THE NATURAL NUMBERS

The *additive structure* $(\mathbb{N}, 0, +)$ of natural numbers with zero and addition satisfies the following:

- Monoid laws

$$0 + n = n = n + 0 \quad , \quad (l + m) + n = l + (m + n)$$

- Commutativity law

$$m + n = n + m$$

and as such is what in the mathematical jargon is referred to as a *commutative monoid*.

Also the *multiplicative structure* $(\mathbb{N}, 1, \cdot)$ of natural numbers with one and multiplication is a commutative monoid:

- Monoid laws

$$1 \cdot n = n = n \cdot 1 \quad , \quad (l \cdot m) \cdot n = l \cdot (m \cdot n)$$

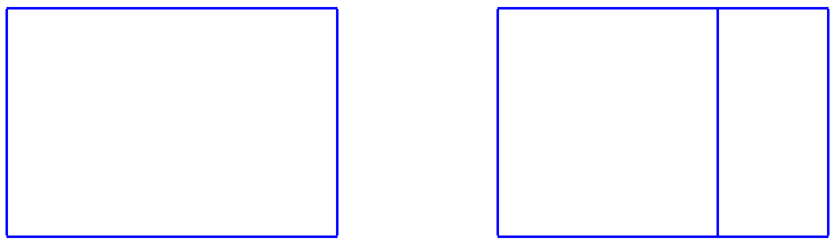
- Commutativity law

$$m \cdot n = n \cdot m$$

The additive and multiplicative structures interact nicely in that they satisfy the

- Distributive law

$$l \cdot (m + n) \quad = \quad l \cdot m + l \cdot n$$



and make the overall structure $(\mathbb{N}, 0, +, 1, \cdot)$ into what in the mathematical jargon is referred to as a *commutative semiring*.

A *semiring* is a structure consisting of

- elements
- commutative monoid structure $(0,+)$
- monoid structure $(1,\cdot)$

satisfying distributivity

$$0\cdot x = 0 = x\cdot 0 \qquad (x+y)\cdot z = x\cdot z + y\cdot z$$

$$x\cdot(y+z) = x\cdot y + x\cdot z$$

It is *commutative* when so is $\cdot$.

A binary operation satisfies cancellation on the left whenever

Cancellation

$x * y = x * z \implies y = z$

The additive and multiplicative structures of natural numbers further satisfy the following laws.

- Additive cancellation

  For all natural numbers k, m, n,

  $$k + m = k + n \implies m = n \quad .$$

- Multiplicative cancellation

  For all natural numbers k, m, n,

  $$\text{if } k \neq 0 \text{ then } k \cdot m = k \cdot n \implies m = n \quad .$$

Inverses

Definition 42

1. *A number* x *is said to admit an* additive inverse *whenever there exists a number* y *such that* $x + y = 0$*.*

In a monoid, say with binary operation $*$ and neutral element e, an inverse for an element x is an element y such that $x*y=e$ and $y*x=e$.

<u>NB</u> If x has inverse y then we may cancelate

$$x*a = x*b \Rightarrow \underbrace{y*x*a}_{= a} = \underbrace{y*x*b}_{= b}$$

Inverses

Definition 42

1. *A number* x *is said to admit an* additive inverse *whenever there exists a number* y *such that* $x + y = 0$*.*

2. *A number* x *is said to admit a* multiplicative inverse *whenever there exists a number* y *such that* $x \cdot y = 1$*.*

Prop. Inverses, whenever they exist, are unique

In a monoid $(e, *)$

Suppose x has inverses y and z. That is

$x * y = e$, $y * x = e$, $z * x = e$, $x * z = e$

$$x * y = e = x * z$$

$$\Rightarrow \quad \begin{array}{c} y * x * y = y * x * z = e * z = z \\ \| \\ e * y = y \end{array}$$

$\boxtimes$

```
-- Proposition
Uniqueness :
  -- Consider
  ( M : Set ) ( e : M ) ( _*_ : M → M → M )
  -- a set M with an element e and a binary operation * such that
  ( y*[x*z]=[y*x]*z : -- * is associative
      ∀{ y x z : M } → ( y * ( x * z ) ) == ( ( y * x ) * z ) )
  ( [y*e]=y : -- e is right neutral
      ∀{ y : M } → y == ( y * e ) )
  ( [e*z]=z : -- e is left neutral
      ∀{ z : M } → ( e * z ) == z )
  -- For all
  ( x y z : M )
    -- if
    → ( ( y * x ) == e ) -- y is a left inverse of x
    -- and
    → ( e == ( x * z ) )  -- z is a right inverse of x
    -- then
    → ( y == z )
    -- they are equal

```

```
-- Proof
Uniqueness M e _*_ y*[x*z]=[y*x]*z y=[y*e] [e*z]=z x y z [y*x]=e e=[x*z]
  = y
      =⟨ y=[y*e] ⟩
    ( y * e )
      =⟨ e=[x*z] |in-ctx y*- ⟩
    ( y * ( x * z ) )
      =⟨ y*[x*z]=[y*x]*z ⟩
    ( ( y * x ) * z )
      =⟨ [y*x]=e |in-ctx -*z ⟩
    ( e * z )
      =⟨ [e*z]=z ⟩
    z
      =
 where
   y*- : M → M
   y*- a = y * a
   -*z : M → M
   -*z a = a * z
```

Extending the system of natural numbers to: (i) admit all additive inverses and then (ii) also admit all multiplicative inverses for non-zero numbers yields two very interesting results:

Extending the system of natural numbers to: (i) admit all additive inverses and then (ii) also admit all multiplicative inverses for non-zero numbers yields two very interesting results:

(i) the *integers*

$$\mathbb{Z} \ : \quad \ldots -n\,,\ \ldots\,,\ -1\,,\ 0\,,\ 1\,,\ \ldots\,,\ n\,,\ \ldots$$

which then form what in the mathematical jargon is referred to as a *commutative ring*, and

(ii) the *rationals* $\mathbb{Q}$ which then form what in the mathematical jargon is referred to as a *field*.

