be a *substructure* of $\mathfrak{B}$, and $\mathfrak{B}$ is an *extension* of $\mathfrak{A}$.

For example, in a language with a two-place function symbol $+$, the structure $(\mathbb{Q}; +_Q)$ is a substructure of $(\mathbb{C}; +_C)$. Here $+_C$ is the addition operation on complex numbers. And $+_Q$, addition on the rationals, is exactly the restriction of $+_C$ to the set $\mathbb{Q}$.

In this example, the set $\mathbb{Q}$ is closed under $+_C$; that is, the sum of two rational numbers is rational. More generally, whenever $\mathfrak{A}$ is a substructure of $\mathfrak{B}$, then $|\mathfrak{A}|$ must be closed under $f^{\mathfrak{B}}$ for every function symbol f. After all, $f^{\mathfrak{B}}(\vec{a})$ (where $\vec{a} \in |\mathfrak{A}|^n$) is nothing but $f^{\mathfrak{A}}(\vec{a})$, which must be some element in $|\mathfrak{A}|$. This closure property even holds for the 0-place function symbols; $c^{\mathfrak{B}}$ must belong to $|\mathfrak{A}|$ for each constant symbol c.

Conversely, suppose we have a structure $\mathfrak{B}$, and let A be any nonempty subset of $|\mathfrak{B}|$ that is closed under all of $\mathfrak{B}$'s functions, as in the preceding paragraph. Then we can make a substructure of $\mathfrak{B}$ with universe A. In fact there is only one way to do this. The universe is A, each predicate parameter P is assigned the restriction of $P^{\mathfrak{B}}$ to A, and similarly for the function symbols. As an extreme case, if the language has no function symbols at all (not even constant symbols), then we can make a substructure out of *any* nonempty subset A of $|\mathfrak{B}|$.

These are basically algebraic concepts, but the following theorem relates them to the logical concepts of truth and satisfaction.

Homomorphism Theorem Let h be a homomorphism of $\mathfrak{A}$ into $\mathfrak{B}$, and let s map the set of variables into $|\mathfrak{A}|$.

(a) For any term t, we have $h(\overline{s}(t)) = \overline{h \circ s}(t)$, where $\overline{s}(t)$ is computed in $\mathfrak{A}$ and $\overline{h \circ s}(t)$ is computed in $\mathfrak{B}$.

(b) For any quantifier-free formula α not containing the equality symbol,

$$\models_{\mathfrak{A}} \alpha[s] \quad \text{iff} \quad \models_{\mathfrak{B}} \alpha[h \circ s].$$

(c) If h is one-to-one (i.e., is an isomorphism of $\mathfrak{A}$ into $\mathfrak{B}$), then in part (b) we may delete the restriction "not containing the equality symbol."

(d) If h is a homomorphism of $\mathfrak{A}$ *onto* $\mathfrak{B}$, then in (b) we may delete the restriction "quantifier-free."

Proof. Part (a) uses induction on t; see Exercise 13. Note that $h \circ s$ maps the set of variables into $|\mathfrak{B}|$; its extension to the set of all terms is $\overline{h \circ s}$. It is $\overline{h \circ s}$ that is here being evaluated at t.

(b) For an atomic formula such as Pt, we have

$$\begin{aligned} \models_{\mathfrak{A}} Pt[s] &\Leftrightarrow \overline{s}(t) \in P^{\mathfrak{A}} \\ &\Leftrightarrow h(\overline{s}(t)) \in P^{\mathfrak{B}} \quad \text{since } h \text{ is a homomorphism} \\ &\Leftrightarrow \overline{h \circ s}(t) \in P^{\mathfrak{B}} \quad \text{by (a)} \\ &\Leftrightarrow \models_{\mathfrak{B}} Pt[h \circ s]. \end{aligned}$$

An inductive argument is then required to handle the connective symbols $\neg$ and $\rightarrow$, but it is completely routine.

(c) In any case,

$$\begin{aligned} \models_{\mathfrak{A}} u = t[s] &\Leftrightarrow \overline{s}(u) = \overline{s}(t) \\ &\Rightarrow h(\overline{s}(u)) = h(\overline{s}(t)) \\ &\Leftrightarrow \overline{h \circ s}(u) = \overline{h \circ s}(t) \quad \text{by (a)} \\ &\Leftrightarrow \models_{\mathfrak{B}} u = t[h \circ s]. \end{aligned}$$

If h is one-to-one, the arrow in the second step can be reversed.

