

7.5 Definability and Isomorphism

A sentence is true or false in a structure. A formula with one free variable is different: it is true of some elements of a structure and false of others, so it picks out a set. In $(\mathbb{N}; +)$ the formula $\exists y (x = y + y)$ is true of $0, 2, 4, \dots$ and false of the odd numbers, so it picks out the even numbers, although the structure has no symbol for “even”. This section asks which sets a structure’s language can pick out. Its first half writes formulas for sets: points, intervals, orders, the primes, a supremum. Its second half, for a second reading, asks why some sets cannot be picked out at all, and answers with a map that moves the elements of a structure without changing anything a formula can see.

Remark (Looking back). Section 4.9 asked what the connectives can say, and answered: every truth function, by a normal form. This section asks the same question of a first-order language inside one structure. There the answer was “everything”; here it depends on the structure, and a set that one structure’s formulas define, another’s cannot.

7.5.1 Formulas define sets

A formula defines the set of elements (or tuples of elements) that make it true.

Definition 7.5.1. Definable Set

Let $\mathfrak{M}$ be a structure with domain D , and φ a formula whose free variables are among $x_1, \dots, x_n$, all different. The set **defined by** φ in $\mathfrak{M}$ is

$$\{(d_1, \dots, d_n) \in D^n : \mathfrak{M}, \ell[x_1 \mapsto d_1] \cdots [x_n \mapsto d_n] \models \varphi\},$$

for any assignment ℓ . A set $S \subseteq D^n$ is **definable** in $\mathfrak{M}$ if some formula defines it.

By Lemma 7.1.1 the set does not depend on ℓ : the assignments $\ell[x_1 \mapsto d_1] \cdots [x_n \mapsto d_n]$, for different ℓ , agree on $x_1, \dots, x_n$, and only the values of the free variables matter. For $n = 1$ the set is a set of elements, and we write it in set-builder form, $\{x \in D : \varphi\}$. Set-builder notation, used since school, is exactly this: the reading of a formula in a structure.

Two remarks on the definition. The structure is part of the question: the same formula defines different sets in different structures, and a set is definable **in** $\mathfrak{M}$, never definable outright. And the formula may use only the symbols of $\mathfrak{M}$: to define a set in $(\mathbb{N}; +)$ we may write $+$, $=$, connectives and quantifiers, and nothing else, not even 0 or $<$.

The connectives act on defined sets as the set operations do. If φ and ψ define S and T (with the same free variable x), then by (S4) and (S5) the formula $\varphi \wedge \psi$ defines $S \cap T$, $\varphi \vee \psi$ defines $S \cup T$, and $\neg\varphi$ defines $D \setminus S$, the elements not in S . So the definable sets of a structure are closed under intersection, union and complement, and a set built from definable sets by these operations is definable without further work.

Example. Sets Defined by Formulas

Each formula is read back in words.

- (a) In $(\mathbb{R}; +, \cdot)$, the formula $\exists y (x = y \cdot y)$, “ x is a square”, defines $[0, \infty)$: a real number is

the square of a real number exactly when it is non-negative.

- (b) In $(\mathbb{N}; +)$, the formula $x + x = x$, “ x added to itself gives itself”, defines $\{0\}$, since $d + d = d$ forces $d = 0$. The formula $\exists z (\neg(z + z = z) \wedge x + z = y)$, “ y is x plus something non-zero”, defines the set of pairs (d, e) with $d < e$.
- (c) In $(\mathbb{N}; \cdot)$, write $U(x)$ for the formula $\forall y (x \cdot y = y)$, “multiplying by x changes nothing”. It defines $\{1\}$: at $x = 0$ the instance $y = 1$ fails, since $0 \cdot 1 = 0$; at $x \geq 2$ the instance $y = 1$ fails too, since $x \cdot 1 = x \neq 1$; and at $x = 1$ every instance holds.
- (d) In $(\mathbb{N}; \cdot)$, the formula

$$\neg U(x) \wedge \forall y \forall z (y \cdot z = x \rightarrow (U(y) \vee U(z))),$$

“ x is not 1, and whenever x is a product, one factor is 1”, defines the primes. At $x = 0$ the instance $y = z = 0$ fails ($0 \cdot 0 = 0$, and neither factor is 1); at $x = 1$ the first conjunct fails; at a composite $x = yz$ with $y, z \geq 2$ the instance at that y, z fails; at a prime, every factorization has a factor 1.

Each definition builds on the last: 0 and 1 are not symbols of these structures, yet the language can name them, and once 1 is defined, “prime” can be written with it. In (d), $U(y)$ is the formula $U(x)$ with y for x and its bound y renamed, say $\forall w (y \cdot w = w)$, so that the substituted letter is not captured.

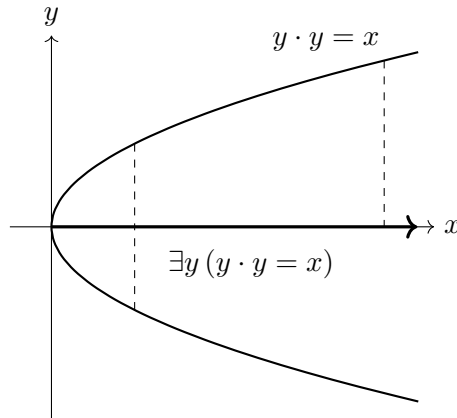
To check that a formula defines a given set, check two directions, as for any equality of sets: every element of the set satisfies the formula, and every element that satisfies the formula is in the set. In (d) the cases $x = 0$, $x = 1$ and “ x composite” are the second direction, and “at a prime” is the first. Leave out a case and a definition can be wrong at one point. Delete the conjunct $\neg U(x)$ from (d): at $x = 1$ every factorization $y \cdot z = 1$ has $y = z = 1$, so the remaining formula is true of 1, and it defines the primes together with 1. Exactly one element changed sides.

