Chapter 2
Semantics of First-Order Languages

In the last chapter, we presented syntactical notions pertaining to first-order theories. However, in general, mathematical theories are not developed syntactically. In this chapter, we give the semantics of first-order languages to connect the syntactical description of a theory with the setting in which a mathematical theory is generally developed. This chapter should also be seen as the beginning of a branch of logic called model theory, which can be thought of as the general study of mathematical structures. Some important notions from model theory, for example, the downward Löwenheim–Skolem theorem, types, homogeneous structures, and definability, are introduced here.

Recall that instead of beginning with the syntactical object group theory, in practice, one begins by defining a group as a nonempty set G with a specified element e and a binary operation $\cdot : G \times G \to G$ satisfying the following three conditions:

1. For every a, b, c in G,
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$
2. For every $a \in G$,
$$a \cdot e = e \cdot a = a.$$
3. For every $a \in G$, there is a $b \in G$ such that
$$a \cdot b = b \cdot a = e.$$

Thus a group consists of a nonempty set G with "interpretations" or "meanings" of the nonlogical symbols $\cdot$ (a binary function symbol) and e (a constant symbol) such that all the axioms of group theory are "satisfied." Further, a statement in the language of group theory is called a theorem if it is satisfied in all groups. Thus, to give the connection we are looking for, first we should define the interpretation or the structure of a language L as a nonempty set A together with the interpretations

S.M. Srivastava, *A Course on Mathematical Logic*, Universitext,
DOI 10.1007/978-1-4614-5746-6_2,

or meanings of all the nonlogical symbols of L. This is known as the semantics of L. Then the models of a theory T are those structures of the language for T in which all axioms are true.

2.1 Structures of First-Order Languages

A *structure* or an *interpretation* of a first-order language L consists of (a) a nonempty set M (called the *universe* of the structure), (b) for each constant symbol c of L, a fixed element $c_M \in M$, (c) for each n-ary function symbol f of L, an n-ary map $f_M : M^n \to M$, and (d) for each n-ary relation symbol p of L, an n-ary relation $p_M \subset M^n$ on M. The interpretation of "=" is always taken to be the equality relation in M.

Any group is a structure of the language of group theory; the usual set of real numbers with the usual 0, 1, $+$, $\cdot$, and $<$ is a structure for the language of the theory of ordered fields. Note that which statement is true in a structure and which is not is irrelevant in the definition of a structure. For instance, the set of all natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$ as the universe, 0 as the interpretation of e, and $+$ the interpretation of $\cdot$ is a structure of the language of group theory even though it is not a group.

Example 2.1.1. Let $\mathbb{N}$ be the set of all natural numbers, and let 0, 1, $+$, $\cdot$, and $<$ have the usual meanings. Further, let $S(n) = n + 1$, $n \in \mathbb{N}$. This is a structure of the language of the theory N defined in Chap. 1. This structure will be called the *standard structure of* N.

Let L be an extension of L' and M a structure of L. By ignoring the interpretations of those nonlogical symbols of L that are not symbols of L', we get a structure M' of L'. We call M' the *restriction* of M to L' and denote it by $M|L'$. In this case we shall also call M an *expansion* of M' to L.

Recall that all variable-free terms can be obtained starting from constant symbols and iterating function symbols on them. Thus, we shall define the interpretation or meaning t_M of each variable-free term t of L in M by induction on the rank of t. The interpretation of a constant symbol c is already given by the structure, namely c_M. If $t_1, \ldots, t_n$ are variable-free terms whose interpretations have been defined and if f is an n-ary function symbol of L, then we define

$$(ft_1 \cdots t_n)_M = f_M((t_1)_M, \ldots, (t_n)_M).$$

By induction on the rank of terms, it is easy to see that we have defined t_M for each variable-free term t of L.

Example 2.1.2. Let L be the language of the theory of rings with identity. For each positive integer m, let $\underline{m}$ denote the term obtained by "adding" 1 to itself m times. Let $P(x)$ be a polynomial expression whose coefficients are of the form $\underline{m}$, i.e., $P(x)$ is a term of the form

$$\underline{m_0} + \underline{m_1}x + \cdots + \underline{m_n}x^n,$$

where x is a variable. Let R be a ring with identity. Then the interpretation of $\underline{m}$ in R is the element $m \in R$ obtained by adding the multiplicative identity of R to itself m times, and for any variable-free term t, the interpretation of $P_x[t]$ in R is the element

$$P(t_R) = m_0 + m_1 t_R + m_2 t_R^2 + \cdots + m_n t_R^n$$

of R.

2.2 Truth in a Structure

In this section, we shall define when a formula of L is true and when it is false in a structure of L. Note that if we have a structure of L with universe M and we would like to know whether there is an element $a \in M$ satisfying a formula $\varphi[x]$, then we have a bit of a problem because φ is a syntactical object and elements of M are not. To circumvent this problem, given a structure of L with universe M, we first describe an extension L_M of the language L.

Given L and a structure of L with universe M, let L_M be the first-order language obtained from L by adding a new constant symbol i_a for each $a \in M$. The symbol i_a is called the *name* of a. We regard M itself as the expansion of M to L_M by setting the interpretation of i_a to be a for each $a \in M$.

We are now in a position to define when a formula of L is true or valid or satisfiable in the structure M. To achieve this, we define the notion of the truth of a closed formula or a sentence of L_M in the structure M. The definition is based on the well-known intended meaning of the logical connectives $\vee$ and $\neg$ and that of the existential quantifier $\exists$. The notion of truth will be defined by defining a function from the set of all closed formulas of L_M to the set $\{T, F\}$ (T for true and F for false) satisfying some conditions. This will be done by induction on the rank of sentences of L_M. If a sentence takes the value T, we shall say that the sentence is true or valid in M; otherwise, it is said to be false in M.

Recall that formulas have been defined inductively starting from atomic formulas and iterating $\neg$, $\vee$, and $\exists$ on them. A variable-free atomic formula is of the form $pt_1 \cdots t_n$, where p is an n-ary relation symbol (including $=$) and $t_1, \ldots, t_n$ are variable-free terms. We say that $pt_1 \cdots t_n$ is true in the structure if

$$p_M((t_1)_M, \ldots, (t_n)_M)$$

holds, i.e.,

$$((t_1)_M, \ldots, (t_n)_M) \in p_M \subset M^n.$$

Otherwise, we say that $pt_1 \cdots t_n$ is false in the structure. A sentence $\neg A$ is true if and only if A is false. A sentence $A \vee B$ is true if either A is true or B is true. Finally, a sentence $\exists v A$ is true if $A_v[i_a]$ is true for some $a \in M$. We say that a formula A of L_M is true in the structure if its closure is true in the structure. If a formula A of L is true in a structure M of L, we also say that A is *valid in the structure* and write $M \models A$. If A is not valid in M, then we write $M \not\models A$.

Note that if A and B are closed formulas, then

$$M \models \neg A \Leftrightarrow M \not\models A$$

and

$$M \models A \vee B \Leftrightarrow M \models A \text{ or } M \models B.$$

Exercise 2.2.1. Give an example of a formula (necessarily not closed) of the language of the theory N that is not true and whose negation is not true in the standard structure $\mathbb{N}$ of N. Similarly, give examples of formulas A and B of the language of the theory N such that $A \vee B$ is valid in the standard structure $\mathbb{N}$ but neither A nor B is valid in $\mathbb{N}$.

Exercise 2.2.2. Show the following:

1. A sentence $A \wedge B$ is valid in a structure if and only if both A and B are valid in the structure.
2. A sentence of the form $\forall v \varphi[v]$ is valid in a structure with universe M if and only if for each $a \in M$ the sentence $\varphi_v[i_a]$ of L_M is valid in the structure.
3. A sentence of the form $A \to B$ is valid in a structure if and only if either A is false or B is true in the structure.
4. A sentence of the form $A \leftrightarrow B$ is valid in a structure if and only if either both A and B are valid or both are not valid in the structure.

Exercise 2.2.3. Let $A[v_1, \ldots, v_n]$ be a formula and $t_1, \ldots, t_n$ be variable-free terms of L. Show that the formulas

$$\forall v_1 \cdots \forall v_n A \to A[t_1, \ldots, t_n]$$

and

$$A[t_1, \ldots, t_n] \to \exists v_1 \cdots \exists v_n A$$

are valid in all structures of L.

2.3 Models and Elementary Classes

A *model* of a first-order theory T is a structure of $L(T)$ with universe M in which all nonlogical axioms of T are valid. For instance, any group is a model of group theory. On the other hand, the set $\mathbb{N}$ of natural numbers, together with the usual 0 and $+$ as the interpretations of e and $\cdot$ respectively, is definitely a structure for the language of group theory but not a model of group theory.

Example 2.3.1. Show that the set of all natural numbers

$$\mathbb{N} = \{0, 1, \ldots\}$$

with the usual meanings of S (the successor function), $+$, $\cdot$, and $<$ is a model of the theory N and also of Peano arithmetic. This model will be called the *standard model* of N or of Peano arithmetic.

A formula A of T that is true in all models of T is called *valid* in T. One writes $T \models A$ if A is valid in T. If A is not valid in some model of T, we shall write $T \not\models A$.

