21 Axiomatizing Integer Arithmetic

In the previous lecture we have presented the axioms of a variety of algebraic structures and looked at certain domains and operations that satisfy these axioms. Of particular interest for us is the domain of integers and its associated operations, since a complete axiomatization of that domain would allow us to reason about arithmetic in first-order logic and to get hold of the foundations of real analysis and a major chunk of mathematics.

Axiomatizing mathematics in a logical framework has been the dream of mathematicians for more than a hundred years, since this would provide a machinery for writing and checking mathematical proofs without having to rely on semantical arguments, which may or may not be flawed in some subtle way. Unfortunately, Gödel's incompleteness theorem, which we will discuss briefly at the end of this course, put an end to this dream – but not completely. There is still a significant part of mathematics that we can express in first-order logic and we can use formal proof systems to prove and verify a lot of interesting results. Today, we're going to look at Integer Arithmetic - let's see how far we get.

21.1 Ordered Integral Domain with Induction

From our investigation of algebraic structures we know that the integers as we know them are an integral domain, but not a field. An integral domain is a domain with two associative and commutative operations + and *, neutral elements for both of them, which we will call 0 and 1 from now on, inverse elements for +, such that the distributivity law and the law of no zero divisors holds.

Integral Domain $\equiv$ $\mathcal{L}$(=,+,*,0,1; ref, sym, trans, subst, distrib, Z
functionality$_+$, assoc$_+$, ident$_+$, inv$_+$, comm$_+$,
functionality$_*$, assoc$_*$, ident$_*$, comm$_*$)

where the axioms are as follows

ref:	$(\forall x)\ x=x$
sym:	$(\forall x,y)\ (x=y \supset y=x)$
trans:	$(\forall x,y,z)\ ((x=y \wedge y=z) \supset x=z)$
subst:	$(\forall x,y)\ (x=y \supset P(.,x,.) \supset P(.,y,.))$ *for every predicate symbol*
functionality$_+$:	$(\forall x,y)(\exists! z)\ x+y = z$
comm$_+$:	$(\forall x,y,z)\ (x+y = z \supset y+x = z))$
assoc$_+$:	$(\forall x,y,z,t)\ ((x+y)+z = t \supset x+(y+z) = t)$
ident$_+$:	$(\forall x)(\ x+0 = x \wedge 0+x = x)$
inv:	$(\forall x)(\exists \bar{x})(\ x+\bar{x} = 0 \wedge \bar{x}+x = 0)$
functionality$_*$:	$(\forall x,y)(\exists! z)\ x*y = z$
comm$_*$:	$(\forall x,y,z)\ (x*y = z \supset y*x = z))$
assoc$_*$:	$(\forall x,y,z,t)\ ((x*y)*z = t \supset x*(y*z) = t)$
ident$_*$:	$(\forall x)(\ x*1 = x \wedge 1*x = x)$
distrib:	$(\forall x,y,z)(\ x*(y+z) = x*y+x*z \wedge (x+y)*z = x*z+y*z)$
Z:	$(\forall x,y)(\ x*y = 0 \supset (x=0 \vee y=0))$

Recall that n-ary functions are represented by (n+1)-ary predicates and that the above presentation of the axioms is an abbreviation for the ones that are really used. The associativity law for +, for instance, really reads as

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

and there is an instance of the substitution axiom for each of the three arguments of R_+.

Integral domains, as we have seen, are not sufficient to characterize the integers. There are quite a few other models for integral domains that have nothing to do with the integers we know. What is missing is that the integers are arranged in an infinite strict linear order, that this order interacts with 0, 1, +, and * in certain ways, and that there is a method to count the integers. Let us begin with axiomatizing the order relation.

The less-than order on integers is a strict ordering relation < that is *linear*, *discrete*, and relates 0 and 1, and is monotone wrt. addition and (nonnegative) multiplication. This leads to the following axioms (which may be redundant).

lt-asym:	$(\forall x,y)\ (x<y \supset \sim(y<x))$
lt-trans:	$(\forall x,y,z)\ ((x<y \wedge y<z) \supset x<z)$
lt-linear:	$(\forall x,y)\ (x<y \vee y<x \vee x=y)$
lt-discrete:	$(\forall x,y)\ \sim(x<y \wedge y<x+1)$
lt-0-1:	$0<1$
lt-mono-+:	$(\forall x,y,z)(x<y \supset x+z < y+z)$
lt-mono-*:	$(\forall x,y,z)((0<z \wedge x<y) \supset x*z < y*z)$

The standard domain of integers $\langle \mathbb{Z}, =, <, +, * \rangle$ is certainly a model of these axioms, but the factorization domains are not, because they violate the monotonicity laws. They do, however, satisfy all the other axioms.