(d) We must extend the routine inductive argument of part (b) to include the quantifier step. That is, we must show that if φ has the property that for every s,

$$\models_{\mathfrak{A}} \varphi[s] \Leftrightarrow \models_{\mathfrak{B}} \varphi[h \circ s],$$

then $\forall x\, \varphi$ enjoys the same property. We have in any case (as a consequence of the inductive hypothesis on φ) the implication

$$\models_{\mathfrak{B}} \forall x\, \varphi[h \circ s] \Rightarrow \models_{\mathfrak{A}} \forall x\, \varphi[s].$$

This is intuitively very plausible; if φ is true of everything in the larger set $|\mathfrak{B}|$, then *a fortiori* it is true of everything in the smaller set ran h. The details are, for an element a of $|\mathfrak{A}|$,

$$\begin{aligned} \models_{\mathfrak{B}} \forall x\, \varphi[h \circ s] &\Rightarrow \models_{\mathfrak{B}} \varphi[(h \circ s)(x \mid h(a))] \\ &\Leftrightarrow \models_{\mathfrak{B}} \varphi[h \circ (s(x \mid a))], && \text{the functions being the same} \\ &\Leftrightarrow \models_{\mathfrak{A}} \varphi[s(x \mid a)] && \text{by the inductive hypothesis.} \end{aligned}$$

Now for the converse, suppose that $\not\models_{\mathfrak{B}} \forall x\, \varphi[h \circ s]$, so that $\models_{\mathfrak{B}} \neg\varphi[(h \circ s)(x \mid b)]$ for some element b in $|\mathfrak{B}|$. We need the implication

(∗) *If* for some b in $|\mathfrak{B}|$, $\models_{\mathfrak{B}} \neg\varphi[(h \circ s)(x \mid b)]$, *then* for some a in $|\mathfrak{A}|$, $\models_{\mathfrak{B}} \neg\varphi[(h \circ s)(s \mid h(a))]$.

For given (∗), we can proceed:

$$\begin{aligned} \models_{\mathfrak{B}} \neg\varphi[(h \circ s)(x \mid h(a))] &\Leftrightarrow \models_{\mathfrak{B}} \neg\varphi[h \circ (s(x \mid a))], && \text{the functions being the same} \\ &\Leftrightarrow \models_{\mathfrak{A}} \neg\varphi[s(x \mid a)] && \text{by the inductive hypothesis} \\ &\Rightarrow \not\models_{\mathfrak{A}} \forall x\, \varphi[s]. \end{aligned}$$

If h maps $|\mathfrak{A}|$ *onto* $|\mathfrak{B}|$, then (∗) is immediate; we take a such that $b = h(a)$. (But there might be other fortunate times when (∗) can be asserted even if h fails to have range $|\mathfrak{B}|$.) ⊣

Two structures $\mathfrak{A}$ and $\mathfrak{B}$ for the language are said to be *elementarily equivalent* (written $\mathfrak{A} \equiv \mathfrak{B}$) iff for any sentence σ,

$$\models_{\mathfrak{A}} \sigma \Leftrightarrow \models_{\mathfrak{B}} \sigma.$$

Corollary 22D Isomorphic structures are elementarily equivalent:

$$\mathfrak{A} \cong \mathfrak{B} \Rightarrow \mathfrak{A} \equiv \mathfrak{B}$$

Actually more is true. Isomorphic structures are alike in every "structural" way; not only do they satisfy the same first-order sentences, they also satisfy the same second-order (and higher) sentences (i.e., they are secondarily equivalent and more).

There are elementarily equivalent structures that are not isomorphic. For example, it can be shown that the structure $(\mathbb{R}; <_R)$ consisting of the set of real numbers with its usual ordering relation is elementarily equivalent to the structure $(\mathbb{Q}; <_Q)$ consisting of the set of rational numbers with its ordering (see Section 2.6). But $\mathbb{Q}$ is a countable set whereas $\mathbb{R}$ is not, so these structures cannot be isomorphic. In Section 2.6 we will see how easy it is to make elementarily equivalent structures of differing cardinalities.