Exercise 2.3.2. Let L be an extension of L', M a structure of L, and M' the restriction of M to L'. Note that M and M' have the same individuals. Use the same constant as a name for an individual in M and M'. Show that a statement of $L'_{M'}$ is valid in M' if and only if it is valid in M.

Let M be a structure of L and $Th(M)$ the set of all sentences of L that are true in M. Then $Th(M)$ is called the *Theory of M*.

A class $\mathcal{M}$ of structures of a language L is called *elementary* if there is a theory T with language L such that elements of $\mathcal{M}$ are precisely the models of T. Thus, the classes of infinite sets, dense linearly ordered sets with no first element and no last element, groups, rings, fields, ordered fields, etc., are elementary classes in the corresponding languages.

A field $\mathbb{K}$ is called *algebraically closed* if every nonconstant polynomial $P(X) \in \mathbb{K}[X]$ has a root in $\mathbb{K}$. Let L be the language of rings. For each $n \geq 1$, let A_n denote the formula

$$\forall v_0 \cdots \forall v_n \exists v_{n+1} (v_0 + v_1 \cdot v_{n+1} + \cdots + v_n \cdot v_{n+1}^n = 0).$$

Then the class of all algebraically closed fields is elementary, axiomatized by axioms of fields and $\{A_n : n \geq 1\}$. ACF will denote the theory of algebraically closed fields, $ACF(0)$ that of algebraically closed fields of characteristic 0, and $ACF(p)$ that of algebraically closed fields of characteristic p, p being a prime.

Exercise 2.3.3. (i) Show that a ring with an identity has more than one element if and only if $0 \neq 1$.

(ii) Show that every algebraically closed field is infinite.
(iii) Show that if $\mathbb{K}$ is a nontrivial ordered field, then $0 < 1$.
(iv) Show that every nontrivial ordered field is of characteristic 0.
(v) Show that every nontrivial ordered field is order-dense.
(vi) Show that if $\mathbb{K}$ is an ordered field, then -1 cannot be written as a sum of squares of finitely many elements in $\mathbb{K}$.
(vii) Show that an algebraically closed field is not *orderable*, i.e., there is no linear order $<$ on the field making it into an ordered field.

Henceforth, we assume that if R is a ring with identity, then $0 \neq 1$.

Example 2.3.4. Let $(R, 0, 1, +, \cdot)$ be a commutative ring with identity. The *theory of left R-modules* has as its language an extension of abelian groups (with a constant symbol $0'$, a binary function symbol $+'$), and, for each $r \in R$, a unary function symbol $r\cdot$. Its axioms are those of abelian groups and the following sentences:

(1)
$$\forall x(1 \cdot x = x).$$

(2)
$$\forall x \forall y(r \cdot (x +' y) = r \cdot x +' r \cdot y).$$

(3)
$$\forall x((r+s) \cdot x = r \cdot x +' s \cdot x).$$

(4)
$$\forall x(r \cdot (s \cdot x) = (r \cdot s) \cdot x).$$

Models of the theory of left R-modules are called *left R-modules*. If, moreover, R is a field, then they are called *vector spaces over R*.

Let G be an abelian group. For any element $x \in G$, let nx denote the term

$$\underbrace{x + \cdots + x}_{n \text{ times}}.$$

We call a group G *divisible* if for every $n \geq 1$ and every $x \in G$ there exists a $y \in G$ such that $ny = x$. Call G *torsion-free* if for every $x \in G$, $x \neq 0$, and for every $n \geq 1$, $nx \neq 0$. Let $0 \neq x \in G$, and let there exist a positive integer n such $nx = 0$. We call the least such n the *order of x in G*.

Exercise 2.3.5. 1. Show that the class of divisible groups and that of torsion-free groups are elementary.
2. Show that every nontrivial ordered abelian group is torsion-free.
3. Let $n > 1$ be an integer. Show that the class of all nontrivial groups G such that every nonzero element in G is of order n is elementary. Also show that such an n must be prime.
4. Let G be a torsion-free, divisible abelian group. For any $x \in G$ and $n > 1$, show that there is a unique $y \in G$ such that $ny = x$. (Subsequently, we shall denote this y by x/n.)

The theories of divisible abelian groups and ordered divisible abelian groups will be denoted by *DAG* and *ODAG*, respectively.

Remark 2.3.6. For any rational number p/q, $q > 0$ relatively prime to p, define $(p/q)x = p(x/q)$. This makes G a vector space over the field $\mathbb{Q}$ of rationals. Further, if G is uncountable and B is a basis of G as a vector space over $\mathbb{Q}$, then B and G are of the same cardinality.

At this stage it is not possible to give examples of nonelementary classes. For instance, it will be proved later that the class of all finite sets is not elementary. Several more examples will be given later.

2.4 Embeddings and Isomorphisms

In this section we introduce notions analogous to subgroups of a group, isomorphisms of rings, isomorphic fields, etc. in the general context of first-order logic.

In the rest of this section, unless otherwise stated, M and N will denote structures of a fixed first-order language L.

For the sake of brevity, a sequence $(a_1,\ldots,a_n)\in N^n$ will sometimes be denoted by $\overline{a}$ and $(i_{a_1},\ldots,i_{a_n})$ by $i_{\overline{a}}$. Further, for any map $\alpha: N\to M$, $\alpha(\overline{a})$ will stand for the sequence $(\alpha(a_1),\ldots,\alpha(a_n))$.

An *embedding* of N into M is a one-to-one map $\alpha: N\to M$ satisfying the following conditions:

(1) For every constant symbol c of L,

$$\alpha(c_N)=c_M.$$

(2) For every n-ary function symbol f of L and every $\overline{a}\in N^n$,

$$\alpha(f_N(\overline{a}))=f_M(\alpha(\overline{a})).$$

(2) For every n-ary relation symbol p of L and every $\overline{a}\in N^n$,

$$p_N(\overline{a})\Leftrightarrow p_M(\alpha(\overline{a})),$$

i.e.,

$$\overline{a}\in p_N\Leftrightarrow \alpha(\overline{a})\in p_M.$$

If, moreover, $\alpha: N\to M$ is a surjection, we call $\alpha: N\to M$ an *isomorphism*. In this case, M and N are called *isomorphic structures*. An *automorphism* of M is an isomorphism from M onto itself.

If $N\subset M$ and the inclusion map $N\hookrightarrow M$ is an embedding, then N is called a *substructure* of M.

Remark 2.4.1. Let N be a subset of a structure M such that for each constant symbol c, $c_M\in N$, and for every function symbol f, N is closed under f_M. We then make N a substructure of M by setting

(i) For every constant symbol c of L,

$$c_N=c_M;$$

(ii) For every n-ary relation symbol p,

$$p_N = p_M \cap N^n,$$

the restriction of p_M to N; and

(iii) For every n-ary function symbol f,

$$f_N = f_M | N^n,$$

the restriction of f_M to N^n.

Example 2.4.2. Let L be the language of group theory. If H is a subgroup of a group G, then H is a substructure of G. If G and H are groups, then a group isomorphism $\alpha : G \to H$ is an isomorphism from the structure G to the structure H.

Note that if G is a group and $H \subset G$ a substructure, then H need not be a subgroup. It is just a subset of G that contains the identity of the group G and is closed under the group operation. For instance, $\mathbb{N} \subset \mathbb{Z}$, the group of all integers, is a substructure but not a subgroup of $\mathbb{Z}$. Similarly, a substructure R' of a ring R with identity is a subset of R containing 0 and 1 and closed under $+$ and $\cdot$, but it may not be a subring.

It will be convenient to have the substructures of a group be a subgroup and those of a ring be its subrings. *Thus, henceforth we shall take the following as the definition of the theory of rings.* Its language is the extension of the language of rings as defined earlier and one more binary function symbol $-$. Its axioms are the axioms of the rings and the following statement:

$$\forall x \forall y \forall z (x - y = z \leftrightarrow x = y + z).$$

Similarly, henceforth the language of groups is augmented with a binary function symbol $-$ and the preceding axiom.

Substructures of a field $\mathbb{F}$ are subrings $\mathbb{D}$ of $\mathbb{F}$ satisfying

$$\forall x \forall y (x \cdot y = 0 \to (x = 0 \vee y = 0)).$$

Such commutative rings with identity are called *integral domains*.

Exercise 2.4.3. Show that if $\mathbb{K}$ is a field, then the ring of polynomials $\mathbb{K}[X_1, \cdots, X_n]$ is an integral domain.

(*Hint*: Let $P(X_1, \cdots, X_n) \cdot Q(X_1, \cdots, X_n) = 0$ and $P \neq 0$. This means that not all coefficients of P are zero and all coefficients of $P \cdot Q$ are zero. By a suitable inductive argument, show that all the coefficients of Q are 0. Also note that this result is true for all integral domains $\mathbb{K}$.)

We now proceed to study the notion of embeddings, isomorphisms, etc. in complete generality. This general study, which is more in the spirit of logic, will turn out to be very useful.

