Sets, Logic and Categories
Solutions to Exercises: Chapter 4

4.1 Let G denote the set of group axioms given at the end of Section 4.1. Show that $\mathrm{G} \vdash \sigma$, where σ is the sentence

$$((\forall x)(\mu(x,x) = \varepsilon) \to (\forall x)(\forall y)(\mu(x,y) = \mu(y,x)).$$

Hint: It is probably easier to prove this in the 'language of mathematics' first and translate the proof into the first-order language. The point is that mathematical proofs can be written in this language, even though they are somewhat clumsy; and, in this form, checking their correctness is a purely mechanical procedure.

The mathematical proof works as follows: suppose that $x^2 = 1$ for all $x \in G$ (this is shorthand for $\mu(x,x) = \varepsilon$). Then, for all x and y, we have $xyxy = 1$. Multiplying on the left by x and on the right by y, using the associative law and the facts that $xx = yy = 1$, we obtain $yx = xy$. Your job is to translate this proof into first-order language.

David Turtle, a student who took the course in 1998–9, constructed a solution to this problem. His proof contained over seven hundred lines. I do not propose to reproduce it here.

4.2 For each of the cases (a) fields, (b) totally ordered sets, (c) graphs, give a first-order language and a set of sentences which axiomatizes the relevant class of structures.
Can this be done for (d) topological spaces, (e) well-ordered sets?

(a) There are several ways to proceed. Perhaps the simplest is to use two binary function symbols (addition and multiplication) and two constant symbols (zero and one). The axioms can be copied more-or-less straightforwardly from any algebra text. For example, the additive and multiplicative inverse axioms are

- $(\forall x)(\exists y)(x+y=0)$,
- $(\forall x)(\neg(x=0)) \to ((\exists y)(x \cdot y = 1))$.

We must also include the axiom $(\neg(0=1))$, since a one-element structure satisfies all the other axioms but is not a field.

Alternative approaches are not so straightforward.

It is possible to do without the constant symbols, since they can be 'defined' by existential axioms:

- $(\exists e)(\forall x)(e+x=x)$,
- $(\exists f)(\forall x)(f \cdot x = x)$.

But then it is more cumbersome to refer to these elements in the inverse axioms and the axiom $(\neg(0=1))$. For example, the last could be written

$$((\forall x)((x+e=x) \wedge (x \cdot f = x)) \to (\neg(e=f)))$$

(quantified over e and f if we want our axioms to be sentences)

It is also possible to include unary functions for additive and multiplicative inverses. The statements of the axioms are easy to write. The only problem is the aesthetic one: the multiplicative inverse of zero is completely arbitrary, so either we leave it unspecified (and so have many non-isomorphic fields where there should only be one), or we define it arbitrarily (say, by $i(0) = 0$) in a way that has nothing to do with the algebra). This type of problem is addressed by 'many-sorted logic'.

Note finally that the choice of axioms has some implications for 'elementary' field theory. In the first approach, the uniqueness of zero and one is built into the axioms, whereas in the second approach, we have to prove that they are unique and use this uniqueness to justify introducing the notation 0 and 1. Arguably, the second appoach teaches us more. Similar remarks apply to the uniqueness of additive and multiplicative inverses.

(b) As explained in Chapter 1, this can be done in two ways, giving rise to strict and non-strict orders respectively. The axioms are given informally there. For non-strict orders, there is one binary relation R, and the axioms are

- $(\forall x)R(x,x)$;
- $(\forall x)(\forall y)(((R(x,y) \wedge R(y,x)) \rightarrow (x = y))$;
- $(\forall x)(\forall y)(\forall z)(((R(x,y) \wedge R(y,z)) \rightarrow (R(x,z))$;
- $(\forall x)(\forall y)((R(x,y) \vee R(y,x))$.

(c) For a simple graph, take a single binary relation (adjacency) satisfying the two axioms of irreflexivity and symmeetry:

- $(\forall x)(\neg R(x,x))$;
- $(\forall x)(\forall y)((R(x,y) \rightarrow R(y,x))$.