Example, revisited. We had an isomorphism h from $(\mathbb{P}; <_P)$ onto $(\mathbb{N}; <_N)$. So in particular, $(\mathbb{P}; <_P) \equiv (\mathbb{N}; <_N)$; these structures are indistinguishable by first-order sentences.

We furthermore noted that the identity map was an isomorphic embedding of $(\mathbb{P}; <_P)$ into $(\mathbb{N}; <_N)$. Hence for a function s: $V \to \mathbb{P}$ and a quantifier-free φ,

$$\models_{(\mathbb{P}; <_P)} \varphi[s] \Leftrightarrow \models_{(\mathbb{N}; <_N)} \varphi[s].$$

This equivalence may fail if φ contains quantifiers. For example,

$$\models_{(\mathbb{P}; <_P)} \forall \mathbf{v}_2(\mathbf{v}_1 \neq \mathbf{v}_2 \to \mathbf{v}_1 < \mathbf{v}_2)[\![1]\!],$$

but

$$\not\models_{(\mathbb{N}; <_N)} \forall \mathbf{v}_2(\mathbf{v}_1 \neq \mathbf{v}_2 \to \mathbf{v}_1 < \mathbf{v}_2)[\![1]\!].$$

An *automorphism* of the structure $\mathfrak{A}$ is an isomorphism of $\mathfrak{A}$ onto $\mathfrak{A}$. The identity function on $|\mathfrak{A}|$ is trivially an automorphism of $\mathfrak{A}$. $\mathfrak{A}$ may or may not have nontrivial automorphisms. (We say that $\mathfrak{A}$ is *rigid* if the identity function is its only automorphism.) As a consequence of the homomorphism theorem, we can show that an automorphism must preserve the definable relations:

Corollary 22E Let h be an automorphism of the structure $\mathfrak{A}$, and let R be an n-ary relation on $|\mathfrak{A}|$ definable in $\mathfrak{A}$. Then for any $a_1, \ldots, a_n$ in $|\mathfrak{A}|$,

$$\langle a_1, \ldots, a_n \rangle \in R \;\Leftrightarrow\; \langle h(a_1), \ldots, h(a_n) \rangle \in R.$$

Proof. Let φ be a formula that defines R in $\mathfrak{A}$. We need to know that

$$\models_{\mathfrak{A}} \varphi[\![a_1, \ldots, a_n]\!] \Leftrightarrow \models_{\mathfrak{A}} \varphi[\![h(a_1), \ldots, h(a_n)]\!].$$

But this is immediate from the homomorphism theorem. ⊣

This corollary is sometimes useful in showing that a given relation is *not* definable. Consider, for example, the structure $(\mathbb{R}; <)$ consisting of the set of real numbers with its usual ordering. An automorphism of this structure is simply a function h from $\mathbb{R}$ onto $\mathbb{R}$ that is strictly increasing:

$$a < b \Leftrightarrow h(a) < h(b).$$

One such automorphism is the function h for which $h(a) = a^3$. Since this function maps points outside of $\mathbb{N}$ into $\mathbb{N}$, the set $\mathbb{N}$ is not definable in this structure.

Another example is provided by elementary algebra books, which sometimes explain that the length of a vector in the plane cannot be defined in terms of vector addition and scalar multiplication. For the map that takes a vector $\mathbf{x}$ into the vector $2\mathbf{x}$ is an automorphism of the plane with respect to vector addition and scalar multiplication, but it is not length-preserving. From our viewpoint, the structure in question,

$$(E; +, f_r)_{r \in \mathbb{R}},$$

has for its universe the plane E, has the binary operation $+$ of vector addition, and has (for each r in the set $\mathbb{R}$) the unary operation f_r of scalar multiplication by r. (Thus the language in question has a one-place function symbol for each real number.) The doubling map described above is an automorphism of this structure. But it does not preserve the set of unit vectors,

$$\{\mathbf{x} \mid \mathbf{x} \in E \text{ and } \mathbf{x} \text{ has length } 1\}.$$

So this set cannot be definable in the structure. (Incidentally, the homomorphisms of vector spaces are called *linear transformations*.)

