Inductively Ordered Integral Domains

The integers as we know them are an integral 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. The axioms are the following.

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:	$(\forall x,y)(\ x*y = 0 \supset (x{=}0 \vee y{=}0))$

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.

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 induction principle 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.

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

```
Peano Arithmetic ≡ ℒ(=,+,∗,0,1; ref, sym, trans, subst,
                          not-surjective, injective, induction,
                          functionality₊, add-base, add-step,
                          functionality∗, 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.

Inductively Ordered Integral Domains satisfy the Peano Axioms and vice versa.