If we want more general graphs possibly containing loops (edges which join a vertex to itself), simply delete the first axiom. Graphs with multiple edges are more difficult. If we never consider graphs with more than α edges between two vertices, we take one binary relation R_β for each cardinal number β not exceeding α, and require that each pair of vertices satisfies exactly one of these relations (and that all are symetric). Note that R_0 is 'non-adjacency'.

But to be completely general, a different approach is needed. The we must take vertices and edges as elements of the structure (distinguishing them by a unary relation V which picks out the vertices). Now in place of adjacency, we can take an 'incidence' relation I between vertices and edges, satisfying

- $(I(x,y) \rightarrow (V(x) \wedge (\neg V(y))))$,
- $((I(x,w) \wedge I(y,w) \wedge I(z,w)) \rightarrow ((\neg(x = y)) \vee (\neg(x = z)) \vee (\neg(y = z))))$.

(I have omitted unniversal quantifiers for clarity.) The second axiom says that an edge is incident with at most two vertices; we could if desired exclude loops by requiring that an edge is incident with at least two vertices.)

(d) A toplogical space requires the specification of a family of open sets, with no restriction on their cardinalities. This cannot be done by the first-order apparatus.

However, before we conclude that the answer is ‘no’, we should consider that finite topological spaces can be determined by first-order axioms. On a finite topological space, let R be the binary relation such that $R(x,y)$ holds if every open set which contains x also contains y. Then

(a) R is reflexive and transitive;

(b) R determines the topology: a set U is open if and only if $x \in U$ and $R(x,y)$ imply $y \in U$;

(c) every reflexive and transitive relation gives rise to a topology by the prescription of (b).

So more is required to answer the question. This can be done by showing that the number of topologies on a set of infinite cardinality α is $2^{2^{\alpha}}$, whereas the number of first-order structures over a fixed language L is only 2^{α} if $\alpha > |L|$.

(e) The definition of well-ordered set seems to require quantification over subsets (‘every non-empty subset contains a least element’). As in (d), more is required to show that there is no clever way around the problem.

A proof can be based on the Compactnss Theorem, discussed in the next chapter. It states that, if Σ is a set of first-order sentences, then Σ is satisfiable (in some first-order structure) if and only if every finite subset of Σ is satisfiable.

Now we argue by contradiction. Let Σ_0 be a set of first-order axioms for well-ordered sets. Extend the language by adding a countable set $c_0, c_1, c_2, \ldots$ of new constant symbols, and let Σ_1 consist of the formulae $c_i < c_j$ for each pair i, j of natural numbers with $j < i$ (note the reversal!), and $\Sigma = \Sigma_0 \cup \Sigma_1$.

We claim that every finite subset of Σ is satisfiable. Take a countable well-ordered set (say, ω). All the sentences in Σ_0 are satisfied, by assumption. Given a finite subset of Σ_1, there are only finitely many of the c_i which are referred to in these sentences; if c_n is the one with largest index, then we may interpret c_i as $n-i$ for $i \leq n$, and all the sentences are valid. The interpretation of the remaining constants is arbitrary.

By the Compactness Theorem, Σ is satisfiable. But a model for Σ would be a well-ordered set contining an infinite descending sequence, a contradiction.

4.3 Can you suggest any reasons why algebra textbooks insist on the closure law as one of the axioms for a group, instead of allowing it to be implicit in the statement that the group operation is a binary function?

Two possible reasons:

(a) It has always been done this way. Authors copy one another so as not to confuse students with different definitions.

(b) In elementary group theory, one of the most important concepts is that of a subgroup, a subset which forms a group in its own right (with the same composition law). If the closure law is not explicitly included, it is easy to forget that it has to be checked!

My own experience of teaching group theory suggests that (b) is the more powerful argument.

There is more to be said. Before the modern definition of a group was invented (in about 1850), a group was a set G of transformations of a set X (that is, bijective functions from X to X) satisfying closure under composition and inversion and containing the identity transformation. Closure cannot be omitted in this definition!