Proposition 2.4.4. *Let $\alpha : N \to M$ be an embedding and $t[v_1, \ldots, v_n]$ a term of L, and let $\overline{a} \in N^n$. Then*

$$\alpha(t[i_{\overline{a}}]_N) = t[i_{\alpha(\overline{a})}]_M.$$

Proof. We prove the result by induction on the rank of t. If t is a variable v_i, then both terms equal $\alpha(a_i)$. If t is a constant c, then the term on the left is $\alpha(c_N)$ and that on the right is c_M. They are equal because α is an embedding.

Now assume that the result is true for $t_1, \ldots, t_k$ and t is the term $f(t_1, \ldots, t_k)$. Then

$$\begin{aligned} \alpha(t[i_{\overline{a}}]_N) &= \alpha(f_N(t_1[i_{\overline{a}}]_N, \ldots, t_k[i_{\overline{a}}]_N)) \\ &= f_M(\alpha(t_1[i_{\overline{a}}]_N), \ldots, \alpha(t_k[i_{\overline{a}}]_N)) \\ &= f_M(t_1[i_{\alpha(\overline{a})}]_M, \ldots, t_k[i_{\alpha(\overline{a})}]_M) \\ &= t[i_{\alpha(\overline{a})}]_M. \end{aligned}$$

The first equality holds by the definition of $t[i_{\overline{a}}]_N$, the second equality holds because α is an embedding, the third equality holds by the induction hypothesis, and the fourth equality holds by the definition of $t[i_{\alpha(\overline{a})}]_M$.

The proof is complete. □

Proposition 2.4.5. *Let $\alpha : N \to M$ be an embedding and $\varphi[v_1, \ldots, v_n]$ an open formula of L, and let $\overline{a} \in N^n$. Then*

$$N \models \varphi[i_{\overline{a}}] \Leftrightarrow M \models \varphi[i_{\alpha(\overline{a})}]. \tag{*}$$

Proof. Recall that the set of all open formulas is the smallest class of formulas that contains all atomic formulas and is closed under $\neg$ and $\vee$. Thus, the result will be proved if we show that the set of formulas φ satisfying $(*)$ contains all atomic formulas and is closed under $\neg$ and $\vee$.

By the definition of the truth in a structure, the definition of embedding, and Proposition 2.4.4, $(*)$ holds for formulas of the form $t = s$ as well as for atomic formulas of the form $p(t_1, \ldots, t_n)$.

Now assume that φ is the formula $\neg\psi$ and the result is true for ψ. Then

$$\begin{aligned} N \models \varphi[i_{\overline{a}}] &\Leftrightarrow N \not\models \psi[i_{\overline{a}}] \\ &\Leftrightarrow M \not\models \psi[i_{\alpha(\overline{a})}] \\ &\Leftrightarrow M \models \varphi[i_{\alpha(\overline{a})}]. \end{aligned}$$

The first and last equivalences hold because the formulas $\psi[i_{\overline{a}}]$ and $\psi[i_{\alpha(\overline{a})}]$ are closed; the second equivalence holds by the induction hypothesis.

The case φ of the form $\psi \vee \eta$ is dealt with similarly:

$$\begin{aligned} N \models \varphi[i_{\overline{a}}] &\Leftrightarrow N \models \psi[i_{\overline{a}}] \text{ or } N \models \eta[i_{\overline{a}}] \\ &\Leftrightarrow M \models \psi[i_{\alpha(\overline{a})}] \text{ or } M \models \eta[i_{\alpha(\overline{a})}] \\ &\Leftrightarrow M \models \varphi[i_{\alpha(\overline{a})}]. \end{aligned}$$

The proof is complete. □

Exercise 2.4.6. Let $\alpha : N \to M$ be a map such that for every atomic $\varphi[v_1,\dots,v_n]$ and every $\overline{a} \in N^n$,

$$N \models \varphi[i_{\overline{a}}] \Leftrightarrow M \models \varphi[i_{\alpha(\overline{a})}].$$

Show that φ is an embedding.

(*Hint*: To show that for any constant symbol c, $\alpha(c_N) = c_M$, let the formula $\varphi[x]$ be $c = x$ and consider $\varphi[i_{c_N}]$; to show that for $a, b \in N$, $\alpha(a) = \alpha(b)$ implies $a = b$, let $\varphi[x,y]$ be the formula $x = y$ and consider $\varphi[i_a, i_b]$, etc.)

Our next result gives a method to build an extension of a structure. Let M be a structure of a first-order language L. We define the *atomic diagram* , or simply the *diagram* of M, denoted by $Diag(M)$, by

$$Diag(M) = \{\varphi[i_{\overline{a}}] : \overline{a} \in M, M \models \varphi[i_{\overline{a}}], \varphi \text{ an atomic formula of } L\}.$$

Proposition 2.4.7. *If $N \models Diag(M)$, then M has an embedding into N.*

Proof. For $a \in M$, take $\alpha(a) = (i_a)_N$. By Exercise 2.4.6, $\alpha : M \to N$ is an embedding. □

Theorem 2.4.8. *Let $\alpha : N \to M$ be an isomorphism and $\varphi[v_1,\dots,v_n]$ a formula of L_N. Then for every $\overline{a} \in N^n$,*

$$N \models \varphi[i_{\overline{a}}] \Leftrightarrow M \models \varphi[i_{\alpha(\overline{a})}]. \qquad (**)$$

In particular, for every sentence φ of L, $N \models \varphi$ if and only if $M \models \varphi$.

Proof. Since an isomorphism is an embedding, by the arguments contained in the proof of Proposition 2.4.5, the set of all formulas φ satisfying $(**)$ contains all atomic formulas and is closed under $\neg$ and $\vee$.

Let $\varphi[v_1,\dots,v_n]$ be a formula of the form $\exists v \psi$, with v different from each of the v_i. Suppose $(**)$ holds for ψ and all $(a, a_1,\dots,a_n) \in N^{n+1}$. To complete the proof, we now have only to show that $(**)$ holds for φ and every $\overline{a} \in N^n$. Thus, we take any $\overline{a} \in N^n$. Then

$$\begin{aligned} N \models \varphi[i_{\overline{a}}] &\Leftrightarrow N \models \psi[i_a, i_{\overline{a}}] \text{ for some } a \in N \\ &\Leftrightarrow M \models \psi[i_{\alpha(a)}, i_{\alpha(\overline{a})}] \text{ for some } a \in N \\ &\Leftrightarrow M \models \psi[i_b, i_{\alpha(\overline{a})}] \text{ for some } b \in M \\ &\Leftrightarrow M \models \varphi[i_{\alpha(\overline{a})}]. \end{aligned}$$

The first equivalence holds by the definition of validity in N, the second equivalence holds by the induction hypothesis, the third equivalence holds because α is surjective, and the last equivalence holds by the definition of validity in M.

The proof is complete. □

An embedding $\alpha : N \to M$ is called an *elementary embedding* if for every formula $\varphi[v_1,\dots,v_n]$ and every $\overline{a} \in N^n$,

$$N \models \varphi[i_{\overline{a}}] \Leftrightarrow M \models \varphi[i_{\alpha(\overline{a})}].$$

If $N \subset M$ and the inclusion $N \hookrightarrow M$ is an elementary embedding, then we say that N is an *elementary substructure* of M or that M is an *elementary extension* of N. The structures N and M are called *elementarily equivalent* if for every closed formula φ,

$$N \models \varphi \Leftrightarrow M \models \varphi.$$

We write $N \equiv M$ if N and M are elementarily equivalent. Clearly, $\equiv$ is an equivalence relation on the class of all structures of L.

Below we present a method to build an elementary extension of a structure. Let M be a structure of a first-order language L. We define the *elementary diagram* of M, denoted by $Diag_{el}(M)$, by

$$Diag_{el}(M) = \{\varphi[i_{\overline{a}}] : \overline{a} \in M, M \models \varphi[i_{\overline{a}}],\ \varphi \text{ a formula of } L\}.$$

As before, we have the following result.

Proposition 2.4.9. *If $N \models Diag_{el}(M)$, then M has an elementary embedding into N.*

Remark 2.4.10. By Theorem 2.4.8, two structures N and M are elementarily equivalent if they are isomorphic. Later on in the book we shall show that any two algebraically closed fields of characteristic 0 are elementarily equivalent. But the field $\overline{\mathbb{Q}}^{\mathrm{alg}}$ of algebraic numbers and the field $\mathbb{C}$ of complex numbers are two algebraically closed fields of characteristic 0 that are not even of the same cardinality. Hence, elementarily equivalent structures need not be isomorphic. Later in these pages we shall show that an elementary embedding $\alpha : N \to M$ need not be surjective.

Theorem 2.4.11. *Let N be a substructure of M. Then N is an elementary substructure of M if and only if for every formula $\varphi[v, v_1, \ldots, v_n]$ and for every $\overline{a} \in N^n$, if there is a $b \in M$ satisfying*

$$M \models \varphi[i_b, i_{\overline{a}}],$$

then there is a $b \in N$ satisfying

$$M \models \varphi[i_b, i_{\overline{a}}].$$

Proof. Let N be an elementary substructure of M. Take a formula $\varphi[v, v_1, \ldots, v_n]$. Let $\overline{a} \in N^n$, and suppose there is a $b \in M$ satisfying $M \models \varphi[i_b, i_{\overline{a}}]$. This means that $M \models \exists v \varphi[v, i_{\overline{a}}]$. Since N is an elementary substructure of M, we have $N \models \exists v \varphi[v, i_{\overline{a}}]$. Thus, there is a $b \in N$ satisfying $N \models \varphi[i_b, i_{\overline{a}}]$. Since N is an elementary substructure of M, $M \models \varphi[i_b, i_{\overline{a}}]$.