- A **group** is a monoid in which every element has an inverse
- A **ring** is a semiring $(0,+), (1,\cdot)$ where $(0,+)$ is group. It is commutative if so is $(1,\cdot)$.
- A **field** is a ring where every non-zero element has a multiplicative inverse.

To be shown shortly

The division theorem and algorithm

Theorem 43 (Division Theorem) *For every natural number* m *and positive natural number* n*, there exists a unique pair of integers* q *and* r *such that* $q \geq 0$*,* $0 \leq r < n$*, and* $m = q \cdot n + r$*.*

!

quotient

remainder

Uniqueness

Suppose q, r are such that $m = q \cdot n + r$

$q \geq 0$, $0 \leq r < n$

and q', r' such that $m = q' \cdot n + r'$

$q' \geq 0$, $0 \leq r' < n$

Then $q \cdot n + r = q' \cdot n + r'$.

W.l.o.g. assume $r \geq r'$

$$\left.\begin{array}{l} r - r' = q'n - q \cdot n = (q' - q) \cdot n \\ r - r' < n \end{array}\right\} \Rightarrow q' - q = 0$$

$$q = q'$$

So $q n + r = q \cdot n + r'$

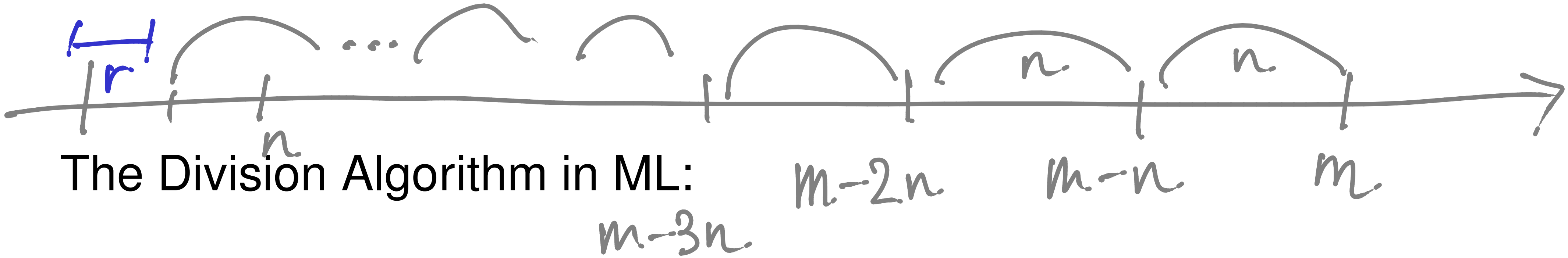
$$\underset{\text{cancellation}}{\Longrightarrow} \quad r = r'.$$

$\boxtimes$

The division theorem and algorithm

Theorem 43 (Division Theorem) *For every natural number* m *and positive natural number* n*, there exists a unique pair of integers* q *and* r *such that* $q \geq 0$, $0 \leq r < n$*, and* $m = q \cdot n + r$*.*

Definition 44 *The natural numbers* q *and* r *associated to a given pair of a natural number* m *and a positive integer* n *determined by the Division Theorem are respectively denoted* $\mathrm{quo}(m, n)$ *and* $\mathrm{rem}(m, n)$*.*



The Division Algorithm in ML:

```
fun divalg( m , n )
  = let
      fun diviter( q , r )
        = if r < n then ( q , r )
          else diviter( q+1 , r-n )
    in
      diviter( 0 , m )
    end

fun quo( m , n ) = #1( divalg( m , n ) )

fun rem( m , n ) = #2( divalg( m , n ) )
```

$m \geq 0,\ n > 0$

$\underline{\text{divalg}}(m,n)$

$\|$

$\underline{\text{diviter}}(0,m)$ $\quad m = 0 \cdot n + m$

$m < n$

$(0,m)$

$\underline{\text{diviter}}(1, m-n)$ $\quad m = 1 \cdot n + (m-n)$

$m-n<n$

$(1, m-n)$

$\underline{\text{diviter}}(2, \overbrace{(m-n)-n}^{m-2n})$

$m = 2 \cdot n + (m-2n)$

Partial Correctness

$m = q \cdot n + r$

$\underline{\text{diviter}}(q, r)$

$r \geq n$

$\underline{\text{diviter}}(q+1, r-n)$

$m = (q+1) \cdot n + (r-n)$

$\vdots$

$r_0 < n$ $\quad$ $\underline{\text{diviter}}(q_0, r_0)$

We established an <u>invariance</u> of the the computation

$m = q_0 \cdot n + r_0$

(q_0, r_0)

Termination

diviter(0, m)

diviter(q, r)

diviter(q+1, r−n)

The second argument always decreases while remaining positive.

Theorem 45 *For every natural number* m *and positive natural number* n*, the evaluation of* $\texttt{divalg}(m, n)$ *terminates, outputing a pair of natural numbers* (q_0, r_0) *such that* $r_0 < n$ *and* $m = q_0 \cdot n + r_0$*.*

PROOF: