Lecture 2: Examples of First-order Theories

Michael Beeson

Logic is the theory of theories

- Therefore one should first have some familiarity with some particular theories.
- Just as you would not start studying zoology without being familiar with a few examples of animals.

Abstract Algebra

Sometime in the nineteenth century, names were given to the following laws of arithmetic and algebra:

- Associative law of multiplication: $(ab)c = a(bc)$.
- Associative law of addition: $(a + b) + c = a + (b + c)$.
- Commutative law of multiplication: $ab = ba$.
- Commutative law of addition: $a + b = b + a$.
- Additive identity: $x + 0 = 0 + x = x$.
- Additive inverses: $x + (-x) = 0$.
- Multiplicative identity: $x \cdot 1 = 1 \cdot x = 1$.
- Multiplicative inverses: $x(x^{-1}) = x^{-1}x = 1$, if $x \neq 0$.
- Left distributive law: $a(b + c) = ab + ac$.
- Right distributive law: $(a + b)c = ac + bc$.

Many systems satisfy some of these laws

- Rational numbers $\mathbb{Q}$
- Real numbers $\mathbb{R}$
- Integers $\mathbb{Z}$ satisfy some but not all of those laws
- Complex numbers $\mathbb{C}$
- Numbers of the form $a + b\sqrt{3}$ for a and b in $\mathbb{Q}$.
- Integers mod p, $\mathbb{Z}_p$, for p a prime.

In class I will go over the proofs of some of the laws for some of these examples.

Permutations

Not every interesting example has both addition and multiplication; and in some cases, an operation that is not really addition or multiplication still satisfies some of those laws: The permutations on a set of n “letters” is called S_n. The operation is composition (performing one permutation after another). Thus $\sigma\tau$ is the result of first doing σ, then doing τ. In class, notation for permutations will be illustrated. The permutations satisfy

- associativity
- identity
- inverses exist

But they do not satisfy commutativity.

Other examples

- The rotations of the plane, under the operation of composition, satisfy the same three laws as the permutations do. They also satisfy commutativity.
- The distance-preserving maps of the plane $\mathbb{R}^2$ to itself, under the operation of composition, also satisfy those three laws. Do they satisfy commutativity?
- The rotations of 3-space $\mathbb{R}^3$ satisfy those three laws. Do they satisfy commutativity?

Group theory

Definition: A **group** is a set X, together with a binary operation on X that is associative, has an identity, which we call e, and has inverses. We write $x \cdot y$ for the operation, without assuming that it means multiplication. That is, it satisfies these three laws:

$$\begin{aligned} x \cdot (y \cdot z) &= (x \cdot y) \cdot z \\ x \cdot e &= x \wedge e \cdot x = x \\ \forall x \exists y \, (x \cdot y &= e \wedge y \cdot x = e) \end{aligned}$$

With this terminology, we can say that the usual number systems

- Form a group under addition, with identity element 0
- The nonzero numbers form a group under multiplication, with identity element 1

That captures all the laws we mentioned above, except in addition the distributive law links addition and multiplication.

Notation for groups

- A mathematician will say a group is “written additively” if the symbol $+$ is used for the operation, and “written multiplicatively” if the symbol $\cdot$, or no symbol at all, is used for the operation.
- Notation for inverses varies accordingly. The use of x^{-1} does not imply there is a more general exponentiation operation.
- The syntax of first-order logic may officially require prefix notation. Then, with f for the operation, the associativity law looks like this:

  $$f(f(a,b),c) = f(a,f(b,c)).$$

  This is almost never written. People use the more familiar “infix” notation.
- Occasionally one sees Polish notation: $++abc = +a+bc$ or “reverse Polish notation”: $ab+c+ = abc++$, both of which have the advantage of not needing parenthesis.
- We say “X forms a group under $+$” instead of the more precise “$(X,+)$ is a group.”