We prove the *if* part of the result by showing that for every formula $\psi[v_1, \ldots, v_n]$ and for every $\overline{a} \in N^n$,

$$N \models \psi[i_{\overline{a}}] \Leftrightarrow M \models \psi[i_{\overline{a}}]. \tag{*}$$

We shall prove $(*)$ by induction on the rank of ψ. By Proposition 2.4.5, $(*)$ is true for all atomic formulas. Arguing as in the proof of that proposition, we can show that if $(*)$ is true for φ, then it is true for $\neg\varphi$, and if φ and ψ satisfy $(*)$, then so does $\varphi \vee \psi$.

Now assume that $\varphi[v_1,\ldots,v_n]$ is a formula of the form $\exists v\psi[v,v_1,\ldots,v_n]$ and $(*)$ holds for ψ and every $(a,a_1,\ldots,a_n) \in N^{n+1}$. Take $\overline{a} \in N^n$.

Suppose $N \models \varphi[i_{\overline{a}}]$. Then there is a $b \in N$ such that $N \models \psi[i_b, i_{\overline{a}}]$. By the induction hypothesis, $M \models \psi[i_b, i_{\overline{a}}]$. Thus, $M \models \varphi[i_{\overline{a}}]$.

Now assume that $M \models \varphi[i_{\overline{a}}]$. So there is a $b \in M$ such that $M \models \psi[i_b, i_{\overline{a}}]$. By our assumptions, there is a $b \in N$ such that $M \models \psi[i_b, i_{\overline{a}}]$. By the induction hypothesis, $N \models \psi[i_b, i_{\overline{a}}]$. Thus, $N \models \varphi[i_{\overline{a}}]$. □

2.5 Some Examples

Let $L(<)$ be a language with only one binary relation symbol $<$.

Proposition 2.5.1. *If $(M,<)$ is a countable linearly ordered set, then there is an embedding $\alpha : M \to \mathbb{Q}$, where $\mathbb{Q}$ is the set of all rational numbers with usual ordering.*

Proof. Let $r_0, r_1, \ldots$ be an enumeration of M such that the r_i are distinct. We define $\alpha(r_n)$ by induction on n. Set $\alpha(r_0) = 0$. Suppose $n > 0$, and $\alpha : \{r_i \in M : i < n\} \to \mathbb{Q}$ has been defined so that it is order-preserving. Since $\mathbb{Q}$ is a dense linearly ordered set with no first element and no last element, there is a $\alpha(r_n) \in \mathbb{Q}$ such that $\alpha : \{r_i \in M : i \le n\} \to \mathbb{Q}$ is order-preserving. Thus we have defined an embedding $\alpha : M \to \mathbb{Q}$. □

Theorem 2.5.2. *Any two countable models $\mathbb{Q}_1$ and $\mathbb{Q}_2$ of DLO are isomorphic.*

Proof. Let $\{r_n\}$ and $\{s_m\}$ be enumerations of $\mathbb{Q}_1$ and $\mathbb{Q}_2$, respectively. Set $n_0 = 0$ and $m_0 = 0$. Suppose for some i, $n_0,\ldots,n_{2i}$ and $m_0,\ldots,m_{2i}$ have been defined so that the map f defined by

$$f(r_{n_j}) = s_{m_j},\ 0 \le j \le 2i,$$

is injective and order-preserving. Now let m_{2i+1} be the first natural number k such that s_k is different from each s_{m_j}, $j \le 2i$. Show that there is a natural number l such that r_l is different from each r_{n_j}, $j \le 2i$, and the extension of f sending r_l to $s_{m_{2i+1}}$ is order-preserving. Set n_{2i+1} to be the first such l. Thus, the map $f(r_{n_j}) = s_{m_j}$, $j \le 2i+1$, is injective and order-preserving. Now define n_{2i+2} to be the first natural number l such that r_l is different from each r_{n_j}, $j \le 2i+1$. Again, observe that there is a natural number k such that s_k is different from each s_{m_j}, $j \le 2i+1$, and the extension of the preceding map by defining $f(r_{n_{2i+2}}) = s_k$ is order-preserving. Set s_{2i+2} to be the least such k. It is easily checked that $f : \mathbb{Q}_1 \to \mathbb{Q}_2$ is an isomorphism. □

Remark 2.5.3. The method of the foregoing proof is fairly common and will be repeated several times. It is known as the back-and-forth argument.

Exercise 2.5.4. Let $A \subset \mathbb{Q}$ be finite and $f : A \to \mathbb{Q}$ be an order-preserving, one-to-one map. Show that there is an order-preserving bijection $g : \mathbb{Q} \to \mathbb{Q}$ extending f.

Proposition 2.5.5. *Two divisible torsion-free abelian uncountable groups G_1 and G_2 are isomorphic if and only if they are of the same cardinality.*

Proof. We need to prove the *if* part only. Since the G_i are uncountable and of the same cardinality, they are of the same dimension as vector spaces over $\mathbb{Q}$. Hence, G_1 and G_2 are isomorphic as vector spaces over $\mathbb{Q}$. In particular, they are isomorphic as groups. □

Corollary 2.5.6. *The additive groups of real and complex numbers are isomorphic.*

Exercise 2.5.7. Show that the theory of divisible, torsion-free abelian groups has exactly $\aleph_0$-many nonisomorphic countable models such that any other countable model is isomorphic to one of these models.

Proposition 2.5.8. *Let $\mathbb{D}$ be an integral domain. Then there is a field $\mathbb{F}$ and an embedding $q : \mathbb{D} \to \mathbb{F}$ such that for every field $\mathbb{K}$ and every embedding $r : \mathbb{D} \to \mathbb{K}$, there is a unique embedding $s : \mathbb{F} \to \mathbb{K}$ such that $s \circ q = r$.*

We give only a sketch of the proof. The routine verifications are left to the reader as an exercise.

Proof. Set

$$E = \{(a,b) \in \mathbb{D} \times \mathbb{D} : b \neq 0\}.$$

We define an equivalence relation $\sim$ on E by

$$(a,b) \sim (c,d) \Leftrightarrow a \cdot d = b \cdot c$$

and set

$$\mathbb{F} = E/\sim \; = \left\{ \frac{a}{b} : (a,b) \in E \right\},$$

the set of all $\sim$-equivalence classes, i.e., $\frac{a}{b}$ denotes the equivalence class containing (a,b). We define

$$0 = \frac{0}{1}, 1 = \frac{1}{1},$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd},$$

$$\frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd}$$

and

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

It is easily checked that these are well defined and make $\mathbb{F}$ a field.

Now define $q : \mathbb{D} \to \mathbb{F}$ by

$$q(a) = \frac{a}{1}, a \in \mathbb{D}.$$

Then $q : \mathbb{D} \to \mathbb{F}$ is an embedding.

Given any embedding r of $\mathbb{D}$ into a field $\mathbb{K}$, define $s : \mathbb{F} \to \mathbb{K}$ by

$$s(\frac{a}{b}) = r(a) \cdot r(b)^{-1}, \ \ \frac{a}{b} \in \mathbb{F}. \qquad \square$$

It is easy to verify that if $q' : \mathbb{D} \to \mathbb{F}'$ is another such pair, then there is an isomorphism $h : \mathbb{F}' \to \mathbb{F}$ such that $h \circ q' = q$. In particular, $\mathbb{F}$ is unique up to isomorphism. Such an $\mathbb{F}$ is called the *quotient field* of $\mathbb{D}$.

Example 2.5.9. The field of rational numbers $\mathbb{Q}$ is the quotient field of the ring of integers $\mathbb{Z}$.

Example 2.5.10. If $\mathbb{K}[X_1, \cdots, X_n]$ is the ring of polynomials over a field $\mathbb{K}$, then its quotient field is denoted by $\mathbb{K}(X_1, \cdots, X_n)$. Its elements are called *rational functions over* $\mathbb{K}$. As described previously, its elements can be thought of as the formal quotients of two polynomials.

Similar results are true for torsion-free abelian groups and ordered abelian groups.

Proposition 2.5.11. *Let H be a torsion-free abelian group. Then there is a torsion-free, divisible abelian group G and an embedding $\alpha : H \to G$ such that for every torsion-free, divisible abelian group G' and every embedding $\beta : H \to G'$, there is a unique embedding $\gamma : G \to G'$ such that $\beta = \gamma \circ \alpha$.*

Proof. Set

$$E = \{(h, n) : h \in H, n > 0\}.$$

Define an equivalence relation $\sim$ on E by

$$(h, n) \sim (h', n') \Leftrightarrow n'h = nh'.$$

Let $\frac{h}{n}$ denote the equivalence class containing $(h, n) \in E$, and set

$$G = E/\sim \ = \left\{ \frac{h}{n} : (h, n) \in E \right\},$$

$$0 = \frac{0}{1},$$

$$\frac{h}{n} + \frac{h'}{n'} = \frac{n'h + nh'}{nn'},$$

and

$$\alpha(h) = \frac{h}{1}, h \in H.$$

Then these are well defined and make G a group with $\alpha : H \to G$ an embedding. Now given a torsion-free, divisible abelian group G' and an embedding $\beta : H \to G'$, define $\gamma : G \to G'$ by

$$\gamma\left(\frac{h}{n}\right) = \frac{\beta(h)}{n}, \quad \frac{h}{n} \in G,$$

where $\frac{\beta(h)}{n}$ is the unique element g of G' such that $ng' = \beta(h)$. $\square$

The group G obtained above is unique up to isomorphism and is called the *divisible hull* of H.