Quick check. What does $\exists y (x = y + y)$ define in $(\mathbb{Z}; +)$? In $(\mathbb{Q}; +)$?

Solution. In $(\mathbb{Z}; +)$, the even integers. In $(\mathbb{Q}; +)$, all of $\mathbb{Q}$: every rational x is $y + y$ for $y = x/2$, which is again rational. Same formula, two structures, two sets.

7.5.2 $\exists$ is a projection

A formula with two free variables defines a set of pairs, and a set of pairs of reals can be drawn. In $(\mathbb{R}; \cdot)$, the formula $y \cdot y = x$ defines $\{(d, e) : e^2 = d\}$, a parabola lying on its side. The formula $\exists y (y \cdot y = x)$ has the one free variable x , and by (S7) it is true of d exactly when some e puts the point (d, e) on the parabola. So it defines the set of first coordinates of the points of the parabola: its **shadow** on the x -axis, $[0, \infty)$.



The dashed segments drop two points, $(1, 1)$ and $(1, -1)$, and the point $(4, 2)$, onto their shadows 1 and 4. No point of the parabola lies above a negative x , so no negative number is in the shadow.

In general, $\exists y \varphi$ defines the **projection** of the set that φ defines: d is in it exactly when some e puts (d, e) in φ 's set, by (S7). Dually, $\forall y \varphi$ keeps the d whose whole vertical line lies in φ 's set, by (S6). This is the picture behind every $\exists$ in a definition: to show a set definable, it is often easiest to describe a set of pairs and project.

The two readings are tied by negation. By (S4), (S6) and (S7), $\forall y \varphi$ is satisfied exactly when $\exists y \neg \varphi$ is not, so the set defined by $\forall y \varphi$ is the complement of the projection of the complement of φ 's set: remove φ 's set from the plane, take the shadow of what is left, and keep the points of the axis that are not in that shadow.

Quick check. In $(\mathbb{R}; \leq, \cdot)$, which set does $\forall y (x \leq y \cdot y)$ define?

Solution. $(-\infty, 0]$. The least value of $y \cdot y$ is 0, at $y = 0$, so $x \leq y^2$ holds for every y exactly when $x \leq 0$. In the picture: the vertical line at x lies wholly in the region $x \leq y^2$ when $x \leq 0$, and the line at a positive x leaves it near $y = 0$.

7.5.3 Define it by a formula

A common task in mathematics is to turn a notion described in words into a formula, and the skill is the reverse of reading back. The notion must be said using only the symbols of the structure, and every variable that is not the defined set's own must be bound.

Example. Maximum, Maximal, Supremum

- (a) In a structure with one two-place symbol $\leq$ read as a partial order: “ x is a **greatest** element” is $\forall y (y \leq x)$, “everything is below x ”. “ x is a **maximal** element” is $\forall y (x \leq y \rightarrow y = x)$, “nothing is above x except x itself”. In the divisibility order on $\{1, 2, 3\}$ ($d \leq e$ when d divides e), 2 and 3 are maximal, and there is no greatest element, since 2 does not divide 3 nor 3 divide 2. On $\{1, 2, 3, 6\}$, 6 is both maximal and greatest.
- (b) Add a one-place symbol A for a set of reals, and work in $(\mathbb{R}; \leq, A)$. “ x is an upper bound of A ” is the formula $B(x)$: $\forall y (A(y) \rightarrow y \leq x)$, “every element of A is at most x ”. “ x is the supremum of A ” is $B(x) \wedge \forall z (B(z) \rightarrow x \leq z)$, “ x is an upper bound, and below every upper bound”. For $A = [0, 1)$, the supremum is 1: it is an upper bound,

and any $z < 1$ is exceeded by an element of $[0, 1)$, such as the larger of 0 and $(z + 1)/2$, so z is not one. No element of A is greatest.

- (c) “ A has a greatest element” is the sentence $\exists x (A(x) \wedge B(x))$, “some element of A is an upper bound of A ”. It is false for $A = [0, 1)$ and true for $A = [0, 1]$.

In (c) the formula $B(x)$ is used inside a larger formula, as a word is used in a sentence. This is how definitions accumulate: each defined notion is an abbreviation, and the full formula is the abbreviation written out.

Defining a notion goes in three steps. First, say the notion in words that use only the structure’s symbols: “upper bound” becomes “every element of A is at most x ”. Second, write each auxiliary notion as a formula with its own free variable, and substitute it where it is used, renaming bound variables so that nothing is captured. Third, check both directions on a small case. The commonest slip is a variable left free. Written without its $\forall y$, the formula $A(y) \rightarrow y \leq x$ has two free variables and defines a set of **pairs**, those (d, e) with $d \notin A$ or $d \leq e$; it is not a property of x at all.

A defined notion can also be given its own symbol, as “even” and “the supremum of A ” are in ordinary mathematics. Section 5.8 showed (Proposition 5.8.2) that such a definition is safe: introducing a predicate symbol by $\forall x (P(x) \leftrightarrow \varphi)$, or a constant for an element that φ is proved to have, proves nothing new about the old symbols. Definability says which notions can be so introduced in a given structure: exactly those some formula of its language defines.

Warning. Greatest is not maximal. A maximal element has nothing strictly above it; a greatest element is above everything. In the divisibility order on $\{1, 2, 3\}$, 2 is maximal and not greatest. Writing $\forall y (y < x)$ for “maximal” defines the wrong set: in that order it defines $\emptyset$, while the maximal elements are 2 and 3.

Quick check. In the divisibility order on $\{1, 2, 3, 4, 6\}$, which elements are maximal? Is there a greatest element?

Solution. 4 and 6: neither divides any other element of the set. There is no greatest element: 4 does not divide 6, and 6 does not divide 4.

