20 Expressing Mathematical Concepts (II)

20.1 Ordering Relations

An ordering relation is a binary predicate `LE(_,_)` that is very similar to an equivalence relation except for one axiom.

`le-ref`:	$(\forall x)\ LE(x,x)$
`antisym`:	$(\forall x,y)\ ((LE(x,y)\ \land\ LE(y,x)) \supset E(x,y))$
`le-trans`:	$(\forall x,y,z)\ ((LE(x,y)\ \land\ LE(y,z)) \supset LE(x,z))$

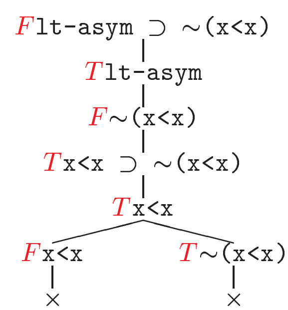
Both ordering relations and equalities are conventionally written in infix notation with predefined predicate symbols. We will adopt this convention from now on and write $x \leq y$ instead of `LE(x,y)` and $x=y$ instead of `E(x,y)`. One has to keep in mind, that these are only notational abbreviations for the "real" formulas, since otherwise we would have to redefine the language of first-order logic. With these notational changes the three axioms receive a more familiar form.

`le-ref`:	$(\forall x)\ x \leq x$
`antisym`:	$(\forall x,y)\ ((x \leq y\ \land\ y \leq x) \supset x=y)$
`le-trans`:	$(\forall x,y,z)\ ((x \leq y\ \land\ y \leq z) \supset x \leq z)$

Note that ordering relations require the existence of an equivalence predicate. It is, however, possible to axiomatize *strict orders* without referring to an equality. A strict order is a binary (infix) predicate $<$ that satisfies the following axioms

`lt-asym`:	$(\forall x,y)\ ((x<y \supset \sim(y<x))$
`lt-trans`:	$(\forall x,y,z)\ ((x<y\ \land\ y<z) \supset x<z)$

These two axioms also imply the irreflexivity of strict orders, as the formula $(\forall x)\ \sim(x<x)$ can be derived by instantiating the axiom of antisymmetry, as the tableau proof to the right shows.



Typical models for a strict order are the conventional less-than relations on natural numers, integers, rationals, or reals. One could, however, also define a strict order on booleans, with false being less than true. Orders also don't have to be linear. The (partial) order of nodes in a tree, for instance, satisfies the axioms for orders as well.

Strict orders can be derived from standard orders and vice versa if one has equality. One could define $x \leq y \equiv x<y \lor x=y$ or $x<y \equiv x \leq y \land \sim(x=y)$, depending on which predicate is axiomatized. It is easy to derive the corresponding axioms from the respective other ones and the equality axioms.

20.2 Algebraic Structures

Algebraic structures such as groups, rings, and fields, are the foundation for proving the structural properties of many well known operations on integers, rationals, reals, finite domains such as $\mathbb{Z}_p$ (where p may be a prime for encryption), etc. We will introduce the axioms of these structures step by step and look at possible models

20.2.1 Semigroups

Mathematically, a *semigroup* is a set S together with an associative binary operation $\circ$. To formalize semigroups in we need to take the language of first order logic and designate the predicate $=$ and the function symbol $\circ$ (to be precise, the predicate $\mathtt{R}_\circ$) as special. We also need the axioms of equality, the functionality axiom, and associativity of $\circ$. As shorthand notation we sometimes write

`Semigroup` $\equiv$ $\mathcal{L}$`(=,`$\circ$`; ref, sym, trans, subst, functionality, assoc)`

where it is automatically understaood that the last two axioms are formulated in terms of the operator $\circ$.

Almost all well-known structures are (models of) semigroups. Common examples are

– $\langle \mathbb{N}, =, + \rangle$, $\langle \mathbb{N}, =, * \rangle$,
– $\langle \mathbb{Z}, =, + \rangle$, $\langle \mathbb{Z}, =, * \rangle$, $\langle \mathbb{Z}, =_2, + \rangle$, (where $\mathsf{x} =_2 \mathsf{y} \equiv \mathsf{x} = \mathsf{y} \bmod 2$)
– $\langle \mathbb{Q}, =, + \rangle$, $\langle \mathbb{R}, =, + \rangle$,
– $\langle \Sigma^*, =, \circ \rangle$, (where $\circ$ is the string append operation).