Proposition 2.5.12. *Let H be an ordered abelian group. Then there is a divisible, ordered abelian group G and an embedding $\alpha : H \to G$ such that for every divisible, ordered abelian group G' and every embedding $\beta : H \to G'$ there is a unique embedding $\gamma : G \to G'$ such that $\beta = \gamma \circ \alpha$.*

Proof. Let $<$ denote the ordering on H. Recall that every ordered abelian group is torsion-free. We proceed as in the proof of Proposition 2.5.11 and define

$$\frac{h}{n} < \frac{h'}{n'} \Leftrightarrow n'h < nh'. \qquad \square$$

The ordered abelian group G is unique up to isomorphism and is called an *ordered divisible hull* of H.

A ring R is called orderable if there is a linear order $<$ on R such that for every $x, y, z \in R$ the following conditions are satisfied.

1. $0 < x$ and $0 < y$ imply $0 < x \cdot y$.
2. $x < y$ implies $x + z < y + z$.

Let D be an ordered integral domain and $\mathbb{K}$ its quotient field. Note that every element of $\mathbb{K}$ can be expressed in the form $\frac{c}{d} \in \mathbb{K}$ with $d > 0$.

Proposition 2.5.13. *Let D be an ordered integral domain and $\mathbb{K}$ its quotient field. For $\frac{a}{b}, \frac{c}{d} \in \mathbb{K}$ with $b, d > 0$, define*

$$\frac{a}{b} < \frac{c}{d} \Leftrightarrow a \cdot d < b \cdot c$$

and

$$\alpha(a) = \frac{a}{1}, \; a \in D.$$

This makes the quotient field $\mathbb{K}$ an ordered field with $\alpha : D \to \mathbb{K}$ an order-preserving embedding. Further, for every ordered field $\mathbb{F}$ and every order-preserving embedding $\beta : D \to \mathbb{F}$, there is a unique order-preserving embedding $\gamma : \mathbb{K} \to \mathbb{F}$ such that $\gamma \circ \alpha = \beta$.

Its entirely trivial proof is left to the reader as an exercise.

2.6 Homogeneous Structures

Let M and N be structures for a language L and $A \subset M$. A map $f : A \to N$ is called *partial elementary* if for every formula $\varphi[\overline{x}]$ and every $\overline{a} \in A$,

$$M \models \varphi[i_{\overline{a}}] \Leftrightarrow N \models \varphi[i_{f(\overline{a})}].$$

Note that a partial elementary map must be injective. Also, if f is partial elementary, then so is f^{-1}.

Remark 2.6.1. If $A = \emptyset \subset M$, then $f : A \to N$ (the empty function) is partial elementary if and only if M and N are elementarily equivalent. In particular, if for some $A \subset M$ there is a partial elementary map $f : A \to N$, then M and N are necessarily elementarily equivalent.

Let κ be an infinite cardinal. We call M *κ-homogeneous* if for all $A \subset M$ of cardinality less than κ, for all partial elementary maps $f : A \to M$, and for all $a \in M$, there is a partial elementary map $g : A \cup \{a\} \to M$ extending f. We call M *homogeneous* if it is $|M|$-homogeneous, where $|M|$ denotes the cardinality of M. We call a theory T *homogeneous* if all its models are homogeneous.

Example 2.6.2. The linearly ordered set of rationals $\mathbb{Q}$ is homogeneous. Let $A \subset \mathbb{Q}$ be finite and $f : A \to \mathbb{Q}$ a partial elementary. Then f is an order-preserving injection. In a slight modification of the argument contained in the proof of Theorem 2.5.2, we see that there is an order-preserving bijection $g : \mathbb{Q} \to \mathbb{Q}$ extending f. Thus, for every formula $\varphi[\overline{x}]$ and every $\overline{a} \in Q$,

$$\mathbb{Q} \models \varphi[i_{\overline{a}}] \Leftrightarrow \mathbb{Q} \models \varphi[i_{g(\overline{a})}].$$

Our contention now follows.

Following the back-and-forth argument, we have the following theorem.

Theorem 2.6.3. *Let M be a countable homogeneous structure of a language L, and let $A \subset M$ be finite. Then every partial elementary map $f : A \to M$ can be extended to an automorphism of M.*

Proof. Fix an enumeration $\{x_n\}$ of the elements of M. Set $f_{-1} = f$. We shall define a sequence $\{f_n\}$ of finite partial elementary maps such that for every n, f_{n+1} extends f_n and x_n belongs to the domain as well as to the range of f_n.

Assume f_n is defined. If $x_{n+1} \in domain(f_n)$, then set $g = f_n$. If $x_{n+1} \notin domain(f_n)$, then, by homogeneity, there is a partial elementary $g : domain(f_n) \cup \{x_{n+1}\} \to M$. Now, if $x_{n+1} \in range(g)$, then we set $f_{n+1} = g$. Otherwise, we take f_{n+1} to be the inverse of a partial elementary map $h : range(g) \cup \{x_{n+1}\} \to M$ extending g^{-1}, which exists by the homogeneity of M.

The map $f_\infty = \cup_n f_n$ is an automorphism of M extending f. $\square$

Using the method of transfinite induction we can easily see that this result can be extended to all homogeneous structures as follows.

Theorem 2.6.4. *Let M be a homogeneous structure of a language L and $A \subset M$ of cardinality less than that of M. Then every partial elementary map $f : A \to M$ can be extended to an automorphism of M.*

Proof. We assume that $|M| > \aleph_0$. Enumerate $M \setminus A = \{a_\alpha : \alpha < |M|\}$, and set $f_0 = f$. By transfinite induction, for each $\alpha < |M|$, we define a partial elementary map $f_\alpha : A \cup \{a_\beta : \beta < \alpha\}$ such that for $\beta < \alpha < |M|$, f_α extends f_β.

Suppose $f_\alpha : A \cup \{a_\beta : \beta < \alpha\} \to M$ has been defined and is partial elementary. Since $|A \cup \{a_\beta : \beta < \alpha\}| < |M|$, by homogeneity, there is a partial elementary extension $f_{\alpha+1} : A \cup \{a_\beta : \beta \leq \alpha\} \to M$ of f_α.

If α is a limit ordinal and f_β, $\beta < \alpha$, have been defined, then we take $f_\alpha = \cup_{\beta<\alpha} f_\beta$. Finally, $g = \cup_{\alpha<|M|} f_\alpha : M \to M$ is a partial elementary map that extends f. □

Let M be a structure for a language L and $\overline{a} \in M^n$. We define

$$tp^M(\overline{a}) = \{\varphi[\overline{x}] : M \models \varphi[i_{\overline{a}}]\}$$

and call it a *complete n-type realized by* $\overline{a}$. Types play a very important role in model theory. $tp^M(\overline{a})$ may be thought of as the set of all properties $\varphi[\overline{x}]$ satisfied by $\overline{a}$.

Theorem 2.6.5. *Let M be a homogeneous structure for a language L and $\overline{a}, \overline{b} \in M^n$. Then $tp^M(\overline{a}) = tp^M(\overline{b})$ if and only if there is an automorphism $\alpha : M \to M$ with $\alpha(\overline{a}) = \overline{b}$.*

Proof. Observe that $tp^M(\overline{a}) = tp^M(\overline{b})$ if and only if the map $\overline{a} \to \overline{b}$ is partial elementary and use Theorem 2.6.4. □

Using the back-and-forth argument, we get the following proposition.

Proposition 2.6.6. *Let M and N be countable homogeneous structures for a language L such that for every $k \geq 1$,*

$$\{tp^M(\overline{a}) : \overline{a} \in M^k\} = \{tp^N(\overline{b}) : \overline{b} \in N^k\}.$$

Then M and N are isomorphic.

Proof. Fix enumerations $\{a_k\}$ and $\{b_k\}$ of M and N, respectively.

Set $a'_0 = a_0$, and consider $tp^M(a'_0)$. By our hypothesis, there is a $b \in N$ such that $tp^M(a'_o) = tp^N(b)$. Let b'_0 be the first such b in the preceding enumeration of N.

Now let b'_1 be the first element in the enumeration of N different from b'_0. By our hypothesis, there exist $a, a' \in M$ such that $tp^M(a,a') = tp^N(b'_0, b'_1)$. In particular, $tp^M(a) = tp^N(b'_0) = tp^M(a'_0)$. Thus, $a \to a'_0$ is partial elementary. Since M is homogeneous, there is an $a'' \in M$ such that $(a,a') \to (a'_0, a'')$ is partial elementary. Therefore, $tp^N(b'_0, b'_1) = tp^M(a,a') = tp^M(a'_0, a'')$. Since $b'_0 \neq b'_1$, $x \neq y$ is in $tp^N(b'_0, b'_1)$. This implies that $a'_0 \neq a''$. We let a'_1 denote the first such a'' in the enumeration of M.