7.5.4 Isomorphic structures (second pass)

This half of the section is for a second reading. It asks when two structures are the same except for the names of their elements, and proves that such structures satisfy the same sentences. From that comes a way to show that a set is **not** definable. It uses functions and bijections in their everyday sense: a rule that sends each element to one element, and, for a bijection, one that matches the two domains one to one, every element of the second domain hit exactly once.

Definition 7.5.2. Isomorphism of Structures

Let $\mathfrak{M}$ and $\mathfrak{N}$ be structures for the same symbols, with domains D and E . An **isomorphism** $h: \mathfrak{M} \rightarrow \mathfrak{N}$ is a bijection $h: D \rightarrow E$ such that

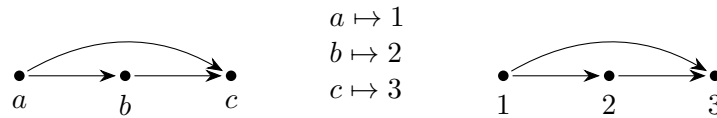
- (i) $h(c^{\mathfrak{M}}) = c^{\mathfrak{N}}$ for each constant c ;
- (ii) $h(f^{\mathfrak{M}}(d_1, \dots, d_n)) = f^{\mathfrak{N}}(h(d_1), \dots, h(d_n))$ for each function symbol f of arity n and all $d_1, \dots, d_n \in D$;
- (iii) $(d_1, \dots, d_n) \in R^{\mathfrak{M}}$ if and only if $(h(d_1), \dots, h(d_n)) \in R^{\mathfrak{N}}$, for each predicate symbol R of arity n and all $d_1, \dots, d_n \in D$.

An isomorphism $\mathfrak{M} \rightarrow \mathfrak{N}$ is an **automorphism** of $\mathfrak{M}$. $\mathfrak{M}$ and $\mathfrak{N}$ are **isomorphic** if an isomorphism $\mathfrak{M} \rightarrow \mathfrak{N}$ exists.

In words: h renames every element, and the renaming carries each constant to the corresponding constant, each operation to the corresponding operation, and each relation onto the corresponding relation, in both directions.

Clause (iii) is needed in both directions. The identity map $1 \mapsto 1, 2 \mapsto 2$, from $\{1, 2\}$ with R empty to $\{1, 2\}$ with $R = \{(1, 2)\}$, is a bijection, and it sends every pair in the first relation into the second, since there are none. Yet the sentence $\exists x \exists y R(x, y)$ is false in the first structure and true in the second. The converse half of (iii) fails at $(1, 2)$, and with it the map is not an isomorphism.

Examples. $(\mathbb{N}, <)$ and the even numbers with $<$ are isomorphic, by $h(d) = 2d$: every even number is $2d$ for exactly one d , and $d < e$ if and only if $2d < 2e$. A finite example, with the bijection as a table:



On the left, $\mathfrak{M}$ has $D = \{a, b, c\}$ and $R^{\mathfrak{M}} = \{(a, b), (b, c), (a, c)\}$; on the right is $(\{1, 2, 3\}, <)$, with an arrow from d to e when $d < e$. The table is a bijection, and it sends the three arrows on the left exactly onto the three on the right. A non-example: $d \mapsto d + 1$, from $(\mathbb{N}, <)$ to itself, preserves $<$ in both directions and is one to one, but it is not onto: nothing is sent to 0. So it is not an automorphism.

Theorem 7.5.1. Isomorphic Structures Satisfy the Same Sentences

Let $h: \mathfrak{M} \rightarrow \mathfrak{N}$ be an isomorphism. For every formula φ and every assignment ℓ in $\mathfrak{M}$,

$$\mathfrak{M}, \ell \models \varphi \quad \text{if and only if} \quad \mathfrak{N}, h \circ \ell \models \varphi,$$

where $h \circ \ell$ gives each variable x the value $h(\ell(x))$. In particular, $\mathfrak{M} \models \sigma$ if and only if $\mathfrak{N} \models \sigma$, for every sentence σ .

In words: renaming the elements, consistently, changes the truth of nothing.

The theorem is most often used backwards: a sentence true in one structure and false in another shows that the two are **not** isomorphic. The sentence $\forall x \exists y (y + y = x)$, “every element is a sum of two equal ones”, is true in $(\mathbb{Q}; +)$ (take $y = x/2$) and false in $(\mathbb{Z}; +)$ (at $x = 1$), so no bijection $\mathbb{Q} \rightarrow \mathbb{Z}$ carries addition to addition, although bijections $\mathbb{Q} \rightarrow \mathbb{Z}$ exist (*Sets, Relations, and Cardinality*, Chapter 3). The converse of the theorem fails: two structures can satisfy the same sentences without being isomorphic, and the optional Section 7.6 meets such a pair.

The proof is in the fold below.

🕒 **Second reading** · *The proof: terms, then formulas*

Idea. An induction on terms and then on formulas, of the kind Section 7.1 gave for Lemma 7.1.1. Each clause of the definition of isomorphism carries one kind of atomic formula across; injectivity carries equations back; and in the quantifier cases, as d runs over D , its image $h(d)$ must run over all of E , which is what “onto” gives.

Proof. Terms. First, $h(t^{\mathfrak{M},\ell}) = t^{\mathfrak{N},h\circ\ell}$ for every term t , by induction on t . For a variable x , both sides are $h(\ell(x))$, by the definition of $h \circ \ell$. For a constant, this is clause (i). For $t = f(t_1, \dots, t_n)$, clause (ii) and the hypothesis for $t_1, \dots, t_n$ give

$$h(f^{\mathfrak{M}}(t_1^{\mathfrak{M},\ell}, \dots, t_n^{\mathfrak{M},\ell})) = f^{\mathfrak{N}}(h(t_1^{\mathfrak{M},\ell}), \dots, h(t_n^{\mathfrak{M},\ell})) = f^{\mathfrak{N}}(t_1^{\mathfrak{N},h\circ\ell}, \dots, t_n^{\mathfrak{N},h\circ\ell}).$$

Formulas. Structural induction on φ , with the claim stated for **all** assignments ℓ at once, since the quantifier clauses change the assignment.