Groups in FOL

- Using a unary function symbol for “inverse”, and a constant for identity, the axioms will be quantifier-free. In particular $x \cdot i(x) = e$ instead of $\forall x \exists y \, (x \cdot y = e)$.
- Often we refer to “the group G” instead of “the group $(G, \cdot)$” or “the group $(G, +)$”, if the operation is clear from the context.
- We almost never mention the identity symbol or a symbol for inverse explicitly but technically a group is a structure $(G, \cdot, e, i)$ (assuming we have chosen that language for our axioms).

Some illustrative examples

The general notion of **submodel** that you learned in your logic course specializes to the older notion of **subgroup**.

- In class we will examine examples of subgroups.
- Starting with the two elements 0, 1, what subgroup of $(\mathbb{R}, +)$ is generated by the Löwenheim-Skolem process? (Technicall, what subgroup of $(\mathbb{R}, +, 0, -)$?)
- Starting with the two elements 1, 2, what subgroup of $(\mathbb{R} - \{0\}, \cdot)$ is generated by the Löwenheim-Skolem process? (Again, technically, what subgroup of

$$(\mathbb{R}, \cdot, 1, i)$$

  ? where i is for multiplicative inverse.)
- (Using the notation x^{-1}, it is hard to name the function symbol itself!)

Further illustrative examples

- An element in a group is of order n (for a fixed integer n) if $x^n = e$, and n is the least such integer.
- The group itself is of order n if it has n elements.

The following examples are intended to refresh your memory about the compactness and completeness theorems you learned in your first logic course. These will be explained in class.

- Give a theory whose models are exactly the groups of order three.
- Show that if a sentence ϕ in group theory is true in groups of arbitrarily large order, then it is true in some infinite group.
- Is it possible to give a sentence ϕ in group theory that is true only in infinite groups?

Field theory

A *field* is a set X with two binary operations $+$ and $\cdot$, such that

- X is a group under $+$, with identity element 0, and
- $X - \{0\}$ is a group under $\cdot$, and
- The distributive laws hold: $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.
- Both commutative laws hold: $a + b = b + a$ and $ab = ba$.

Now the notion of "submodel" specializes to "subfield", a notion that is very important in number theory.

Ring theory

A *ring* is like a field, but two axioms about multiplication are dropped:

- multiplicative inverses are not required (but their existence is not denied either).
- multiplication does not have to be commutative (but it might be).

Thus $\mathbb{Z}$ is a ring, but not a field.
Technically, $(\mathbb{Z}, +, \cdot, 0, 1)$ is a ring but not a field.
The $n \times n$ matrices (for a fixed n such as 2 or 3) with coefficients in a given field (such as $\mathbb{R}$) form a non-commutative ring. (If you do not know how to multiply matrices, that's not important in this logic course; it's just an example.)

Vector Spaces

A **vector space** is an (additively-written) group (the "vectors"), together with a field (the "scalars") and an operation of "scalar multiplication" that takes a vector and a scalar and produces a vector.

- The operation of scalar multiplication satisfies these laws:

$$\begin{aligned} a(u+v) &= au+av \\ (a+b)u &= au+bu \end{aligned}$$

- for example, the vectors could be elements of $\mathbb{R}^3$ and the scalars just real numbers.
- But also, the vectors could be functions from $\mathbb{R}$ to $\mathbb{R}$, or other more complicated things.
- How do we formalize this in FOL? Answer, we use two "sorts" or two unary predicates. This will be elaborated in class.

Abstract Algebra

That is the study of groups, rings, fields, and vector spaces.

- Usually in the training of mathematicians, the year after calculus is devoted to the study of these structures. They have many interesting and useful properties and are fundamental to the rest of mathematics.
- Formulating the notions of group, field, and vector space was a big advance in mathematics, because:
- it allowed proving things **once** in the most general context, instead of multiple times; and
- it allowed people to recognize familiar axioms in new situations. As soon as you can recognize that some operation and set form a group, then immediately you know a lot about the situation.
- It's the very **essence** of the usefulness of these notions that *these axioms have many models*. That's the driving idea of these axiomatizations.