Chapter 15
Symmetries and Logical Visibility One More Time

Abstract My aim in this book was to explain the concept of mathematical structure, and to show examples of techniques that are used to study them. It would be hard to do it honestly without introducing some elements of logic and set theory. In a textbook, the line of thought may sometimes get lost in technical details. Now, when all necessary material has been covered, I can give a summary and a brief description of what this book is about.

15.1 Structures

What is a structure? It is a set, called the domain, with a set of relations on it. Any set can serve as a domain of a structure. In the logic approach to structures, the first step is to forget about what the elements of the domain are made of, and to consider only how the elements and their finite sequences (ordered pairs, triples, etc.) are related by the relations of the structure. To know a structure defined this way, means to understand the geometry of its parametrically definable sets. We are not only interested in the subsets of the domain, but also in the whole multidimensional spectrum of the definable subsets of all of Cartesian powers of the domain.

Where do all the sets come from? This is a difficult question. In modern mathematics we rely on the axiomatic method. The axioms determine what we know about the universe of sets. This is the reason for the detour through the axioms of the Zermelo-Fraenkel set theory in Chap. 6.

Once the status of sets and relations gets clarified, the question is what do we want to know about a mathematical structure. What is there to see in it? Here, for a partial answer we resorted to first-order logic. What we "see" in a structure is what can be defined from its relations by means of logic, hence we can talk about a sort of *logical seeing*.

Let X be a domain of a structure. For each $n > 0$, the parametrically definable subsets of X^n form a Boolean algebra, which means that if A and B are parametrically definable subsets of X^n, then so are their intersection $A \cap B$, their union $A \cup B$, and their complements $\bar{A}$ and $\bar{B}$, and those set operations correspond, respectively, to forming conjunctions, disjunctions, and negations of the defining

R. Kossak, *Mathematical Logic*, Springer Graduate Texts in Philosophy 3,
https://doi.org/10.1007/978-3-319-97298-5_15

formulas. Those are the basic sets that we see through the eyes of logic, but the formalism of first-order logic allows us to describe more sets. Taking Boolean combinations of formulas with different sequences of variables results in definable sets in higher dimensions. For example if $\varphi(x_1, x_2)$ and $\psi(x_3)$ are formulas with free variables x_1, x_2, and x_3 respectively, then $\varphi(x_1, x_2)$ defines a subset of X^2, $\psi(x_3)$ defines a subset of X, and $\varphi(x_1, x_2) \wedge \psi(x_3)$ defines a subset of X^3. Finally, quantification corresponds to projections from higher dimensions to lower.

In the case of tame structures, the geometry of one-dimensional definable sets to large extent determines the geometry in higher dimensions, and the general theory of such structures leads to descriptions and classifications of all parametrically definable sets. We do understand those structures well. We see them. In this book, we could not get into more advanced details of the model theory of tame structures, but we could see some elements of the theory and the role that first-order logic plays in it.[1]

Wild structures are just wild, and there is no hope for any general theory of all of their parametrically definable sets. The first-order analysis of those wild structures reveals an enormous complexity in the geometry of the definable sets. From the basic relations, using mechanical rules for the syntax of first-order logic one can generate a whole hierarchy of mathematical objects with each level more complex than the previous one.

In both cases, tame and wild, symmetries are an important tool in the analysis of structures. Much information about a structure can be gained by the study of the subsets of its domain that are invariant under symmetries. Think of corner points of a square, or the central point of a star-shaped graph. If a structure has symmetries, we can learn much from describing and classifying them, but many structures do not have symmetries, and then it helps to consider elementary extensions instead. Every structure with an infinite domain has an elementary extension to a larger structure. This combined with the power of set-theoretic methods, allows us to construct structures with interesting properties. In particular, every structure with an infinite domain can be extended to a structure with many symmetries.

There are many attractive examples we could have discussed, but we concentrated on the classical number structures. It is quite fascinating to see the historical development of the number system, and then to see how the corresponding number structures grew from very wild, to completely tame. It took many pages to tell that story. Now we can tell it again briefly.