Atomic. By (S1), $\mathfrak{M}, \ell \models R(t_1, \dots, t_n)$ means that the tuple of the values $t_i^{\mathfrak{M},\ell}$ is in $R^{\mathfrak{M}}$. By clause (iii) that holds exactly when the tuple of their images is in $R^{\mathfrak{N}}$, and by the claim for terms the images are the values $t_i^{\mathfrak{N},h\circ\ell}$: this is (S1) for $\mathfrak{N}, h\circ\ell$. *Equations.* $t_1^{\mathfrak{M},\ell} = t_2^{\mathfrak{M},\ell}$ implies $h(t_1^{\mathfrak{M},\ell}) = h(t_2^{\mathfrak{M},\ell})$; the converse holds because h is **injective**. With the claim for terms, this is (S2) on both sides. $\perp$ is satisfied on neither side, by (S3).

Connectives. The answers for φ and ψ agree on the two sides by hypothesis, and (S4), (S5) combine them by the same rule on both sides.

Universal quantifier. $\mathfrak{M}, \ell \models \forall x \varphi$ holds if and only if $\mathfrak{M}, \ell[x \mapsto d] \models \varphi$ for every $d \in D$, by (S6); by the hypothesis, applied to the assignment $\ell[x \mapsto d]$, if and only if $\mathfrak{N}, h\circ(\ell[x \mapsto d]) \models \varphi$ for every $d \in D$. Now $h \circ (\ell[x \mapsto d]) = (h \circ \ell)[x \mapsto h(d)]$: both give x the value $h(d)$ and every other variable y the value $h(\ell(y))$. As d runs over D , $h(d)$ runs over **all** of E , because h is **onto**. So the condition says that $\mathfrak{N}, (h \circ \ell)[x \mapsto e] \models \varphi$ for every $e \in E$, which is (S6) for $\mathfrak{N}, h \circ \ell \models \forall x \varphi$.

Existential quantifier. The same, with (S7): some $d \in D$ works on the left exactly when some $e = h(d) \in E$ works on the right, and every $e \in E$ is such an $h(d)$, since h is **onto**.

For a sentence, Lemma 7.1.1 makes the assignment irrelevant on both sides, which gives the last sentence of the statement. ■

Quick check. Why can no sentence in the symbol $<$ tell $(\mathbb{N}, <)$ from the even numbers with $<$?

Solution. Doubling is an isomorphism between them, so by [Theorem 7.5.1](#) they satisfy the same sentences.

7.5.5 What an automorphism cannot move (second pass)

An automorphism is a renaming of a structure onto itself. By the theorem, a formula cannot tell an element from its image.

Corollary 7.5.2. Automorphisms Preserve Definable Sets

If h is an automorphism of $\mathfrak{M}$ and $S \subseteq D$ is definable in $\mathfrak{M}$, then for every $d \in D$, $d \in S$ if and only if $h(d) \in S$.

Proof. Let φ , with free variable x , define S , and let ℓ be an assignment with $\ell(x) = d$. By [Theorem 7.5.1](#) with $\mathfrak{N} = \mathfrak{M}$, $\mathfrak{M}, \ell \models \varphi$ if and only if $\mathfrak{M}, h \circ \ell \models \varphi$. The first says $d \in S$; since $(h \circ \ell)(x) = h(d)$, the second says $h(d) \in S$. ■

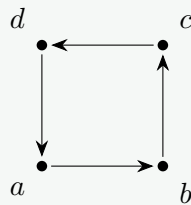
So to show that a set is **not** definable, find an automorphism that moves an element of it to an element outside it.

Example. Zero Cannot Be Defined from the Order of the Integers

In $(\mathbb{Z}, <)$, the shift $h(d) = d + 1$ is an automorphism: it is a bijection, with inverse $d \mapsto d - 1$, and $d < e$ if and only if $d + 1 < e + 1$. It sends 0 to 1, and $1 \notin \{0\}$. By [Corollary 7.5.2](#), $\{0\}$ is not definable in $(\mathbb{Z}, <)$: no formula in $<$ alone singles out zero among the integers.

Contrast $(\mathbb{N}, <)$. There $\{0\}$ is definable, by $\forall y \neg(y < x)$, “nothing is below x ”. The corollary is not contradicted, since $d \mapsto d + 1$ is not an automorphism of $(\mathbb{N}, <)$: it is not onto.

A finite picture: the four-cycle below, with $D = \{a, b, c, d\}$ and R the four arrows $a \rightarrow b \rightarrow c \rightarrow d \rightarrow a$.



The rotation $a \mapsto b, b \mapsto c, c \mapsto d, d \mapsto a$ is a bijection that sends each arrow to an arrow and each non-arrow to a non-arrow, so it is an automorphism. Applied once, twice or three times, it moves any element to any other, so no single element is definable.

A minimal change makes one element definable again. Add the loop (a, a) to R . Now $R(x, x)$ defines $\{a\}$, and the rotation is no longer an automorphism, since it sends the arrow (a, a) to (b, b) , which is not an arrow. The method can only use the automorphisms a structure has;

each of the three non-trivial rotations sends the loop (a, a) to a loop at b , c or d , so adding one arrow removed all three.

Warning. An automorphism shows that a set is **not** definable; it never shows that one is. That no automorphism moves a set is not evidence that a formula defines it. To show a set definable, write the formula.

Quick check. In the four-cycle, where does the rotation send the set $\{a, c\}$? Could $\{a, c\}$ be definable?