Here is an example of a proof based on the above axioms. We want to prove $x<y \supset \bar{y}<\bar{x}$

(1)	lt-mono-+	$x<y \supset x+\bar{y} < y+\bar{y}$
(2)	comm_+	$x+\bar{y}=\bar{y}+x$
(3)	$\mathrm{subst}_<$, (2)	$x+\bar{y} < y+\bar{y} \supset \bar{y}+x < y+\bar{y}$
(4)	inv	$y+\bar{y} = 0$
(5)	$\mathrm{subst}_<$, (4)	$\bar{y}+x < y+\bar{y} \supset \bar{y}+x < 0$
(6)	lt-mono-+	$\bar{y}+x < 0 \supset (\bar{y}+x)+\bar{x} < 0+\bar{x}$
(7)	assoc_+	$(\bar{y}+x)+\bar{x} = \bar{y}+(x+\bar{x})$
(8)	lt-mono-+	$(\bar{y}+x)+\bar{x} < 0+\bar{x} \supset \bar{y}+(x+\bar{x}) < 0+\bar{x}$
(9)	inv	$x+\bar{x} = 0$
(10)	$\mathrm{subst}_<$, (9)	$\bar{y}+(x+\bar{x}) = \bar{y}+0$
(11)	ident_+	$\bar{y}+0 = \bar{y}$
(12)	$\mathrm{subst}_<$, (11)	$\bar{y}+(x+\bar{x}) = \bar{y}$
(13)	$\mathrm{subst}_<$, (12)	$\bar{y}+(x+\bar{x}) < 0+\bar{x} \supset \bar{y} < 0+\bar{x}$
(14)	ident_+	$0+\bar{x} = \bar{x}$
(15)	$\mathrm{subst}_<$, (14)	$\bar{y} < 0+\bar{x} \supset \bar{y} < \bar{x}$

Chain (1),(3),(5),(6),(8),(13),(15): $x<y \supset \bar{y} < \bar{x}$

This proof structure only tells us where and how axioms have to be instantiated. In a tableau proof all steps would have to be assembled into one large chain of application of implications.

The above axioms are almost sufficient to uniquely characterize integers. In fact, it is difficult to construct a model different from the standard integers that satisfies all the axioms. Because of linearity, discreteness, and monotonicity of < wrt. addition, and the property that we just proved, the elements of the domain must be arranged in a linear order

$\texttt{...1}\overline{\texttt{+}}\texttt{1 < }\overline{\texttt{1}}\texttt{ < 0 < 1 < 1+1 < 1+1+1 ...}$

and, as we will see, the recursive definition of addition is expressed in the identity and associativity axioms. However, there is still some freedom for defining multiplication differently from the standard multiplication. Although `x*(y+1)=(x*y)+x` follows from distributivity and identity, we are not forced to define `x*0=0` for $x \neq 0$.

Furthermore, we have no means to guarantee the existence of other recursively defined functions, because there is still one axiom missing – the induction principle. It states that the domain has to be organized in a way that all properties of a number can be iteratively reduced to a property of zero. Since we allow both positive and negative integers, the induction has to go both ways.

ind: $(P(0) \wedge (\forall x)(0<x \supset P(x-1) \supset P(x)) \wedge (\forall x)(x<0 \supset P(x+1)) \supset P(x)) \supset (\forall x)P(x)$

Like substitution, the induction principle is an axiom scheme. It has to be instantiated for every predicate that is used in the set of formulas under consideration.

All these axioms taken together turn out to be equivalent to those that we know from more direct formalizations of integers, as we will show next.

21.2 Inductively Ordered Integral Domain vs Peano Arithmetic

Most axiomatizations of arithmetic are based on the Peano axioms. These axioms characterize the natural numbers together with the operations + and *. If we include the axioms of equality, then Peano Arithmetic can be defined as

$$\texttt{Peano Arithmetic} \equiv \mathcal{L}(\texttt{=,+,*,0,1; ref, sym, trans, subst, not-surjective, injective, induction, functionality}_{+}\texttt{, add-base, add-step, functionality}_{*}\texttt{, mul-base, mul-step)}$$

where the axioms are as follows

Equality Axioms		
ref:	$(\forall x)\ x=x$	
sym:	$(\forall x,y)\ (x=y \supset y=x)$	
trans:	$(\forall x,y,z)\ ((x=y \wedge y=z) \supset x=z)$	
subst:	$(\forall x,y)\ (x=y \supset P(.,x,.) \supset P(.,y,.))$	*for every P*
Successor Axioms		
non-surjective	$(\forall x)\ \sim(x+1 = 0)$	
injective	$(\forall x,y)\ (x+1=y+1 \supset x=y)$	
induction	$(P(0) \wedge (\forall x)(P(x) \supset P(x+1))) \supset (\forall x)P(x)$	*for every P*
Addition Axioms		
add-base	$(\forall x)\ (x+0 = x)$	
add-step	$(\forall x,y)\ (x+(y+1) = (x+y)+1)$	
Multiplication Axioms		
mul-base	$(\forall x)\ (x*0 = 0)$	
mul-step	$(\forall x,y)\ (x*(y+1) = (x*y)+x)$	