Now let a'_2 be the first element in the enumeration of M not belonging to $\{a'_0, a'_1\}$. By our hypothesis, there exist $b, b', b'' \in N$ such that $tp^N(b, b', b'') = tp^M(a'_0, a'_1, a'_2)$. In particular, $tp^N(b, b') = tp^M(a'_0, a'_1) = tp^N(b'_0, b'_1)$. Thus, $(b, b') \to (b'_0, b'_1)$ is partial elementary. Since N is homogeneous, there exists a $b''' \in N$ such that $(b, b', b'') \to (b'_0, b'_1, b''')$ is partial elementary. Hence, $tp^N(b'_0, b'_1, b''') = tp^N(b, b', b'') = tp^M(a'_0, a'_1, a'_2)$. Since $a'_2 \notin \{a'_0, a'_1\}$, $b''' \notin \{b'_0, b'_1\}$. Let b'_2 be the first such b''' in the enumeration of N.

Continuing this back-and-forth method, we shall get enumerations $\{a'_k\}$ and $\{b'_k\}$ of M and N, respectively, such that for every k, $(a'_o, \cdots, a'_k) \to (b'_o, \cdots, b'_k)$ is partial elementary. Plainly, $a'_i \to b'_i$ defines an isomorphism from M to N. □

2.7 Downward Löwenheim–Skolem Theorem

In this section we present a method of constructing elementary substructures of small cardinality. From this it will follow that if a countable theory has a model, then it has a countable model. In particular, if there is a model of set theory, then there is a countable model of set theory. This is an important result in set theory. In Chap. 5, we will present a method to construct elementary extensions of arbitrarily large cardinalities.

Theorem 2.7.1 (Downward Löwenheim–Skolem theorem). *Let M be a structure of L and $X \subset M$. Suppose L has at most κ nonlogical symbols and κ an infinite cardinal number. Then there is an elementary substructure N of M such that $X \subset N$ and the cardinality of N is at most* $\max(\kappa, |X|)$*, where $|X|$ denotes the cardinality of X.*

Proof. Essentially, our N will be the smallest subset of M containing X satisfying the following conditions:

(i) Each $c_M \in N$, where c is a constant symbol of L.
(ii) The set N is closed under f_M for every function symbol f of L.
(iii) Whenever a sentence of the form $\exists v\varphi$ is valid in M, there is an element $a \in N$ such that $M \models \varphi_v[i_a]$.

By induction on k, we shall define

$$N_0 \subset N'_1 \subset N_1 \subset \ldots \subset N_k \subset N'_k \subset N_{k+1} \subset \ldots \subset M$$

such that each N'_k is a substructure of N and for every formula of the form $\exists v\varphi[v, v_1, \ldots, v_n]$ and every $\overline{a} \in N_k'^n$, if $M \models \exists v\varphi[v, i_{\overline{a}}]$, then there is a $b \in N_{k+1}$ such that $M \models \varphi[i_b, i_{\overline{a}}]$. Further, each N_k is of cardinality $\leq \max(\kappa, |X|)$.

Let N_0 be the smallest subset of M containing X that contains all c_M and that is closed under all f_M. Note that $|N_0| \leq \max(\kappa, |X|)$ and that N_0 is a substructure of M.

Suppose N_k has been defined such that $|N_k| \leq \max(\kappa, |X|)$. Now we define N'_k and N_{k+1}. Let N'_k be the smallest subset of M containing N_k that is closed under all f_M. Then $|N'_k| \leq \max(\kappa, |X|)$.

Fix a formula of the form $\varphi[v, v_1, \ldots, v_n]$. Let ψ be the formula $\exists v \varphi$. For every $\overline{a} = (a_1, \ldots, a_n) \in (N'_k)^n$, whenever $M \models \psi[i_{\overline{a}}]$, there is a $b \in M$ such that $M \models \varphi[i_b, i_{\overline{a}}]$. Choose and fix one such b. Let N_{k+1} be obtained from N'_k by adding all the b thus chosen. Again note that $|N_{k+1}| \leq \max(\kappa, |X|)$.

Set

$$N = \cup_k N_k.$$

Then:

(i) For every constant symbol c, $c_M \in N$;
(ii) For every function symbol f, N is closed under f_M;
(iii) $|N| \leq \max(\kappa, |X|)$ and $X \subset N$.

Thus, N is a substructure of M as in Remark 2.4.1.

Let $\varphi[v_1, \ldots, v_n]$ be any formula and $\overline{a} \in N^n$. Since N is a substructure of M, by Theorem 2.4.11, the proof will be complete if we show that for every formula $\varphi[v, v_1, \ldots, v_n]$ and for every $\overline{a} \in N^n$, if there is a $b \in M$ satisfying $M \models \varphi[i_b, i_{\overline{a}}]$, then there is a $b \in N$ satisfying $M \models \varphi[i_b, i_{\overline{a}}]$. Let $\varphi[v, v_1, \ldots, v_n]$ be a formula, and let $\overline{a} \in N^n$ and $b \in M$ be such that $M \models \varphi[i_b, i_{\overline{a}}]$. Since $N_k \subset N_{k+1}$ for all k, there is a natural number p such that each $a_i \in N_p$. By the definition of N_{p+1}, there is a $b \in N_{p+1} \subset N$ such that $M \models \varphi[i_b, i_{\overline{a}}]$. □

Remark 2.7.2. In the foregoing proof we used an important axiom of set theory called the axiom of choice.

Axiom of choice: If $\{X_i : i \in I\}$ is a family of nonempty sets, then there is a map $f : I \to \cup_{i \in I} X_i$ such that $f(i) \in X_i$ for all $i \in I$.

A function f satisfying the conclusion of the axiom of choice is called a *choice function* for the family $\{X_i : i \in I\}$. The axiom of choice asserts only the existence of a choice function – it gives no method to produce a choice function.

The theory obtained by adding the axiom of choice to the axioms of *ZF* is denoted by *ZFC*.

Corollary 2.7.3. *If a countable theory has a model, then it has a countable model.*

Corollary 2.7.4. *If ZF (or ZFC) has a model, then it has a countable model M.*

Remark 2.7.5. This seemingly paradoxical result calls for an explanation. First, we call a set x *transitive* if $y \in x \Rightarrow y \subset x$. In *ZF*, it can be shown that if M is a countable model of *ZF*, then it has a countable transitive model. Thus, we assume that M is countable and transitive.

Now, *ZF* proves that *there is an uncountable set*. Since M is a model of *ZF*, this statement is true in the model M. In particular, there is a set x in M such that

$$M \models |x| > \aleph_0.$$

Since M is transitive, $x \subset M$. But M itself is countable!

In the real world V (a model of ZFC in the present case, assuming that it exists), M is countable. Thus, in the real world there is a function f from $\mathbb{N}$ onto x. We have not asserted that such an $f \in M$. And in our situation, no such f belongs to M. This is not a contradiction at all.

Let $(R,<)$ be a linearly ordered set and $A \subset R$. An element u of R is called an *upper bound of* A if for every $a \in A$, $a \leq u$, where $x \leq y$ means that either $x < y$ or $x = y$. If u is an upper bound of A and no $v < u$ is an upper bound of A, then u is called the *least upper bound* of A. A linearly ordered set R is called *complete* if every nonempty subset A of R that has an upper bound has a least upper bound.

Proposition 2.7.6 (Cantor). *Every complete, order-dense, linearly ordered set $(R,<)$ with more than one element is uncountable.*

Proof. If possible, assume that R is countable. We shall arrive at a contradiction. Fix an enumeration $R = \{r_n\}$ of R. Let $x_0 < y_0$ be two distinct points of R. Since R is order-dense, there is a $x \in R$ such that $x_0 < x < y_0$. Let n be the first integer such that $x_0 < r_n < y_0$. Set $x_1 = r_n$. Since R is order-dense, there is a $y \in R$ such that $x_1 < y < y_0$. Set $y_1 = r_m$, where m is the first natural number with $x_1 < r_m < y_0$. Assuming, $x_0 < \cdots < x_n < y_n < \cdots < y_0$ have been defined, set x_{n+1} to be the first r_l such that $x_n < r_l < y_n$. Then take y_{n+1} to be the first r_k such that $x_{n+1} < r_k < y_n$.

Since $\{x_n\}$ is bounded above, it has a least upper bound, say r_p. Clearly, $r_p \leq y_n$ for all n. But, by our construction, no r_p can be the least upper bound of $\{x_n\}$. This contradiction proves our result. □

Here is an interesting corollary.

Corollary 2.7.7. *Let $L = L(<)$ be a language with only one nonlogical symbol, a binary relation symbol. Then the class $\mathcal{M}$ of all complete, order-dense, linearly ordered $L(<)$-structures with more than one point is not elementary.*

Proof. Suppose T is a theory with language $L(<)$ whose models are precisely the structures in $\mathcal{M}$. Clearly, T has a model. Since T is countable, T has a countable model. But, by Cantor's theorem, no structure in $\mathcal{M}$ is countable. □

Exercise 2.7.8. Show that the class of all complete ordered fields is not elementary.