15.2 The Natural Numbers

The German mathematician Leopold Kronecker famously said that "God made the integers, all else is the work of man." We outlined that work in great detail. We built everything from the natural numbers, but we did not assume that God gave them to us, we built them from scratch ourselves.

[1] For a technical exposition see [36].

The domain $\mathbb{N}$ can be defined in many ways. In set theory, following John von Neumann, we define them by declaring that the empty set $\varnothing$ stands for 0, then $\{\varnothing\}$ is 1, $\{\varnothing, \{\varnothing\}\}$ is 2, $\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$ is 3, and so on. We discussed this in Chap. 6. Defining natural numbers this way has its advantages, but there is nothing sacred about this definition. Before von Neumann, Ernst Zermelo defined natural numbers to be: $\varnothing$, $\{\varnothing\}$, $\{\{\varnothing\}\}$, $\{\{\{\varnothing\}\}\}$... and that is fine too. The whole point here was not to start with some assumed common conception of what the natural numbers should be, but to ground the notion in a more rudimentary set-theoretic background.

The natural numbers form a set and this set as such is a trivial structure, not different from any other countable infinite set. It becomes a fascinating structure once it is equipped with addition and multiplication. Von Neumann's approach allows us to give straightforward set-theoretic definitions of both operations, and thus the structure $(\mathbb{N}, +, \cdot)$ is born. After all this effort, we can forget about what the natural numbers are made of. We have a set and a set of two relations on it, and this is all we need for further analysis.

The natural numbers are linearly ordered, but there is no need to include the ordering relation since it is definable in $(\mathbb{N}, +, \cdot)$. Since the defining formula $\neg(x = y) \wedge \exists z(x + z = y)$ does not involve multiplication, the relation $x < y$ is already definable in $(\mathbb{N}, +)$. Using the ordering, it is easy to see that every natural number is definable. This is a fundamental feature of the natural numbers. There is an old mathematical joke about a theorem that says "Every natural number is interesting." Indeed, 0 is interesting because it is the least number; 1 is interesting because it is the least positive number; 2 is the least even number; 3 is the least odd prime number; 4 is the least even square; and so on. To prove the theorem, suppose that there is a natural number that is not interesting. Then there must be a least such number m. So all numbers smaller than m are interesting, but m is not. That is a curious property, and it clearly makes m interesting. So m is interesting after all, and this contradiction finishes the proof of the theorem.

Since every natural number is definable in $(\mathbb{N}, <)$ without parameters, this structure is rigid, it has no nontrivial symmetries. In order to show that $(\mathbb{N}, <)$ is minimal, we used symmetries of its elementary extension $(\mathbb{N}^*, <)$. Even though the successor function $S(x) = x + 1$ is definable in $(\mathbb{N}, <)$, the whole addition relation is not. If we could define addition in $(\mathbb{N}, <)$, it would follow that $(\mathbb{N}, +)$ is minimal, but we know that it is not.[2]

The structure $(\mathbb{N}, +)$ is not minimal, but still quite tame. By theorem of Ginsburg and Spanier, proved in 1966, every set of natural numbers definable in $(\mathbb{N}, +)$ is ultimately periodic, which means that for every such set X there are numbers m and p such that for any n, if $m < n$ then n is a member of X if and only if $n + p$ is. After an unpredictable initial segment, every definable set becomes quite well-behaved. This rules out a possibility of defining sets such as the set of all square numbers, or the set of primes. None of them is ultimately periodic. When we expand $(\mathbb{N}, +)$ by adding multiplication, it gets wild. $(\mathbb{N}, +, \cdot)$ is the ultimate wild structure. Any other structure that contains a definable isomorphic copy of $(\mathbb{N}, +, \cdot)$ is also wild.

[2]For example, the formula $\exists y[y + y = x]$ defines the set of even numbers (which is neither finite nor cofinite).