Exercises

1. Show that (a) $\Gamma; \alpha \models \varphi$ iff $\Gamma \models (\alpha \to \varphi)$; and (b) $\varphi \models\!\!\!=\!\!\!| \; \psi$ iff $\models (\varphi \leftrightarrow \psi)$.

2. Show that no one of the following sentences is logically implied by the other two. (This is done by giving a structure in which the sentence in question is false, while the other two are true.)
   (a) $\forall x \forall y \forall z (Pxy \to Pyz \to Pxz)$. Recall that by our convention $\alpha \to \beta \to \gamma$ is $\alpha \to (\beta \to \gamma)$.
   (b) $\forall x \forall y (Pxy \to Pyx \to x = y)$.
   (c) $\forall x \exists y\, Pxy \to \exists y \forall x\, Pxy$.

3. Show that

$$\{\forall x(\alpha \to \beta), \forall x\, \alpha\} \models \forall x\, \beta.$$

4. Show that if x does not occur free in α, then $\alpha \models \forall x\, \alpha$.

5. Show that the formula $x = y \to Pzfx \to Pzfy$ (where f is a one-place function symbol and P is a two-place predicate symbol) is valid.

6. Show that a formula θ is valid iff $\forall x\, \theta$ is valid.

7. Restate the definition of "$\mathfrak{A}$ satisfies φ with s" in the way described

on page 84. That is, define by recursion a function $\overline{h}$ such that $\mathfrak{A}$ satisfies φ with s iff $s \in \overline{h}(\varphi)$.

8. Assume that Σ is a set of sentences such that for any sentence τ, either $\Sigma \models \tau$ or $\Sigma \models \neg\tau$. Assume that $\mathfrak{A}$ is a model of Σ. Show that for any sentence τ, we have $\models_{\mathfrak{A}} \tau$ iff $\Sigma \models \tau$.
9. Assume that the language has equality and a two-place predicate symbol P. For each of the following conditions, find a sentence σ such that the structure $\mathfrak{A}$ is a model of σ iff the condition is met.
   (a) $|\mathfrak{A}|$ has exactly two members.
   (b) $P^{\mathfrak{A}}$ is a function from $|\mathfrak{A}|$ into $|\mathfrak{A}|$. (A *function* is a single-valued relation, as in Chapter 0. For f to be a function from A into B, the domain of f must be all of A; the range of f is a subset, not necessarily proper, of B.)
   (c) $P^{\mathfrak{A}}$ is a permutation of $|\mathfrak{A}|$; i.e., $P^{\mathfrak{A}}$ is a one-to-one function with domain and range equal to $|\mathfrak{A}|$.
10. Show that

$$\models_{\mathfrak{A}} \forall \mathbf{v}_2\, Q\mathbf{v}_1\mathbf{v}_2[\![c^{\mathfrak{A}}]\!] \quad \text{iff} \quad \models_{\mathfrak{A}} \forall \mathbf{v}_2\, Qc\mathbf{v}_2.$$

   Here Q is a two-place predicate symbol and c is a constant symbol.
11. For each of the following relations, give a formula which defines it in $(\mathbb{N}; +, \cdot)$. (The language is assumed to have equality and the parameters $\forall$, $+$, and $\cdot$).
   (a) $\{0\}$.
   (b) $\{1\}$.
   (c) $\{\langle m, n\rangle \mid n \text{ is the successor of } m \text{ in } N\}$.
   (d) $\{\langle m, n\rangle \mid m < n \text{ in } \mathbb{N}\}$.
   Digression: This is merely the tip of the iceberg. A relation on $\mathbb{N}$ is said to be *arithmetical* if it is definable in this structure. All decidable relations are arithmetical, as are many others. The arithmetical relations can be arranged in a hierarchy; see Section 3.5.
12. Let $\mathfrak{R}$ be the structure $(\mathbb{R}; +, \cdot)$. (The language is assumed to have equality and the parameters $\forall$, $+$, and $\cdot$. $\mathfrak{R}$ is the structure whose universe is the set $\mathbb{R}$ of real numbers and such that $+^{\mathfrak{R}}$ and $\cdot^{\mathfrak{R}}$ are the usual addition and multiplication operations.)
   (a) Give a formula that defines in $\mathfrak{R}$ the interval $[0, \infty)$.
   (b) Give a formula that defines in $\mathfrak{R}$ the set $\{2\}$.
   *(c) Show that any finite union of intervals, the endpoints of which are algebraic, is definable in $\mathfrak{R}$. (The converse is also true; these are the only definable sets in the structure. But we will not prove this fact.)
13. **Prove part (a) of the homomorphism theorem.**