2.8 Definability

In this section, we introduce the interesting and important notion of definability. This gives rise to interesting questions and applications in mathematics, which is very important from a logic point of view, too. For instance, this formed the basis for Gödel's model of constructible sets in which the axiom of choice and the continuum hypothesis hold. This also plays an important role in decidability questions pertaining to models.

Throughout this section, unless otherwise stated, M will stand for a structure of a language L.

For $n \geq 1$, $X \subset M^n$ is called *definable* (in the language L) if there is a formula $\varphi[v_1, \cdots, v_n, w_1, \cdots, w_m]$ of L and a $\overline{b} \in M^m$ such that

$$\overline{a} \in X \Leftrightarrow M \models \varphi[i_{\overline{a}}, i_{\overline{b}}].$$

$\overline{b}$ is called the *parameters*. If the parameters come from a subset A of M, we call X A-definable. Note that if X is definable, it is A-definable for some finite $A \subset M$. A function $f : M^k \to M^l$ is called definable if its graph is definable. An element $a \in M$ is called A-definable if the singleton set $\{a\}$ is A-definable.

Example 2.8.1. Let M be a structure for a language L. Then every finite $D \subset M^n$ is definable. To see this when $n = 1$, let $D = \{a_1, \cdots, a_k\} \subset M$. Then the formula $\vee_{i=1}^{k}(x = i_{a_i})$ defines D. The proof for $n > 1$ is left to the reader as an exercise.

Example 2.8.2. If c, f, and p are respectively constant, function, and relation symbols of L, then their interpretations c_M, f_M, and p_M are $\emptyset$-definable. The formula $x = c$ defines c_M, the formula $y = fx_1 \cdots x_n$ defines f_M, with f an n-ary function symbol, whereas the formula $py_1 \cdots y_m$ defines p_M, with p an m-ary relation symbol.

Since formulas are described inductively, it is natural to expect an inductive definition of definable sets, which we present in the next lemma. Its entirely routine proof is left as an exercise for the reader. For a set M, a family of subsets of M^n, $n \geq 1$, will be called a *pointclass*.

Lemma 2.8.3. *Let M be a structure of a language L. The pointclass of all definable subsets of M^n, $n \geq 1$, is the smallest pointclass $\mathcal{D}$ satisfying the following conditions:*

1. *$\{c_M\}$, p_M and the graph of f_M, c, p, and f respectively constant, relation, and function symbols of L, belong to $\mathcal{D}$.*
2. *The set $\{\overline{a} \in M^n : a_i = a_j\} \in \mathcal{D}$, $1 \leq i < j \leq n$.*
3. *If $A \subset M^{n+m}$ is in $\mathcal{D}$ and $\overline{b} \in M^m$, then the section*

$$A_{\overline{b}} = \{\overline{a} \in M^n : (\overline{a}, \overline{b}) \in A\} \in \mathcal{D}.$$

4. *If $A, B \subset M^n$ are in $\mathcal{D}$, then so are $A \cup B$ and $M^n \setminus A$.*
5. *If $A \subset M^{n+1}$ is in $\mathcal{D}$, then so is its projection*

$$\pi(A) = \{\overline{a} \in M^n : \exists a \in M((\overline{a}, a) \in A)\}.$$

Exercise 2.8.4. 1. Show that the pointclass $\mathcal{D}$ of definable sets is closed under finite intersections and under substitutions by definable functions, i.e., if $A \subset M^n$ is in $\mathcal{D}$ and $f_1, \cdots, f_n : M^m \to M$ are definable, then so is the set $B \subset M^m$ defined by

$$\overline{a} \in B \Leftrightarrow \overline{f}(\overline{a}) \in A.$$

In particular, if A is definable, then so is $M \times A$.

2. Show that if $A \subset M^{n+1}$ is definable, then so is its *coprojection* $B \subset M^n$ defined by

$$\overline{a} \in B \Leftrightarrow \forall a \in M((\overline{a}, a) \in A).$$

3. Show that $f = (f_1, \cdots, f_l) : M^k \to M^l$ is definable if and only if each $f_1, \cdots, f_l$ is definable.
4. Show that if $f : M^k \to M^l$ and $g : M^l \to M^m$ are definable, then so is their composition $g \circ f : M^k \to M^m$.
5. For $A \subset M$, define the *definable closure of* A, denoted by $dcl(A)$, by

$$dcl(A) = \{x \in M : x \;\; A - \text{definable}\}.$$

Show that $A \subset dcl(A)$, $A \subset B \Rightarrow dcl(A) \subset dcl(B)$, and $dcl(dcl(A)) = dcl(A)$.

Example 2.8.5. $<$ is $\emptyset$-definable in the ring of reals $\mathbb{R}$. This follows from

$$x < y \Leftrightarrow \exists z(z \neq 0 \wedge y = x + z^2).$$

Example 2.8.6. If L is the language of a ring without subtraction and R is a ring, then the subtraction $z = x - y$ is $\emptyset$-definable in the language L:

$$z = x - y \leftrightarrow x = y + z.$$

Example 2.8.7. Let $\mathbb{F}$ be a field and $R = \mathbb{F}[X_1, \cdots, X_n]$ the ring of polynomials over $\mathbb{F}$. We regard $\mathbb{F}$ as the set of all polynomials of degree 0. Then $\mathbb{F}$ is an $\emptyset$-definable subset of the ring R. It is defined by

$$x \in \mathbb{F} \Leftrightarrow x = 0 \vee \exists y(x \cdot y = 1).$$

Example 2.8.8. It was proved by Lagrange that every positive integer is a sum of squares of four integers. From this it follows that $<$ is $\emptyset$-definable in the ring $\mathbb{Z}$:

$$x < y \Leftrightarrow \exists z_1 \exists z_2 \exists z_3 \exists z_4 (z_1 \neq 0 \wedge y = x + z_1^2 + \cdots + z_4^2).$$

In particular, the set of all natural numbers is an $\emptyset$-definable subset of $\mathbb{Z}$.

It is known that if $\mathbb{K}$ is an algebraically closed field of characteristic 0, then the ring $R = \mathbb{K}[X_1, \cdots, X_n]$ of polynomials over $\mathbb{K}$ satisfies Fermat's last theorem, i.e., if $n > 2$, then the equation $x^n + y^n = z^n$ has no nontrivial solution in R, i.e., if (x, y, z) is a solution, then $x, y, z \in \mathbb{K}$. (See [10], p. 194.) This implies the following:

Example 2.8.9. If $\mathbb{K}$ is an algebraically closed field of characteristic zero, then $\mathbb{K}$ is an $\emptyset$-definable subset of the field of rational functions $\mathbb{K}(X_1, \cdots, X_n)$. For instance, it is defined by the formula

$$f \in \mathbb{K} \Leftrightarrow \exists g \exists h(f = h^3 = 1 + g^3).$$

Example 2.8.10. Let $\mathbb{K}$ be a field. A subset X of $\mathbb{K}^n$ is defined by an atomic formula if and only if it is the set of all zeros (roots) of a polynomial over $\mathbb{K}$.

We need a well-known result of Hilbert now. (See [10].) Let $\mathbb{K}$ be a field, and let $P \subset \mathbb{K}[X_1, \cdots, X_n]$. Define

$$\mathcal{V}(P) = \{\overline{a} \in \mathbb{K}^n : f(\overline{a}) = 0 \text{ for all } f \in P\}.$$

Sets of the form $\mathcal{V}(P)$ are called *Zariski closed sets* or *affine algebraic varieties* in $\mathbb{K}^n$. Note that if $P \subset Q \subset \mathbb{K}[X_1, \cdots, X_n]$, then $\mathcal{V}(Q) \subset \mathcal{V}(P)$.

Theorem 2.8.11 (Weak Hilbert Basis Theorem). *If $\mathbb{K}$ is a field and $V \subset \mathbb{K}^n$ is Zariski closed, then there is a finite $P \subset \mathbb{K}[X_1, \cdots, X_n]$ such that $V = V(P)$.*

It follows that Zariski closed sets $V \subset \mathbb{K}^n$ are precisely the sets defined by finite conjunctions of atomic formulas, i.e., by finitely many polynomial equations.

Exercise 2.8.12. Readers familiar with topology should show that Zariski closed subsets of $\mathbb{K}^n$ are the family of all closed subsets of a topology on $\mathbb{K}^n$. This topology is called the *Zariski topology*.

Example 2.8.13. Let $\mathbb{K}$ be a field, and let $M_{m\times n}(\mathbb{K})$ denote the set of all $m \times n$ matrices over $\mathbb{K}$. We identify $M_{m\times n}(\mathbb{K})$ with $\mathbb{K}^{mn}$ in a canonical way. We shall follow the usual convention and write $M_n(\mathbb{K})$ in place of $M_{n\times n}(\mathbb{K})$. Show the following:

1. The determinant function $A \to |A|, A \in M_n(\mathbb{K})$ (i.e., its graph) is $\emptyset$-definable.
2. The set of all $n \times n$ nonsingular matrices $GL_n(\mathbb{K})$ is $\emptyset$-definable. In fact, it is defined by the negation of a polynomial equation.
3. Show that the matrix multiplication $M_{m\times n}(\mathbb{K}) \times M_{n\times k}(\mathbb{K}) \to M_{m\times k}(\mathbb{K})$ is $\emptyset$-definable.