The multiplicative structure on natural numbers $(\mathbb{N}, \cdot)$ is also not minimal. In the language of multiplication one can define the set of square numbers (which is neither finite nor cofinite). The set of primes is also definable. It is interesting though that the ordering of the natural numbers is not definable. This follows from the fact that $(\mathbb{N}, \cdot)$ has nontrivial automorphisms. If p and q are prime numbers, then the function that permutes p and q and fixes all other prime numbers can be extended to a symmetry of $(\mathbb{N}, \cdot)$ (this is not obvious, see hints in the exercise section). Hence, in $(\mathbb{N}, \cdot)$ all prime numbers share the same type. Since 2 is prime, and all other primes are odd, it also follows, that the set of even numbers is not definable in $(\mathbb{N}, \cdot)$.

The results about definability in $(\mathbb{N}, +)$ and $(\mathbb{N}, \times)$ imply that addition of natural numbers is not definable from multiplication, and that multiplication is not definable from addition. This is an intriguing corollary. Even though addition of natural numbers *determines* their multiplication, first-order logic does not capture it.

15.3 The Integers

The set of integers $\mathbb{Z}$ is obtained by appending negative opposites of all natural number to $\mathbb{N}$. To make this "appending" precise, in Chap. 4, we defined the integers in a special way to show how the extended structure $(\mathbb{Z}, +, \cdot)$ can be defined in $(\mathbb{N}, +, \cdot)$. This showed how, from the logical point of view, the larger structure is no more complex than the one it contains. It also turned out that the larger structure is not less complex, because $\mathbb{N}$ is definable in $(\mathbb{Z}, +, \cdot)$, for example by the following formula $\varphi(x)$ in which x is the only free variable

$$\exists x_1 \exists x_2 \exists x_3 \exists x_4 [x = x_1^2 + x_2^2 + x_3^2 + x_4^2].$$

This works because of a theorem of Joseph-Louis Lagrange, who proved in 1770 that every positive integer is the sum of four squares. Notice that the formula involves both $+$ and $\cdot$. Equipped with $\varphi(x)$ we can also define the ordering of the integers, since for all integers x and y, $x < y$ if and only if $y + (-x)$ is positive. Hence, the relation $x < y$ is defined by the formula

$$\exists v \exists w [x + v = 0 \wedge w = y + v \wedge \varphi(w)].$$

This definition is decidedly more involved that the one that defines the ordering of the natural numbers in $(\mathbb{N}, +)$. One reason is that the use of multiplication in $\varphi(x)$ is not accidental. The ordering of the integers is not definable in $(\mathbb{Z}, +)$. The function $f(x) = -x$ is a symmetry of $(\mathbb{Z}, +)$, and consequently the type of any integer is the same as the type of its opposite. Addition alone cannot decide whether $0 < 1$ or $0 < -1$, because $f(0) = 0$, and $f(1) = -1$, hence $(0, 1)$ and $(0, -1)$ have the same first-order properties in $(\mathbb{Z}, +)$.

The argument above shows that 1 is not definable without parameters in $(\mathbb{Z}, +)$. It is definable in $(\mathbb{Z}, +, \cdot)$ as the only number x other than 0, such that $x \cdot x = x$. Since 1 and the ordering are definable in $(\mathbb{Z}, +, \cdot)$, it follows that every integer is definable; hence $(\mathbb{Z}, +, \cdot)$ is rigid.

15.4 The Rationals

The set of rational numbers $\mathbb{Q}$ together with addition and multiplication is first-order definable in $(\mathbb{Z}, +, \cdot)$, hence it is also first-order definable in $(\mathbb{N}, +, \cdot)$. Since 0 and 1 are definable in $(\mathbb{Q}, +, \cdot)$ by the same formulas that defined them in $(\mathbb{Z}, +, \cdot)$, one can show that all rational numbers are definable; hence $(\mathbb{Q}, +, \cdot)$ is rigid. However, $(\mathbb{Q}, +)$ has more symmetries than $(\mathbb{Z}, +)$. While $f(x) = -x$ is the only nontrivial symmetry of $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ has many more. In is not difficult to see, and we leave it as an exercise, that for every positive rational number p, the function $f_p(x) = p \cdot x$ is a symmetry.

Lagrange's theorem also holds for the rationals: each non-negative rational number is the sum of fours squares of rational numbers. Hence, the ordering of the rationals is definable in $(\mathbb{Q}, +, \cdot)$.