14. What subsets of the real line $\mathbb{R}$ are definable in $(\mathbb{R}; <)$? What subsets of the plane $\mathbb{R} \times \mathbb{R}$ are definable in $(\mathbb{R}; <)$?

    Remarks: The nice thing about $(\mathbb{R}; <)$ is that its automorphisms are exactly the order-preserving maps from $\mathbb{R}$ onto itself. But stop after the binary relations. There are 2^{13} definable ternary relations, so you do not want to catalog all of them.

15. Show that the addition relation, $\{\langle m, n, p\rangle \mid p = m + n\}$, is not definable in $(\mathbb{N}; \cdot)$. *Suggestion*: Consider an automorphism of $(\mathbb{N}; \cdot)$ that switches two primes.

    Digression: Algebraically, the structure of the natural numbers with multiplication is nothing but the free Abelian semigroup with $\aleph_0$ generators (viz. the primes), together with a zero element. There is no way you could define addition here. If you could define addition, then you could define ordering (by Exercise 11 and the natural transitivity statement). But one generator looks just like another. That is, there are $2^{\aleph_0}$ automorphisms — simply permute the primes. None of them is order-preserving except the identity.

16. Give a sentence having models of size $2n$ for every positive integer n, but no finite models of odd size. (Here the language should include equality and will have whatever parameters you choose.) *Suggestion*: One method is to make a sentence that says, "Everything is either red or blue, and f is a color-reversing permutation."

    Remark: Given a sentence σ, it might have some finite models (i.e., models with finite universes). Define the *spectrum* of σ to be the set of positive integers n such that σ has a model of size n. This exercise shows that the set of even numbers is a spectrum.

    For example if σ is the conjunction of the field axioms (there are only finitely many, so we can take their conjunction), then its spectrum is the set of powers of primes. This fact is proved in any course on finite fields. The spectrum of $\neg\,\sigma$, by contrast, is the set of all positive integers (non-fields come in all sizes).

    Günter Asser in 1955 raised the question: Is the complement of every spectrum a spectrum? Once you realize that simply taking a negation does not work (cf. the preceding paragraph), you see that this is a nontrivial question. In fact the problem, known as the spectrum problem, is still open. But modern work has tied it to another open problem, whether or not co-NP = NP.

17. (a) Consider a language with equality whose only parameter (aside from $\forall$) is a two-place predicate symbol P. Show that if $\mathfrak{A}$ is finite and $\mathfrak{A} \equiv \mathfrak{B}$, then $\mathfrak{A}$ is isomorphic to $\mathfrak{B}$. *Suggestion*: Suppose the universe of $\mathfrak{A}$ has size n. Make a single sentence σ of the form $\exists\, v_1 \cdots \exists\, v_n\, \theta$ that describes $\mathfrak{A}$ "completely." That is, on the one hand, σ must be true in $\mathfrak{A}$. And on the other hand, any model of σ must be exactly like (i.e., isomorphic to) $\mathfrak{A}$.

*(b) Show that the result of part (a) holds regardless of what parameters the language contains.

18. A universal ($\forall_1$) formula is one of the form $\forall x_1 \cdots \forall x_n\, \theta$, where θ is quantifier-free. An existential ($\exists_1$) formula is of the dual form $\exists x_1 \cdots \exists x_n\, \theta$. Let $\mathfrak{A}$ be a substructure of $\mathfrak{B}$, and let $s : V \to |\mathfrak{A}|$.
   (a) Show that if $\models_{\mathfrak{A}} \psi[s]$ and ψ is existential, then $\models_{\mathfrak{B}} \psi[s]$. And if $\models_{\mathfrak{B}} \varphi[s]$ and φ is universal, then $\models_{\mathfrak{A}} \varphi[s]$.
   (b) Conclude that the sentence $\exists x\ Px$ is not logically equivalent to any universal sentence, nor $\forall x\ Px$ to any existential sentence.
   Remark: Part (a) says (when φ is a sentence) that any universal sentence is "preserved under substructures." Being universal is a syntactic property — it has to do with the string of symbols. In contrast, being preserved under substructures is a semantic property — it has to do with satisfaction in structures. But this semantic property captures the syntactic property up to logical equivalence (which is all one could ask for). That is, if σ is a sentence that is always preserved under substructures, then σ is logically equivalent to a universal sentence. (This fact is due to Łoś and Tarski.)