Obviously it is easy to define domains and operations that are not semigroups. As an example take the domain $\mathsf{D} = \mathbb{Z}$ with subtraction as interpretation of $\circ$. Clearly (10 - 5) -3 is not the same as 10 - (5 -3).

Most of the above models also satisfy the commutativity axiom. However, it is not possible to prove `Semigroup` $\supset$ `comm`, as there are semigroups like $\langle \Sigma^*$`, =, `$\circ\rangle$ that are not commutative. Using the tableau method we can also construct a finite (2-element) counterexample for this statement. I'll leave that as an exercise for those who are interested.

20.2.2 Monoids

Monoids are semigroups that have an *identity* (or neutral) element. Given the experience we have gathered so far, their formalization is straightforward.

`Monoid` $\equiv$ $\mathcal{L}$`(=,`$\circ$`,id; ref, sym, trans, subst, functionality, assoc, ident)`

where the axiom of identity is

`ident:` $(\forall$`x)( x`$\circ$`id = x` $\wedge$ `id`$\circ$`x = x)`

Of course, we could also avoid designating and axiomatizing the parameter `id` and formulate an axiom about the existence of a unique neutral element.

`ident-exists:` $(\exists !$`id)`$(\forall$`x)( x`$\circ$`id = x` $\wedge$ `id`$\circ$`x = x)`

The advantage of doing so is that the models of monoids are also models of semigroups, that is we don't have to extend them by a constant. The disadvantage is that we can't refer to that element in separate axioms when we extend monoids to groups.

All of the above semigoups are also monoids. For $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ the identity of `+` is `0` and the identity of `*` is `1`. For strings, the identity is the empty string. If we require strings to be non-empty, then we lose the monoid property, that is $\langle \Sigma^+, =, \circ \rangle$ is a semigroup but not a monoid. Again, it is easy to construct a finite semigroup that is not a monoid.

20.2.3 Groups

Groups are monoids with inverse elements for $\circ$. We formalize this as

Group $\equiv$ $\mathcal{L}$(=,$\circ$,id; ref, sym, trans, subst, functionality, assoc, ident, inv)

where the axiom about the existence of inverse elements is

inv: $(\forall x)(\exists \bar{x})(\ x \circ \bar{x} = id \ \wedge\ \bar{x} \circ x = id)$

In this case, we cannot replace the axiom about the existence of inverse elements by one about a designated parameter, as the chice of the inverse element depends on the element to which the operation $\circ$ shall be applied.

Many of the above monoids are also groups, but some operations do not allow for inverses.
– $\langle \mathbb{Z}, =, + \rangle$, $\langle \mathbb{Z}, =_2, + \rangle$, $\langle \mathbb{Q}, =, + \rangle$, and $\langle \mathbb{R}, =, + \rangle$, are groups but
– $\langle \mathbb{N}, =, + \rangle$, $\langle \mathbb{N}, =, * \rangle$, $\langle \mathbb{Z}, =, * \rangle$, and $\langle \Sigma^*, =, \circ \rangle$ are not.

It is interesting to notice that $\langle \mathbb{Z}, =_2, - \rangle$ is a group although $\langle \mathbb{Z}, =, - \rangle$ is not. The simple reason for that is that in this specal case addition and subtraction are identical. $\langle \mathbb{Z}, =_3, * \rangle$ has an inverse element for every element but 0.

20.2.4 Rings

Domains like $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are characterized by the fact that there are more than just (commutative) groups. Besides addition they have a second operation, multiplication that interacts with addition in a specific way. The simplest algebraic construct that has this property is a *ring*. A ring is a set S together with two operations $+$ and $*$ such that $\langle S,=,+ \rangle$ is a commutative group and $\langle S,=,* \rangle$ is a semigroup.

