Formalizing Fundamental Concepts

- **Equality** is a binary predicate Eq(_,_) that comes with three axioms

  ref: $(\forall x)\ E(x,x)$
  sym: $(\forall x,y)\ (E(x,y) \supset E(y,x))$
  trans: $(\forall x,y,z)\ ((E(x,y) \wedge E(y,z)) \supset E(y,x))$

  In addition we need an axiom stating that we can replace equal for equal.

  subst: $(\forall x,y)\ (E(x,y) \supset P(..,x,..) \supset P(..,y,..))$

  This is an *axiom scheme* that needs to be instantiated for every predicate symbol that occurs in the set of formulas under consideration.

  An important derived concept is the unique-existence operator

  $(\exists ! x) P(x) \equiv (\exists x)(P(x) \wedge (\forall y)(P(y) \supset E(x,y)))$

- **n-ary Functions** can be described by (n+1)-ary predicates.

  A unary function f is described by a predicate R_f, where $R_f(x,y)$ is supposed to express that $f(x)$=y. We need two axioms.

  functionality: $(\forall x)(\exists ! y)\ R_f(x,y)$
  functional equality: $(\forall x,x',y,y')((E(x,x') \wedge R_f(x,y) \wedge R_f(x',y')) \supset E(y,y'))$

  These axioms have to be stated for every function symbol to be introduced. Functional equality can be derived from substitution. Most commonly we will deal with *binary operators*, usually written in infix format $x \circ y$. We may want additional properties such as commutativity or associativity.

  comm: $(\forall x,y,z)\ (R_\circ(x,y,z) \supset R_\circ(y,x,z))$
  assoc: $(\forall x,y,z,s,t,w)\ (R_\circ(x,y,s) \supset R_\circ(s,z,w) \supset R_\circ(y,z,t) \supset R_\circ(x,t,w))$

  As abbreviation we write $f(x)=y$ instead of $R_f(x,y)$ and use infix notation where possible.

- **Constants** are best described by their effect on operators. One could therefore characterize the integer 0, for instance, by the axiom

  zero: $(\forall x)(x+0 = x \wedge x*0 = 0)$

  Alternatively, one may state the existence of a unique element with the desired properties.

  zero-exists: $(\exists ! zero)(\forall x)(x+zero = x \wedge x*zero = zero)$

- **Ordering Relations** are binary predicates LE(_,_) with the following axioms

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

  From now on we write $x \leq y$ instead of $LE(x,y)$ and $x=y$ instead of $E(x,y)$.

  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: $(\forall x,y,z)\ ((x<y \wedge y<z) \supset x<z)$

Algebraic Structures

We denote a mathematical structure with operations *op* and axioms $axioms$ by $\mathcal{L}(ops, axioms)$.

A *semigroup* is a set S together with an associative binary operation $\circ$.

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

where the last two axioms are formulated in terms of the operator $\circ$.

Monoids are semigroups hat have an *identity* (or neutral) element.

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$)$

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$)$

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)

Commutatives rings where the identity of + has no proper divisors are *integral domains*.

Integral Domain $\equiv$ $\mathcal{L}$(=,+,*,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: $(\forall x,y)($ x*y = id $\supset$ (x=id $\vee$ y=id)$)$

Integral domains that offer inverses for multiplication too are called *fields*.

Field $\equiv$ $\mathcal{L}$(=,+,*,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'$_*$: $(\forall x)(\sim$(x=id) $\supset$ $(\exists \bar{x})($ x*$\bar{x}$ = e $\wedge$ $\bar{x}$*x = e$))$