19. An $\exists_2$ formula is one of the form $\exists x_1 \cdots \exists x_n\, \theta$, where θ is universal.
   (a) Show that if an $\exists_2$ sentence in a language not containing function symbols (not even constant symbols) is true in $\mathfrak{A}$, then it is true in some finite substructure of $\mathfrak{A}$.
   (b) Conclude that $\forall x \exists y\ Pxy$ is not logically equivalent to any $\exists_2$ sentence.

20. Assume the language has equality and a two-place predicate symbol P. Consider the two structures $(\mathbb{N}; <)$ and $(\mathbb{R}; <)$ for the language.
   (a) Find a sentence true in one structure and false in the other.
   *(b) Show that any $\exists_2$ sentence (as defined in the preceding exercise) true in $(\mathbb{R}; <)$ is also true in $(\mathbb{N}; <)$. *Suggestion*: First, for any finite set of real numbers, there is an automorphism of $(\mathbb{R}; <)$ taking those real numbers to natural numbers. Secondly, by Exercise 18, universal formulas are preserved under substructures.

21. We could consider enriching the language by the addition of a new quantifier. The formula $\exists! x\, \alpha$ (read "there exists a unique x such that α") is to be satisfied in $\mathfrak{A}$ by s iff there is one and only one $a \in |\mathfrak{A}|$ such that $\models_{\mathfrak{A}} \alpha[s(x \mid a)]$. Assume that the language has the equality symbol and show that this apparent enrichment comes to naught, in the sense that we can find an ordinary formula logically equivalent to $\exists! x\, \alpha$.

22. Assume that $\mathfrak{A}$ is a structure and h is a function with $\operatorname{ran} h = |\mathfrak{A}|$.

Show that there is a structure $\mathfrak{B}$ such that h is a homomorphism of $\mathfrak{B}$ onto $\mathfrak{A}$. *Suggestion*: We need to take $|\mathfrak{B}| = \operatorname{dom} h$. In general, the axiom of choice will be needed to define the functions in $\mathfrak{B}$, unless h is one-to-one.

Remark: The result yields an "upward Löwenheim–Skolem theorem without equality" (cf. Section 2.6). That is, any structure $\mathfrak{A}$ has an extension to a structure $\mathfrak{B}$ of any higher cardinality such that $\mathfrak{A}$ and $\mathfrak{B}$ are elementarily equivalent, except for equality. There is nothing deep about this. Not until you add equality.

23. Let $\mathfrak{A}$ be a structure and g a one-to-one function with $\operatorname{dom} g = |\mathfrak{A}|$. Show that there is a unique structure $\mathfrak{B}$ such that g is an isomorphism of $\mathfrak{A}$ onto $\mathfrak{B}$.

24. Let h be an isomorphic embedding of $\mathfrak{A}$ into $\mathfrak{B}$. Show that there is a structure $\mathfrak{C}$ isomorphic to $\mathfrak{B}$ such that $\mathfrak{A}$ is a substructure of $\mathfrak{C}$. *Suggestion*: Let g be a one-to-one function with domain $|\mathfrak{B}|$ such that $g(h(a)) = a$ for $a \in |\mathfrak{A}|$. Form $\mathfrak{C}$ such that g is an isomorphism of $\mathfrak{B}$ onto $\mathfrak{C}$.

    Remark: The result stated in this exercise should not seem surprising. On the contrary, it is one of those statements that is obvious until you have to prove it. It says that if you can embed $\mathfrak{A}$ isomorphically into $\mathfrak{B}$, then for all practical purposes you can pretend $\mathfrak{A}$ is a substructure of $\mathfrak{B}$.