Solution. The rotation sends a to b and c to d , so it moves $a \in \{a, c\}$ to $b \notin \{a, c\}$. By [Corollary 7.5.2](#), $\{a, c\}$ is not definable. Its complement $\{b, d\}$ is not definable either, by the same rotation.

Remark (Looking ahead). *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 6, proves that any two complete ordered fields are isomorphic, by an isomorphism built from the rationals below each element; by this section, they then satisfy the same sentences.

7.5.6 Exercises

7.5.6.1 A. Check your understanding

Exercise. A1

- Define “ $S \subseteq D$ is definable in $\mathfrak{M}$ ”.
- Write formulas defining, in $(\mathbb{N}; +)$, the even numbers and the set $\{0\}$.
- Why does a formula with two free variables define a set of pairs, and not a set of elements?
- (*Second pass.*) State [Theorem 7.5.1](#).
- (*Second pass; key proof.*) Where does the proof of [Theorem 7.5.1](#) use that h is onto, and where that it is injective? What goes wrong for $d \mapsto d + 1$ on $(\mathbb{N}, <)$?
- (*Second pass.*) Why does $x \mapsto x + 1$ show $\{0\}$ undefinable in $(\mathbb{Z}, <)$ but not in $(\mathbb{N}, <)$?

Solution. (a) Some formula φ with free variable x (at most) defines it: $S = \{d \in D : \mathfrak{M}, \ell[x \mapsto d] \models \varphi\}$, for any assignment ℓ ([Definition 7.5.1](#)).

(b) $\exists y (x = y + y)$, “ x is a sum of two equal numbers”; $x + x = x$, “ x added to itself is itself”.

(c) Its truth depends on the values of both variables (and, by Lemma 7.1.1, on nothing else), so it is true or false of pairs of values.

(d) If $h: \mathfrak{M} \rightarrow \mathfrak{N}$ is an isomorphism, then $\mathfrak{M}, \ell \models \varphi$ if and only if $\mathfrak{N}, h \circ \ell \models \varphi$, for every formula φ and every assignment ℓ in $\mathfrak{M}$; in particular $\mathfrak{M}$ and $\mathfrak{N}$ satisfy the same sentences.

(e) Onto: in the $\forall$ and $\exists$ cases, so that $h(d)$ runs over all of E as d runs over D . Injective: in the equation case, to go from $h(t_1^{\mathfrak{M},\ell}) = h(t_2^{\mathfrak{M},\ell})$ back to $t_1^{\mathfrak{M},\ell} = t_2^{\mathfrak{M},\ell}$. The map $d \mapsto d + 1$ is not onto, and the $\forall$ case fails: $\forall y \neg(y < x)$ is satisfied when x has the value 0, and not when x has the value $h(0) = 1$, because the element 0 below 1 is exactly the one the map never reaches.

(f) It is an automorphism of $(\mathbb{Z}, <)$ and moves 0; it is not an automorphism of $(\mathbb{N}, <)$ (not onto), and in $(\mathbb{N}, <)$ the set $\{0\}$ is in fact definable, by $\forall y \neg(y < x)$.

Exercise. A2: Drill

Each part takes a line or two. Parts (a)–(f) belong to the first half of the section; parts (g)–(l) to the second half (second pass). They run from reading a formula, through writing one, to judging maps and using them.

- (a) What subset of $\mathbb{Z}$ does $\exists y (x = y + y + y)$ define in $(\mathbb{Z}; +)$?
- (b) Define $\{0\}$ in $(\mathbb{Z}; +)$.
- (c) Define the pairs with $x \leq y$ in $(\mathbb{N}; +)$.
- (d) In $(\{1, 2, 3\}, <)$, which set does $\forall y \neg(y < x)$ define? In $(\mathbb{Z}, <)$?
- (e) Write “ x is maximal” and “ x is greatest” for a partial order $\leq$.
- (f) In $(\mathbb{R}; 1, +, \cdot)$, φ is $x \cdot x + y \cdot y = 1$. What does $\exists y \varphi$ define?
- (g) Is $h(d) = 2d$ an isomorphism from $(\mathbb{Z}, <)$ to the even integers with $<$?
- (h) Is $h(d) = -d$ an automorphism of $(\mathbb{Z}, <)$? Of $(\mathbb{Z}; +)$?
- (i) Using (h), is $\{1\}$ definable in $(\mathbb{Z}; +)$?
- (j) Is that consistent with (b)?
- (k) $\mathfrak{M}$ has $D = \{a, b, c\}$ and $R^{\mathfrak{M}} = \{(a, c), (b, c)\}$. Which singletons are definable?
- (l) Are $(\mathbb{N}, <)$ and $(\mathbb{Z}, <)$ isomorphic? Give a sentence that shows it.

Solution.

- (a) The multiples of 3.
- (b) $x + x = x$.
- (c) $\exists z (x + z = y)$, “ y is x plus something”.
- (d) $\{1\}$, “nothing is below x ”; $\emptyset$, since every integer has a smaller one.
- (e) $\forall y (x \leq y \rightarrow y = x)$; $\forall y (y \leq x)$.
- (f) $[-1, 1]$, the shadow of the unit circle on the x -axis.
- (g) Yes: a bijection onto the evens, and $d < e$ if and only if $2d < 2e$.
- (h) Not of $(\mathbb{Z}, <)$: $0 < 1$, but $-0 = 0 > -1$. Yes of $(\mathbb{Z}; +)$: it is a bijection (its own inverse), and $-(d + e) = (-d) + (-e)$.
- (i) No: the automorphism $d \mapsto -d$ sends 1 to $-1 \notin \{1\}$.
- (j) Yes: $d \mapsto -d$ sends 0 to 0, so it does not move $\{0\}$.
- (k) $\{c\}$, by $\exists y R(y, x)$, “something points to x ”. Not $\{a\}$ or $\{b\}$: swapping a and b (and fixing c) is an automorphism.
- (l) No. $\exists x \forall y \neg(y < x)$, “there is a least element”, is true in $(\mathbb{N}, <)$ and false in $(\mathbb{Z}, <)$;

isomorphic structures would agree on it.