If we drop multiplication and its axioms, we get a very simple arithmetical theory called *Presburger Arithmetic*, which is quite expressive but still decidable. However, it cannot capture all of arithmetic, since this includes the set of computable functions, which are known to be undecidable. Once we include multiplication, however, all of arithmetic can be represented, as we will show later. In the following we will show that the two characterizations do in fact express the same, provided we restrict ourselves to natural numbers.

21.2.1 Inductively Ordered Integral Domains satisfy the Peano Axioms

The equality axioms `ref`, `sym`, `trans`, and `subst` and the functionality laws of addition and multiplication are the same in both formalizations of arithmetic. For the remaining Peano axioms we have to add the restriction `nat(x)` to every quantifier, where `nat(x)` is defined as `nat(x)` $\equiv$ `0<x` $\vee$ `x=0`.

`non-surjective`: Here is a tableau-like derivation of the law of non-surjectivity from the axioms of inductively ordered integral domains.

$F\,\mathbb{Z}\text{-Ax} \supset (\forall x)(\mathrm{nat}(x) \supset \sim(x+1 = 0))$
$T\,\mathbb{Z}\text{-Ax})$
$F\,(\forall x)(\mathrm{nat}(x) \supset \sim(x+1 = 0))$
$F\,(\mathrm{nat}(a) \supset \sim(a+1 = 0))$
$T\,0<a \vee a=0$
$F\sim(a+1 = 0)$
$T\,(a+1 = 0)$

$T\,0<a$	$T\,a=0$	
$T\,0<1$	$T\,0<1$	`lt-0-1`
$T\,0+0<a+1$	$T\,0+1=0$	`lt-mono subst`
$T\,0<a+1$	$T\,1=0$	`ident,subst`
$T\,0<0$	$T\,0<0$	`subst`
$T\sim(0<0)$	$T\sim(0<0)$	`irref`, *derived from* `asym`
$F\,0<0$	$F\,0<0$	
$\times$	$\times$	

For the remaining proofs we will use a more conventional reasoning style, as the formal proofs become quite tedious. It should be noted, however, that all the laws can be derived by purely logical reasoning from the axioms. No semantical reasoning or knowledge about the integers is involved.

`injective`: The law $(\forall x,y)\ (x+1=y+1 \supset x=y)$ can be proven as follows.

	$x+1=y+1$	
$\supset$	$(x+1)+\bar{1} = (y+1)+\bar{1}$	`functionality`
$\supset$	$x+(1+\bar{1}) = y+(1+\bar{1})$	`assoc`
$\supset$	$x+0 = y+0$	`inv, subst`
$\supset$	$x = y$	$\texttt{ident}_+$, `subst`

`induction`: The law $(P(0) \wedge (\forall x)(P(x) \supset P(x+1))) \supset (\forall x)P(x)$ *for every* P is a special instance of the induction axiom `ind`, restricted to natural numbers.

`add-base`: $(\forall x)\ (x+0 = x)$ is an instance of $\texttt{ident}_+$

`add-step`: $(\forall x,y)\ (x+(y+1) = (x+y)+1)$ is an instance of $\texttt{assoc}_+$

`mul-base`: `(∀x) (x*0 = 0)` This actually requires an inductive proof. We use the already proven law of induction from Peano Arithmetic for this purpose.

The base case uses `ident`$_+$, `ident`$_*$, and `distrib`

```
0*0 = 0*0 + 0 = 0*0 + 0*1 = 0*(0+1) = 0*1 = 0
```

In the step case we prove `x*0 = 0 ⊃ (x+1)*0 = 0` as follows.

```
x*0 = 0  ⊃  (x+1)*0 = x*0 + 1*0 = 0+0 = 0
```

`mul-step`: `(∀x,y) (x*(y+1) = (x*y)+x)` can be shown using `distrib`, `ident`$_*$, and `subst`.

```
x*(y+1) = (x*y) + (x*1)= (x*y) + x
```

Thus all inductively ordered integral domains must satisfy the Peano Axioms.