15.5 The Reals

With the introduction of the real numbers we enter a completely new territory. The set of real numbers is uncountable, so it cannot be definably interpreted in $(\mathbb{N}, +, \cdot)$. It is too large. To construct it we needed to appeal to set theory. Real numbers are complex objects as individuals, but the structure of the field of real numbers is much less complex than that of the rationals. It takes much less effort to define the ordering: the relation $x < y$ for the real numbers is defined by the formula $\neg(x = y) \wedge \exists z[x + z \cdot z = y]$, and this is due to the fact that every positive real number has a square root.

The field $(\mathbb{R}, +, \cdot)$ is order-minimal, and, as a consequence, neither $\mathbb{N}$, nor $\mathbb{Z}$, nor $\mathbb{Q}$ are definable in it. The rational numbers are not definable in $(\mathbb{R}, +, \cdot)$ as a set, but each rational number is defined by the same definition that defines it in $(\mathbb{Q}, +, \cdot)$. For each real number r, the type of r over $(\mathbb{R}, +, \cdot)$ includes the formulas $p < x$, and $x < q$, for all rational p and q such that $p < r$, and $r < q$. In fact, r is the only real number making all those formulas true. It follows that $(\mathbb{R}, +, \cdot)$ is rigid. No rational number can be moved by a symmetry because they are all definable without parameters, and no irrational number can be moved, because it is firmly trapped between two sets of rational numbers.

There are more definable reals than just the rationals. Each polynomial equation in one unknown with integer coefficients is either an identity, or has a finite number of solutions. Since the ordering is definable, for a given equation $p(x) = 0$ that has finitely many solutions, its smallest solution is definable, the next smallest solution is definable, and so on. Hence all real solutions of such equations are definable. The numbers that are members of finite solution sets of polynomial equations with integer coefficients are called *algebraic*.

The set of algebraic numbers includes many irrational numbers such as $\sqrt{2}$ or the golden ratio $\frac{1+\sqrt{5}}{2}$, and it is closed under addition and multiplication, and additive

and multiplicative inverses, i.e. if a and b are algebraic then so are $a + b$, $a \cdot b$, and $-a$, and $\frac{1}{a}$ (if $a \neq 0$). Since the collection of all polynomial equations with integer coefficients is countable, and each nontrivial equation has only finitely many solutions, the set of real algebraic numbers is countable. The set of real numbers is uncountable, hence there are many real numbers that are not algebraic. Those numbers are called *transcendental*. Many important mathematical constants, such as π and Euler's constant e, are transcendental, but in each case it takes an effort to prove it. It can be shown that the real algebraic numbers are the only numbers that are definable in $(\mathbb{R}, +, \cdot)$. It follows that there are no first-order definitions of π and e, even though they are uniquely determined by their first-order types (i.e. their Dedekind cuts). Transcendentals are not logically visible in $(\mathbb{R}, +, \cdot)$.

We can also say a bit about parametrically definable sets of real numbers. It follows from order-minimality that if a set A of real numbers is infinite, and is parametrically definable in $(\mathbb{R}, +, \cdot)$, then it must contain an interval, and that implies that it is not only infinite, but is in fact uncountable. Every interval of the real line has the same cardinality as the whole set of real numbers. It is of power continuum. Hence, every parametrically definable in $(\mathbb{R}, +, \cdot)$ set of real numbers is either finite (small), or of the power continuum (very large). No formula defines a set of cardinality $\aleph_0$.

15.6 The Complex Numbers

The field of the complex numbers $(\mathbb{C}, +, \cdot)$ is the ultimate number structure. It has an interesting history and remarkable applications. Much more space would be needed to do justice to all that. We will just scrape the surface.