7.5.6.2 B. Practice

Exercise. B1: Define it by a formula

Define by a formula, and read each formula back in words. Parts (i)–(iii) are in $(\mathbb{N}; \cdot)$; parts (iv) and (v) are in $(\mathbb{R}; \leq, A)$, with A a one-place symbol.

- (i) “ x divides y ”.
- (ii) “ x is a square”.
- (iii) “ x and y have no common divisor except 1”.
- (iv) “ A is bounded above”.
- (v) “ A has a supremum that is not in A ”.

Solution.

- (i) $\exists z (x \cdot z = y)$: “ y is x times something”.
- (ii) $\exists y (y \cdot y = x)$: “ x is something times itself”.
- (iii) $\forall z ((\exists u (z \cdot u = x) \wedge \exists v (z \cdot v = y)) \rightarrow \forall w (z \cdot w = w))$: “every common divisor z of x and y is 1”. The consequent is $U(z)$ of [Example \(Sets Defined by Formulas\)](#) (c), with its bound variable renamed to w : written with the bound y of U , it would capture the free y . (At $x = y = 0$ every z is a common divisor, so the formula fails, as it should.)
- (iv) $\exists x B(x)$, with $B(x)$ the upper-bound formula $\forall y (A(y) \rightarrow y \leq x)$: “some x is at least every element of A ”.
- (v) $\exists x (B(x) \wedge \forall z (B(z) \rightarrow x \leq z) \wedge \neg A(x))$: “some least upper bound of A is not in A ”.

Marking scheme. (10 points) 2 for each part: 1 for the formula, 1 for its reading back, with any auxiliary formula (U , B) written out or cited. Fatal error (0 for the part): a free variable left over that is not one of the defined set’s.

Exercise. B2: What does this formula define?

Describe the set each formula defines.

- (i) $\exists y (x = y \cdot y \cdot y)$ in $(\mathbb{R}; \cdot)$.
- (ii) The same formula in $(\mathbb{Z}; \cdot)$.
- (iii) $\forall y (y \cdot x = x)$ in $(\mathbb{N}; \cdot)$.
- (iv) $\exists z (\neg(z + z = z) \wedge x + z = y)$ in $(\mathbb{Z}; +)$.
- (v) $\exists y (x < y \wedge \forall z (\neg(x < z \wedge z < y)))$ in $(\mathbb{Q}, <)$, and in $(\mathbb{Z}, <)$.

Solution.

- (i) All of $\mathbb{R}$: every real number has a real cube root.
- (ii) The cubes, $\{\dots, -8, -1, 0, 1, 8, 27, \dots\}$.
- (iii) $\{0\}$: at $x = 0$, $y \cdot 0 = 0$ for every y ; at $x \geq 1$, the instance $y = 0$ fails.

- (iv) All pairs (x, y) with $x \neq y$. In $\mathbb{Z}$, $z = y - x$ always exists, and it is non-zero exactly when $x \neq y$. The same formula defined $x < y$ in $(\mathbb{N}; +)$ (Example (Sets Defined by Formulas) (b)); in $\mathbb{Z}$, where a negative z is available, it defines something else.
- (v) In $(\mathbb{Q}, <)$, $\emptyset$: between x and any larger y lies $(x + y)/2$. In $(\mathbb{Z}, <)$, all of $\mathbb{Z}$: take $y = x + 1$.

Marking scheme. (10 points) 2 for each part; in (iv), full marks require noticing that $\mathbb{Z}$ is not $\mathbb{N}$. Fatal error (0 for the part): an answer that ignores the structure, such as the same set for both structures in (v).

Exercise. B3: Automorphisms of small structures

(Second pass.)

- (a) Find every automorphism of $\mathfrak{M}$: $D = \{1, 2, 3, 4\}$, $R^{\mathfrak{M}} = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$, the answer given to Exercise (B1: Construct a relation, or show none exists, used later) (ii).
- (b) Which singletons and which two-element subsets of D does that leave possibly definable? Define those that are.
- (c) Is $d \mapsto d + 1$ an automorphism of $(\mathbb{Z}; <, 0)$, with 0 a constant?

Solution. (a) An automorphism sends related pairs to related pairs and unrelated pairs to unrelated pairs. 4 is the only element related to nothing, so it must go to 4. 3 is the only element related to itself and to nothing else, so it must go to 3. That leaves 1 and 2, which may stay or be swapped, and both choices preserve R . So there are two automorphisms: the identity, and the swap of 1 and 2.

(b) $\{1\}$ and $\{2\}$ are not definable: the swap moves them. $\{3\}$ is defined by $R(x, x) \wedge \forall y (R(x, y) \rightarrow y = x)$; $\{4\}$ by $\neg R(x, x)$. Among the two-element sets, $\{1, 2\}$ is defined by $\exists y (R(x, y) \wedge \neg(y = x))$, “ x is related to something else”, and $\{3, 4\}$ by its negation $\neg \exists y (R(x, y) \wedge \neg(y = x))$. The other four, $\{1, 3\}$, $\{1, 4\}$, $\{2, 3\}$, $\{2, 4\}$, are moved by the swap, so none is definable.

(c) No: it sends the value 0 of the constant to 1, and clause (i) of Definition 7.5.2 asks $h(0) = 0$.

Marking scheme. (10 points) 4 for (a): both automorphisms, with the argument that 3 and 4 are fixed. 4 for (b): each definable set with its formula, and each other set with the automorphism that moves it. 2 for (c). Fatal error (0 for (b)): claiming a set definable because no automorphism moving it was found.