Ring $\equiv$ $\mathcal{L}$(=,+,*,id; ref, sym, trans, subst,
functionality$_+$, assoc$_+$, ident$_+$, inv$_+$, comm$_+$,
functionality$_*$, assoc$_*$
distrib)

where the distributivity axiom is the following

distrib: $(\forall x,y,z)(\ x*(y+z) = x*y + x*z \ \wedge\ (x+y)*z = z*z\ y*z)$

A ring that also has an identity for multiplication is called a *ring with unity*.

U-Ring $\equiv$ $\mathcal{L}$(=,+,*,id,e; ref, sym, trans, subst,
functionality$_+$, assoc$_+$, ident$_+$, inv$_+$, comm$_+$,
functionality$_*$, assoc$_*$, ident$_*$
distrib)

where `e` denotes the identity of $*$. Since the multiplication operations for $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ always led to monoids, these three domains and the factorization groups of $\mathbb{Z}$, that is $\langle \mathbb{Z}, =, +, * \rangle$, $\langle \mathbb{Z}, =_2, +, * \rangle$, $\langle \mathbb{Q}, =, +, * \rangle$, and $\langle \mathbb{R}, =, +, * \rangle$, are also rings with unity. Another interesting ring with unity is the ring of booleans $\langle \mathbb{B}, =, \Leftrightarrow, \vee \rangle$ with respective identities T and F, since can derive the laws of propositional logic solely from the ring axioms for the operations $\Leftrightarrow$ and $\vee$. Note that in all these cases the "multiplication" is also commutative.

20.2.5 Integral Domains

All the concepts so far were not sufficient to distinguish between $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and the factorization groups of $\mathbb{Z}$. However, the integers satisfy another interesting property that is not shared by all the factorization groups. We know that 0, the identity of addition has no proper divisors: if i*j=0 then either i or j must be 0. Commutative rings that have this property are called *integral domains*.

```
Integral Domain ≡ ℒ(=,+,*,id,e; ref, sym, trans, subst,
                                 functionality₊, assoc₊, ident₊, inv₊, comm₊,
                                 functionality*, assoc*, ident*, comm*,
                                 distrib, Z)
```

where Z is the axiom of "no zero divisors":

```
Z:  (∀x,y)( x*y = id  ⊃  (x=id ∨ y=id))
```

$\langle\mathbb{Z}, =, +, *\rangle$, $\langle\mathbb{Q}, =, +, *\rangle$, and $\langle\mathbb{R}, =, +, *\rangle$ are integral domains but $\langle\mathbb{Z}, =_4, +, *\rangle$, is not, although $\langle\mathbb{Z}, =_2, +, *\rangle$ and $\langle\mathbb{Z}, =_3, +, *\rangle$ are. The distinguishing factor between $\mathbb{Z}$ and its factorization domains is the existence of a strict linear order on $\mathbb{Z}$ and the induction principle. We will discuss this in the next lecture.

20.2.6 Fields

What distinguishes the rationals from the integers? They are "more complete" in the sense that they offer inverses for multiplication too – except, of course for 0. Integral domains that have this additional property are called *fields*.

```
Field ≡ ℒ(=,+,*,id,e; ref, sym, trans, subst,
                        functionality₊, assoc₊, ident₊, inv₊, comm₊,
                        functionality*, assoc*, ident*, inv'*, comm*,
                        distrib, Z)
```

Note that the axiom about the exstence of inverses for * needs to be slightly different.

```
inv'*:    (∀x)(∼(x=id) ⊃ (∃x̄)( x*x̄ = e ∧ x̄*x = e))
```

$\langle\mathbb{Q}, =, +, *\rangle$ and $\langle\mathbb{R}, =, +, *\rangle$ are fields but $\langle\mathbb{Z}, =, +, *\rangle$ is not. Interestingly, $\langle\mathbb{Z}, =_3, +, *\rangle$ is a field too, although $\langle\mathbb{Z}, =_2, +, *\rangle$ and $\langle\mathbb{Z}, =_4, +, *\rangle$ are not.

Rationals and reals also have a density property with respect to a strict linear order and reals satisfy the axiom of the existence of least upper bounds, limits of converging sequences, or other variations of the "completeness" axiom.