21.2.2 Algebraic laws of Peano Arithmetic

Proving the laws of inductively ordered integral domains from the Peano axioms is possible, but quite tedious. One has to proceed in a particular order, since otherwise the proofs become very difficult. We give a few examples

Equality and functionality laws are the same in both cases. functional notation

`assoc`$_+$: `(∀x,y,z) ((x+y)+z = x+(y+z))` has to be proven by induction.

```
((x+y)+0 = x+y = x+(y+0) add-base, subst

(x+y)+z = x+(y+z) ⊃ (x+y)+(z+1) = ((x+y)+z)+1     add-base
                                = (x+(y+z))+1     subst
                                = x+((y+z)+1)     add-base
                                = x+(y+(z+1))     add-base, subst
```

`ident`$_+$: The first part of `(∀x)( x+0 = x ∧ 0+x = x)` corresponds to the axiom `add-base`, the second is proven by induction.

```
0+0 = 0
0+x = x  ⊃  0+(x+1) = (0+x)+1 = x+1
```

`comm`$_+$: `(∀x,y) (x+y = y+x)` needs a double induction. The base case is an instance of `ident`$_+$. For the step case we first prove `(∀x) (x+1 = 1+x)`.

```
0+1 = 1 = 1+0
x+1 = 1+x  ⊃  (x+1)+1 = (1+x)+1 = 1+(x+1)
```

We then use the law in the remaining argument.

```
x+y = y+x  ⊃  x+(y+1) = (x+y)+1 = (y+x)+1 = 1+(y+x) = (1+y)+x = (y+1)+x
```

`inv`: This law does not hold for natural numbers

`assoc`$_*$, `ident`$_*$, `comm`$_*$: similar to the laws for addition.

`distrib`: The first part of $(\forall$`x,y,z)( x*(y+z) = x*y + x*z` $\wedge$ `(x+y)*z = x*z + y*z)` implies the second since we have commutativity for both addition and multiplication. Again we need induction

```
x*(y+0) = x*y = x*y + 0 = x*y + x*0
x*(y+z) = x*y + x*z  ⊃  x*(y+(z+1)) = x*((y+z)+1))
                                    = (x*(y+z)) + x
                                    = (x*y + x*z) + x
                                    = x*y + (x*z + x)
                                    = x*y + (x*(z+1))
```

`Z`: To prove $(\forall$`x,y)( x*y = 0` $\supset$ `(x=0` $\vee$ `y=0)` we first show a generalization of the non-surjectivity axiom: $(\forall$`x,y)(x+y=0` $\supset$ `y=0)`. Again we use induction.

```
x+0 = 0 ⊃  0 = 0
x+(y+1) = 0  ⊃  (x+y)+1 = 0  ∧ ∼((x+y)+1 = 0) ⊃ False ⊃ (y+1) = 0
```

We use this law in the induction step.

```
x*0 = 0  ⊃ 0=0
(x*y = 0  ⊃  (x=0 ∨ y=0))  ⊃  x*(y+1) = 0
                           ⊃  (x*y)+x = 0
                           ⊃  x = 0
                           ⊃  (x=0 ∨ (y+1)=0)
```

For the discrete linear order we define `x<y` $\equiv$ $(\exists$`z)(x+z+1 =y)`. The seven axioms can then be proven by induction.

21.3 Nonstandard Integers

A few weeks ago we have proven the compactness of first-order logic, which means that a denumerable set S of first-order formulas is uniformly satisfiable in a denumerable domain if all finite subsets of S are satisfiable. In other words, an infinite set of axioms has a model if all its finite subsets have one. This observation allows us to construct a non-standard model of integers.

Consider the set

$S =$ `Peano Axioms` $\cup$ {, $\sim$(a_0=0), $\sim$(a_0=1), $\sim$(a_0=1+1), $\sim$(a_0=1+1+1), ...}.

Clearly every finite subset of S has a model, since we can always pick a constant that is greater than all the (interpretations of) numbers mentioned in that finite set. By compactness, the whole set S *must be satisfiable*, that is there is a model $\langle$D,=,+,*,0,1$\rangle$ where D is a enumerable set that contains $\mathbb{N}$ and a constant a_0 that is different from, or greater than, all the natural numbers.

Since the operations + and * are defined on all elements of D there must also be elements a_0+1, a_0+1+1, a_0+1+1, ... and we can go on defining a set S_1 that yields a constant, which is greater than all these values, and define set S_2, S_3, ... to go on further. We call the elements created this way *nonstandard* numbers because they do behave like numbers but are infinitely large. The laws of logic guarantee that such numbers must exist. We may even go on and diagonalize over the sets S_i to get even larger constants than that, but we must remain in the realm of denumerable sets to use the compactness argument.