7.5.6.3 C. Going deeper

Exercise. C1: The definable subsets of $(\mathbb{Z}, <)$

(Second pass.)

- (a) Prove that the only subsets of $\mathbb{Z}$ definable in $(\mathbb{Z}, <)$ by a formula with one free variable are $\emptyset$ and $\mathbb{Z}$.

- (b) Show that the relation “ $y = x + 1$ ” is definable in $(\mathbb{Z}, <)$.
 (c) Why does (a) not contradict (b)?

Solution. (a) $\emptyset$ and $\mathbb{Z}$ are defined by $\neg(x = x)$ and $x = x$. Conversely, let S be definable and non-empty, with $n \in S$, and let $m \in \mathbb{Z}$. The shift $d \mapsto d + (m - n)$ is an automorphism of $(\mathbb{Z}, <)$: it is a bijection, with inverse $d \mapsto d - (m - n)$, and $d < e$ if and only if $d + (m - n) < e + (m - n)$. It sends n to m , so $m \in S$ by [Corollary 7.5.2](#). Since m was arbitrary, $S = \mathbb{Z}$.

(b) $x < y \wedge \neg \exists z (x < z \wedge z < y)$, “ y is above x with nothing in between”. In $\mathbb{Z}$ it holds of (d, e) exactly when $d < e$ and no integer lies strictly between, that is, $e = d + 1$: if $e = d + 1$, an integer z with $d < z < d + 1$ does not exist; if $e \geq d + 2$, then $z = d + 1$ lies between.

(c) The corollary, and the argument of (a), concern sets of elements. “ $y = x + 1$ ” defines a set of pairs, and a shift moves each pair $(n, n + 1)$ to another pair $(m, m + 1)$ of the same set, so the set of pairs is not moved. What (a) forbids is a formula singling out some integers and not others; (b) singles out a relation that every integer has to its successor.

Marking scheme. (10 points) 5 for (a): the shift shown to be an automorphism (bijective and order-preserving), then the corollary applied. 3 for (b), with both directions checked in $\mathbb{Z}$. 2 for (c). Fatal error (0 for (a)): using $d \mapsto -d$, which does not preserve $<$.

Exercise. C2: Challenge: the automorphisms of $(\mathbb{Q}, <)$

(Second pass.)

- (a) Show that $x \mapsto 2x$, and $x \mapsto x + q$ for each rational q , are automorphisms of $(\mathbb{Q}, <)$.
 (b) Deduce that the only subsets of $\mathbb{Q}$ definable in $(\mathbb{Q}, <)$ by a formula with one free variable are $\emptyset$ and $\mathbb{Q}$.
 (c) Show that $\{x \in \mathbb{Q} : x > 0\}$ is definable in $(\mathbb{Q}; <, 0)$, with 0 a constant, but not in $(\mathbb{Q}, <)$.

Solution. (a) Both are bijections of $\mathbb{Q}$, with inverses $x \mapsto x/2$ and $x \mapsto x - q$, and both preserve $<$ in both directions: $x < y$ if and only if $2x < 2y$, if and only if $x + q < y + q$.

(b) The translations alone suffice: given p in a non-empty definable set S and any $p' \in \mathbb{Q}$, the automorphism $x \mapsto x + (p' - p)$ sends p to p' , so $p' \in S$ by [Corollary 7.5.2](#). As in C1, $S = \mathbb{Q}$.

(c) In $(\mathbb{Q}; <, 0)$ the formula $0 < x$ defines it. In $(\mathbb{Q}, <)$ it is neither $\emptyset$ nor $\mathbb{Q}$, so by (b) it is not definable.

Marking scheme. (10 points) 3 for (a), 4 for (b), 3 for (c). Fatal error (0 for (b)): an argument with $x \mapsto 2x$ alone, which fixes 0 and so cannot move 0 to anything else.

7.5.6.4 R. Review

Exercise. R1

Decide whether each sequent is derivable, and justify your answer.

- (a) $(p \rightarrow q) \rightarrow r \vdash p \rightarrow r$.
 (b) $(p \rightarrow q) \rightarrow r \vdash q \rightarrow r$.

Solution. (a) Not derivable. Look for a refuting row, backwards from the conclusion: $p \rightarrow r$ is false only when $p = T$ and $r = F$. The premise must then be true, so its hypothesis $p \rightarrow q$ must be false, which needs $q = F$. In the row $p = T, q = F, r = F$, the premise is $F \rightarrow F$, true, and the conclusion is $T \rightarrow F$, false. By Corollary 4.7.3 there is no derivation.

(b) Derivable. The goal is an implication, so open a box on q ; the premise is waiting for $p \rightarrow q$, which a box on p produces by repeating q (the goal-directed and premise-directed steps of the search method of Section 3.1).

1		$(p \rightarrow q) \rightarrow r$	
2		q	asm, for $\rightarrow I$
3		p	asm, for $\rightarrow I$
4		q	R 2
5		$p \rightarrow q$	$\rightarrow I$ 3–4
6		r	$\rightarrow E$ 1, 5
7		$q \rightarrow r$	$\rightarrow I$ 2–6

The row method of (a) could not settle (b): no row refutes it, and only a derivation (or Theorem 4.8.4) shows it is derivable.

Exercise. R2

Derive $\neg(P \rightarrow \neg Q) \vdash \neg\neg P \wedge \neg\neg Q$ without RAA and without derived rules that use it. Which rule would you need to derive $P \wedge Q$ itself?

Solution. The goal is a conjunction, so derive each conjunct. Each is a negation, so each gets a $\neg I$ box, whose goal is $\perp$. The only way to use the premise $\neg(P \rightarrow \neg Q)$ is to clash with it, so inside each box we build $P \rightarrow \neg Q$. In the first box, from $\neg P$: a $\rightarrow I$ box on P clashes P with $\neg P$ and uses $\perp E$ (the pattern of Proposition 2.1.2). In the second, from $\neg Q$: a $\rightarrow I$ box on P simply repeats $\neg Q$. These are the rules of Chapters 1 and 2 (Definition 2.2.1, Definition 2.1.1, Definition 1.4.1).