The field $(\mathbb{C}, +, \cdot)$ is minimal. Every parametrically definable in $(\mathbb{C}, +, \cdot)$ subset of $\mathbb{C}$ is either finite or cofinite. Complex numbers that are elements of finite sets definable without parameters are called *algebraic*. Algebraic numbers are solutions of polynomial equations with integer coefficients. All real algebraic numbers, as defined in the previous section, are algebraic in the complex sense, and there are many more complex algebraic numbers that are not real. Prime examples the imaginary unit $i = (0, 1)$, and its additive inverse $-i = (0, -1)$.[3] Since there are only countably many definitions, and the union of countable many finite sets in countable, it follows that there are many non-algebraic complex numbers, and those numbers are also called transcendental. All real transcendental numbers are also transcendental as complex numbers, but unlike in the real field, where each number has its own unique type, in the complex field all transcendental numbers share the same type. There is only one type of a transcendental number in $(\mathbb{C}, +, \cdot)$! Even more is true, if z_1 and z_2 are transcendental, then there is a symmetry f of $(\mathbb{C}, +, \cdot)$ such that $f(z_1) = z_2$. In particular, there is a symmetry f such that $f(\pi) = e$. While the real field is rigid, the complex field has lots and lots of symmetries.

[3] i and $-i$ are the only solutions of $x^2 + 1 = 0$.

Here is one example of a nontrivial symmetry. The function that maps (a, b) to $(a, -b)$ is called *conjugation*. It is not difficult to check that conjugation is a symmetry of $(\mathbb{C}, +, \cdot)$. Under this symmetry, the image of i is $-i$, hence those two algebraic numbers have the same type. The numbers i and $-i$ have exactly the same first-order properties in $(\mathbb{C}, +, \cdot)$, they are indiscernible.

Conjugation maps every real number $r = (r, 0)$ to itself. All real numbers are fixed under conjugation. It follows that the graph of conjugation, i.e. the set G of all conjugate pairs of complex numbers $((a, b), (a, -b))$ is not a definable subset of $\mathbb{C}^2$. If G were definable by some formula $\varphi(x, y)$, then the set of real numbers would be defined by the formula $\varphi(x, x)$, but we know that it cannot be defined in $(\mathbb{C}, +, \cdot)$, because it is neither finite nor cofinite in $\mathbb{C}$.

Using conjugation we can also show that there cannot be any definable linear ordering of the complex numbers. For each linear ordering $<$, either $-i < i$ or $i < -i$, but conjugation swaps i with $-i$; hence, if the ordering were definable, it would follow that $-i < i$ if and only if $i < -i$, but that can't be.

All those results illustrate that there is very little one can see in $(\mathbb{C}+, \cdot)$ with the eyes of logic. This is certainly a weakness, since there is much going on there. One of the most well-known modern mathematical images is probably the *Mandelbrot set*. Many videos showing zooms deep into the boundary of the Mandelbrot set are available on youtube. They show the immense complexity of the set that is defined in a surprisingly simple way. For any complex number c, one starts with 0, and then iterates the function $z \mapsto z^2 + c$. This defines a sequence of numbers that either converges to 0, or stays in a bounded region of $\mathbb{C}$, or moves farther and farther away from 0 "escaping to infinity." The Mandelbrot set is the set of those numbers c for which the sequence does not escape to infinity.

The procedure used to define the Mandelbrot set involves addition and multiplication of complex numbers but it cannot be written in first-order fashion over $(\mathbb{C}+, \cdot)$, because the Mandelbrot set is neither finite nor cofinite. This means that there are concepts used in the definition that cannot be formalized in first-order logic in the language of the field of complex numbers. It is a subtle issue, so let us take a closer look.

The definition refers to distances of complex numbers from 0. This distance of a point (a, b) from 0 is perfectly well-defined in $(\mathbb{R}, +, \cdot)$; it is $\sqrt{a^2 + b^2}$. The function $f(a, b) = \sqrt{a^2 + b^2}$ is definable in $(\mathbb{R}, +, \cdot)$, but it cannot be definable over $(\mathbb{C}, +, \cdot)$ because its range is neither finite nor cofinite.