A family $\mathcal{A}$ of subsets of a set X is called an *algebra of sets on X* if it contains X and is closed under complementations and finite unions. Sets belonging to the algebra of subsets of $\mathbb{K}^n$ generated by affine algebraic varieties $V \subset \mathbb{K}^n$ are called *constructible sets*.

Exercise 2.8.14. A subset $C \subset \mathbb{K}^n$ is constructible if and only if it is defined by an open formula.

Example 2.8.15. Let $D \subset \mathbb{R}^n$ be definable. Then its *closure*

$$\overline{D} = \{\overline{a} \in \mathbb{R}^n : \forall \varepsilon(\varepsilon > 0 \to \exists \overline{b} \in D(\sum_{i=1}^{n}(a_i - b_i)^2 < \varepsilon))\}$$

is definable.

If $\varphi[\overline{y}, i_{\overline{c}}]$, $\overline{c} \in \mathbb{R}$, defines D, then the formula

$$\forall x(x > 0 \to \exists \overline{y}(\varphi[\overline{y}, i_{\overline{c}}] \wedge \sum(x_i^2 - y_i^2) < x))$$

defines the closure of D.

Proposition 2.8.16. *Let $D \subset M^n$ be A-definable and $f : M \to M$ an automorphism of M such that $f(a) = a$ for all $a \in A$. Then $D = f(D)$. In particular, f fixes all A-definable points.*

Proof. Let $\varphi[\overline{x}, i_{\overline{a}}]$, with a_i in A, define D. For every any $\overline{b} \in M^n$, we have

$$\begin{aligned}\overline{b} \in D &\Leftrightarrow M \models \varphi[i_{\overline{b}}, i_{\overline{a}}] \\ &\Leftrightarrow M \models \varphi[i_{f(\overline{b})}, i_{f(\overline{a})}] \\ &\Leftrightarrow M \models \varphi[i_{f(\overline{b})}, i_{\overline{a}}] \\ &\Leftrightarrow f(\overline{b}) \in D.\end{aligned}$$

The second equivalence holds because f is an automorphism of M. The first and last equivalences hold because $\varphi[\overline{x}, i_{\overline{a}}]$ defines D. Our proof is complete. □

It is well known that for every finite sequence $\overline{a}$ of complex numbers there is a real number r and a complex number s (not in $\mathbb{R}$) such that there is a field isomorphism $f : \mathbb{C} \to \mathbb{C}$ fixing each $\overline{a}$ and mapping r to s. Thus we get the following interesting result.

Proposition 2.8.17. *The set of all real numbers $\mathbb{R}$ is not a definable subset of the field of complex numbers $\mathbb{C}$.*

Later we shall prove that the set of all rational numbers $\mathbb{Q}$ is not a definable subset of the field of real numbers. In a remarkable result (see [4] for an excellent account of this) using deep results on diophantine equations, Julia Robinson proved the following theorem.

Theorem 2.8.18 (J. Robinson). *The set of all integers is an $\emptyset$-definable subset of the ring of rational numbers $\mathbb{Q}$.*

The importance of these results for decision problems will be explained now.

Let M be a structure of L and $N \subset M$ a substructure. Suppose $\varphi[x, i_{\overline{a}}]$ defines N. For any formula ψ we define its *relativization to N*, denoted by ψ^N, by induction on the rank of ψ as follows: if ψ is atomic, then ψ^N is ψ. Further,

$$(\neg\psi)^N = \neg\psi^N, (\psi \vee \eta)^N = \psi^N \vee \eta^N$$

and

$$(\exists y \psi)^N = \exists y(\varphi[y, i_{\overline{a}}] \wedge \psi^N).$$

We may think of ψ^N as the relativization of ψ to N.

Proposition 2.8.19. *Let N be a definable substructure of M. Then for every formula $\psi[x_0, \cdots, x_{n-1}]$ and every $\overline{b} \in N^n$,*

$$N \models \psi[i_{\overline{b}}] \Leftrightarrow M \models \psi^N[i_{\overline{b}}].$$

Proof. We prove the result by induction on ψ. The result is clearly true for atomic ψ and is true for $\neg\psi$ ($\psi \vee \eta$) if it is true for ψ (resp. for ψ and η).

Now suppose the result is true for $\psi[x, x_0, \cdots, x_{n-1}]$ and every $\overline{c} \in N^{n+1}$ and $\eta[x_0, \cdots, x_{n-1}] = \exists x\psi$. Take any $\overline{b} \in N^n$.

Suppose $M \models \eta^N[i_{\overline{b}}]$. Then there is a $b \in M$ such that $M \models \varphi[i_b, i_{\overline{a}}]$ as well as $M \models \psi^N[i_b, i_{\overline{b}}]$. Since φ defines N, $b \in N$. By the induction hypothesis, $N \models \psi[i_b, i_{\overline{b}}]$. Thus, $N \models \eta[i_{\overline{b}}]$.

Now assume that $\overline{b} \in N^n$ and $N \models \eta[i_{\overline{b}}]$. Thus, there is a $b \in N$ such that $N \models \psi[i_b, i_{\overline{b}}]$. By the induction hypothesis, $M \models \psi^N[i_b, i_{\overline{b}}]$. Since φ defines N, $M \models \varphi[i_b, i_{\overline{a}}]$. This proves that $M \models \psi^N[i_{\overline{b}}]$. □

Remark 2.8.20. Suppose M is such that there is an algorithm to decide if a statement of L_M is true in M or not. Such a structure is called decidable. Otherwise it is called undecidable. (The concept of an algorithm will be defined later in the book.) The last result tells us that if $N \subset M$ is definable and M decidable, then N is decidable. Equivalently, if N is undecidable, so is M. It was proved by Tarski that $\mathbb{R}$ as an ordered field and $\mathbb{C}$ are decidable. It was proved by Gödel that $\mathbb{N}$ is undecidable in the language of the ordered ring. Julia Robinson's result implies that the ordered field of rationals is undecidable. These things will be dealt with in more detail later.

Suppose M is a structure of L and $f_M : M^n \to M$ definable, defined by, say, $\varphi[y, \overline{x}, i_{\overline{a}}]$. Let L' be the expansion of L obtained by introducing an n-ary function symbol f. We regard M as a structure of L' by interpreting f by f_M. For any formula ψ of L', let ψ^f be the formula of L obtained from ψ by replacing each subformula of ψ of the form $\eta[\cdots f\overline{t}\cdots]$ by the formula $\exists u(u = f\overline{t} \wedge \eta[\cdots u \cdots])$, where u is a variable not occurring in ψ, and then by replacing each subformula of the form $t = f(\overline{s})$ by $\varphi[t, \overline{s}, i_{\overline{a}}]$. If necessary, new variables should be used so that the essential nature of the formula φ is not changed. Then

Proposition 2.8.21.

$$M \models \psi \Leftrightarrow M \models \psi^f.$$

Its entirely trivial proof is left as an exercise. This result implies that if a set is definable by a formula of L', it is definable by a formula of L. A similar result is true for definable relations on M.

Let L and L' be first-order languages, M an L-structure, and N an L'-structure. We say that N is *interpretable in M* if there are a structure $N' \subset M^k$ (for some k) of L' with N' and interpretations of all nonlogical symbols of L in N' definable by formulas of L so that N and N' are isomorphic.

Example 2.8.22. If $\mathbb{K}$ is a field, then the group $GL_n(\mathbb{K})$ is interpretable in the field $\mathbb{K}$.

Let $GL_n^+(\mathbb{R})$ denote the set of all $n \times n$-real matrices with determinant positive, $O(n)$ the set of all orthonormal $n \times n$-real matrices, and $SO(n)$ the subgroup of $O(n)$ of matrices of determinant 1. Similarly, let $U(n)$ denote the set of all unitary matrices over $\mathbb{C}$ and $SU(n)$ the subgroup of $U(n)$ of determinant 1.

Let $\mathbb{K}$ be a field. A *linear algebraic group over* $\mathbb{K}$ is a subgroup G of $GL_n(\mathbb{K})$ such that G and the graph of the matrix multiplication on G are affine algebraic varieties. In general, an *algebraic group over* $\mathbb{K}$ is a group G that is an affine algebraic variety over $\mathbb{K}$, and the group operation $\cdot : G \times G \to G$ (more precisely, its graph) is an affine algebraic variety, i.e., definable by polynomial equations.

Example 2.8.23. The groups $GL_n^+(\mathbb{R})$, $O(n)$, and $SO(n)$ are interpretable in the field of reals. Moreover, $O(n)$ and $SO(n)$ are linear algebraic groups over $\mathbb{R}$. The groups $U(n)$ and $SU(n)$ are algebraic over $\mathbb{C}$ and interpretable in the field of complex numbers $\mathbb{C}$.

Springer

http://www.springer.com/978-1-4614-5746-6

A Course on Mathematical Logic
Srivastava, S.M.
2013, XII, 198 p.,
ISBN: 978-1-4614-5746-6