1	$\neg(P \rightarrow \neg Q)$	
2	$\neg P$	asm, for $\neg$ I
3	P	asm, for $\rightarrow$ I
4	$\perp$	$\neg$ E 3, 2
5	$\neg Q$	$\perp$ E 4
6	$P \rightarrow \neg Q$	$\rightarrow$ I 3–5
7	$\perp$	$\neg$ E 6, 1
8	$\neg\neg P$	$\neg$ I 2–7
9	$\neg Q$	asm, for $\neg$ I
10	P	asm, for $\rightarrow$ I
11	$\neg Q$	R 9
12	$P \rightarrow \neg Q$	$\rightarrow$ I 10–11
13	$\perp$	$\neg$ E 12, 1
14	$\neg\neg Q$	$\neg$ I 9–13
15	$\neg\neg P \wedge \neg\neg Q$	$\wedge$ I 8, 14

No RAA is used. To reach $P \wedge Q$ we would need P from $\neg\neg P$ and Q from $\neg\neg Q$, that is, $\neg\neg$ E, which is derived with RAA (Proposition 2.5.1), or an RAA box directly (Definition 2.5.1). The look-alike is Exercise (B1: Three searches) (b), $\neg(P \rightarrow Q) \vdash P \wedge \neg Q$: there the conjunct P needed RAA, while $\neg Q$ came by $\neg$ I alone. Here both conjuncts stop at a double negation. That no derivation of P (or of $P \wedge Q$) from the premise avoids RAA is true, but we state it without proof, and nothing depends on it.

Exercise. R3

Derive $\neg\exists x (P(x) \rightarrow \neg Q(x)) \vdash \forall x (\neg\neg P(x) \wedge \neg\neg Q(x))$ without RAA.

Solution. The goal is $\forall x$, so open a flagged box with a fresh name x_0 (Definition 5.4.1); the new goal is $\neg\neg P(x_0) \wedge \neg\neg Q(x_0)$. Inside, run the derivation of R2 ([Exercise \(R2\)](#)) with $P(x_0)$ and $Q(x_0)$ in place of P and Q . One change: the premise is now $\neg\exists x (P(x) \rightarrow \neg Q(x))$, not $\neg(P \rightarrow \neg Q)$, so each clash first turns $P(x_0) \rightarrow \neg Q(x_0)$ into $\exists x (P(x) \rightarrow \neg Q(x))$ by $\exists$ I at x_0 (Definition 5.5.1).

1		$\neg \exists x (P(x) \rightarrow \neg Q(x))$	
2	x_0	$\neg P(x_0)$	asm, for $\neg$ I
3		$P(x_0)$	asm, for $\rightarrow$ I
4		$\perp$	$\neg$ E 3, 2
5		$\neg Q(x_0)$	$\perp$ E 4
6		$P(x_0) \rightarrow \neg Q(x_0)$	$\rightarrow$ I 3–5
7		$\exists x (P(x) \rightarrow \neg Q(x))$	$\exists$ I 6
8		$\perp$	$\neg$ E 7, 1
9		$\neg \neg P(x_0)$	$\neg$ I 2–8
10		$\neg Q(x_0)$	asm, for $\neg$ I
11		$P(x_0)$	asm, for $\rightarrow$ I
12		$\neg Q(x_0)$	R 10
13		$P(x_0) \rightarrow \neg Q(x_0)$	$\rightarrow$ I 11–12
14		$\exists x (P(x) \rightarrow \neg Q(x))$	$\exists$ I 13
15		$\perp$	$\neg$ E 14, 1
16		$\neg \neg Q(x_0)$	$\neg$ I 10–15
17		$\neg \neg P(x_0) \wedge \neg \neg Q(x_0)$	$\wedge$ I 9, 16
18		$\forall x (\neg \neg P(x) \wedge \neg \neg Q(x))$	$\forall$ I 2–17

The side condition of $\forall$ I at line 18: x_0 does not appear in the premise on line 1, no box is open at line 18, and x_0 does not appear in the conclusion. The flagged box immediately contains the $\neg$ I box of line 2, so it is cited from line 2, the first line of that inner box. Lines 7 and 14 are legal $\exists$ I steps: $P(x_0) \rightarrow \neg Q(x_0)$ is $(P(x) \rightarrow \neg Q(x))[x_0/x]$. The whole derivation is R2's, run inside a flagged box, with an $\exists$ I before each clash.

Exercise. R4

Is the sentence $\forall x \exists y (x < y) \rightarrow \exists y \forall x (x < y)$ true in $(\mathbb{N}, <)$? Is it derivable?

Solution. True in $(\mathbb{N}, <)$? No. The hypothesis $\forall x \exists y (x < y)$ is true in $(\mathbb{N}, <)$: each d has $d + 1$ above it. The conclusion $\exists y \forall x (x < y)$ is false: a candidate e fails at $x = e$, since $e < e$ is false. By (S5) of Definition 7.1.3, an implication with a true hypothesis and a false conclusion is false.

Derivable? No. By the soundness statement of Section 7.2, a derivable sentence is true in every structure; this one is false in $(\mathbb{N}, <)$, so no derivation exists.

Why these tools. A structure settles the question in two lines, while a derivation search could only fail, and a failed search proves nothing. A truth table is the wrong look-alike: it reads the sentence as $p \rightarrow q$ with two atoms, and a refuting row for $p \rightarrow q$ says nothing here, since

the sentence $\forall x P(x) \rightarrow \exists x P(x)$ has the same shape and is derivable (Proposition 5.5.1, then $\rightarrow$ I). The soundness statement used here is proved in Section 7.3.