One could ask if the Mandelbrot set is second-order definable. In second-order logic one can define much. For example, let us take a look at the following second-order formula $\Phi(x)$.

$$\forall X[(0 \in X \wedge \forall z(z \in X \Longrightarrow z + 1 \in X) \Longrightarrow x \in X].$$

$\Phi(x)$ says that x belongs to any set that contains 0 and is closed under successor. In other words, x is in the smallest X with that property. Such a smallest set exists, and it is exactly the set of natural numbers $\mathbb{N}$. The field $(\mathbb{C}+, \cdot)$ is minimal, hence one can not define $\mathbb{N}$ in it by a first-order formula, but we just showed that it can be done by

a second-order one. Since $\mathbb{N}$ is second-order definable over $(\mathbb{C}, +, \times)$ a whole copy of $(\mathbb{N}, +, \cdot)$ is second-order definable as well, and that means that the second-order structure of the complex field is very complex indeed. Still, the Mandelbrot set is not second-order definable. That is because symmetries preserve not only the first-order definable properties, but all second-order properties as well. Suppose $M(x)$ were a second-order formula defining the Mandelbrot set. The Mandelbrot set contains small transcendental numbers, for example $\frac{1}{\pi}$; hence $M(\frac{1}{\pi})$ holds in $(\mathbb{C}, +, \cdot)$. But that implies that every transcendental number r is in the Mandelbrot set, since for every such number there is a symmetry f of $(\mathbb{C}, +, \times)$ such that $f(\frac{1}{\pi}) = r$. That is a contradiction, since the Mandelbrot set is bounded, and there are unboundedly many transcendental numbers, for example π is too large to be in the Mandelbrot set.

The discussion above is not intended to show that logical formalism is so deficient that it cannot capture something that is naturally defined in a mathematical language. The procedure that defines the Mandelbrot set can be easily converted to a second-order formula that defines that set over $(\mathbb{R}, +, \cdot)$. The reader who was patient enough to get to this point, may be ready to try to write such a formula.

Exercises

Exercise 15.1 *The Fundamental Theorem of Arithmetic says that every natural number can be uniquely written as a product of powers of prime numbers (in increasing order of primes). For example* $12 = 2^2 \cdot 3$, *and* $300 = 2^2 \cdot 3 \cdot 5^2$. *Hence, every number can be written in the form* $2^k \cdot 3^l \cdot m$ *for some natural number* m. *If* 2 *or* 3 *are missing in the representation, then the corresponding* k *or* l *are equal to* 0. *Consider the function* $f : \mathbb{N} \longrightarrow \mathbb{N}$, *defined by* $f(2^k \cdot 3^l \cdot m) = 3^k \cdot 2^l \cdot m$. *Show that* f *is a symmetry of* $(\mathbb{N}, \cdot)$.

Exercise 15.2 *Use the previous exercise to show that the ordering of the natural numbers is not definable in* $(\mathbb{N}, \cdot)$.

Exercise 15.3 *Show that 0 is the only integer that is definable without parameters in* $(\mathbb{Z}, +)$. *Hint: The function* $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ *defined by* $f(x) = -x$ *is a symmetry of* $(\mathbb{Z}, +)$.

Exercise 15.4 *Show that every rational number is definable without parameters in* $(\mathbb{Q}, +, \cdot)$. *Hint: See Exercise* 8.1.

Exercise 15.5 *Show that for every rational number* p *other than* 0, *the function* $f_p(x) = p \cdot x$ *is a symmetry of* $(\mathbb{Q}, +)$.

Exercise 15.6 *Every fraction* $\frac{p}{q}$ *can be written as* $\frac{p \cdot q}{q^2}$. *Apply this and Lagrange's theorem to prove that every positive rational number is equal to the sum of fours squares of rational numbers. This shows that the ordering of the rational numbers is definable in* $(\mathbb{Q}, +, \cdot)$.

Exercise 15.7 *The two solutions of the equation* $x^2 - x - 1 = 0$ *are* $\frac{1+\sqrt{5}}{2}$ *and* $\frac{1-\sqrt{5}}{2}$. *Write first-order formulas defining each of these numbers in* $(\mathbb{R}, +, \cdot)$.

Exercise 15.8 *Show that the function* $f : \mathbb{C} \longrightarrow \mathbb{C}$ *defined by* $f(a, b) = (a, -b)$ *is a symmetry of* $(\mathbb{C}, +, \cdot)$.

Exercise 15.9 * *Find a second-order definition of the Mandelbrot set over* $(\mathbb{R}, +, \cdot)$.