25. Consider a fixed structure $\mathfrak{A}$. Expand the language by adding a new constant symbol c_a for each $a \in |\mathfrak{A}|$. Let $\mathfrak{A}^+$ be the structure for this expanded language that agrees with $\mathfrak{A}$ on the original parameters and that assigns to c_a the point a. A relation R on $|\mathfrak{A}|$ is said to be *definable from points* in $\mathfrak{A}$ iff R is definable in $\mathfrak{A}^+$. (This differs from ordinary definability only in that we now have parameters in the language for members of $|\mathfrak{A}|$.) Let $\mathfrak{R} = (\mathbb{R}; <, +, \cdot)$.
    (a) Show that if A is a subset of $\mathbb{R}$ consisting of the union of finitely many intervals, then A is definable from points in $\mathfrak{R}$ (cf. Exercise 12).
    (b) Assume that $\mathfrak{A} \equiv \mathfrak{R}$. Show that any subset of $|\mathfrak{A}|$ that is nonempty, bounded (in the ordering $<^{\mathfrak{A}}$), and definable from points in $\mathfrak{A}$ has a least upper bound in $|\mathfrak{A}|$.

    Digression: Often when people speak of definability within a structure, this is the concept they mean. The more standard phrase is "definable from parameters"; here "points" is used because the word "parameter" is used in a different sense in this chapter.

    The real ordered field can be characterized up to isomorphism by saying that it is a complete ordered field. (This fact should be included in any analysis course.) But completeness (i.e., that nonempty bounded sets have least upper bounds) is not a first-order property. See Example 4 in Section 4.1 for its second-order statement. The first-order "image" of completeness is given by the schema obtained from that second-order statement by replacing $\boldsymbol{X}$ by a first-order formula φ. The resulting schema (i.e., the set of sentences you get by letting φ vary and taking universal closure) says that the least-upper-bound property holds for the sets that are definable from points. Ordered fields satisfying those sentences are called "real closed-ordered fields."

The surprising fact is that such fields were not invented by logicians. They were previously studied by algebraists and you can read about them in van der Waerden's *Modern Algebra* book (volume I). Of course, he uses a characterization of them that does not involve logic.

What Tarski showed is that any real closed-ordered field is elementarily equivalent to the field of real numbers. From this it follows that the theory of the real-ordered field is decidable.

26. (a) Consider a fixed structure $\mathfrak{A}$ and define its *elementary type* to be the class of structures elementarily equivalent to $\mathfrak{A}$. Show that this class is EC_Δ. *Suggestion*: Show it is $\mathrm{Mod\,Th}\,\mathfrak{A}$.
    (b) Call a class $\mathcal{K}$ of structures *elementarily closed* or ECL if whenever a structure belongs to $\mathcal{K}$ then all elementarily equivalent structures also belong. Show that any such class is a union of EC_Δ classes. (A class that is a union of EC_Δ classes is said to be an $\mathrm{EC}_{\Delta\Sigma}$ class; this notation is derived from topology.)
    (c) Conversely, show that any class that is the union of EC_Δ classes is elementarily closed.
27. Assume that the parameters of the language are $\forall$ and a two-place predicate symbol P. List all of the non-isomorphic structures of size 2. That is, give a list of structures (where the universe of each has size 2) such that any structure of size 2 is isomorphic to exactly one structure on the list.
28. For each of the following pairs of structures, show that they are not elementarily equivalent, by giving a sentence true in one and false in the other. (The language here contains $\forall$ and a two-place function symbol $\circ$.)
    (a) $(\mathbb{R}; \times)$ and $(\mathbb{R}^*; \times^*)$, where $\times$ is the usual multiplication operation on the real numbers, $\mathbb{R}^*$ is the set of non-zero reals, and $\times^*$ is $\times$ restricted to the non-zero reals.
    (b) $(\mathbb{N}; +)$ and $(\mathbb{P}; +^*)$, where $\mathbb{P}$ is the set of positive integers, and $+^*$ is usual addition operation restricted to $\mathbb{P}$.
    (c) Better yet, for each of the four structures of parts (a) and (b), give a sentence true in that structure and false in the other three.