Lemma 42 *A positive real number* x *is rational iff*

$$\exists \textit{ positive integers } m, n : \quad x = m/n \wedge \neg(\exists \textit{ prime } p : p \mid m \wedge p \mid n) \qquad (\dagger)$$

PROOF: ($\Leftarrow$) Straightforward.

($\Rightarrow$) Let x be a positive rational number; so, by definition, (1) $x = m_0/n_0$ for some positive integers m_0 and n_0.

RTP: The statement ($\dagger$).

We proceed by contradiction. So assume that ($\dagger$) is not the case.

Equivalently, we have:

$\neg(\exists \text{ pos. int. } m,n.\ x = m/n \wedge \neg(\exists \text{ prime } p.\ p|m \wedge p|n))$

$\iff \forall \text{ pos. int } m,n.\ \neg(x = m/n \wedge \neg(\exists \text{ prime } p.\ p|m \wedge p|n))$

$\iff \forall \text{ pos. int } m,n.\ \neg(x = m/n) \vee (\exists \text{ prime } p.\ p|m \wedge p|n)$

$\stackrel{(2)}{\iff} \forall \text{ pos. int } m,n.\ x = m/n \Rightarrow (\exists \text{ prime } p.\ p|m \wedge p|n)$

By instantiation:

(3) $x = m_0/n_0 \Rightarrow \exists \text{ prime } p.\ p|m_0 \wedge p|n_0$

So from (1) and (3), we have $\exists \text{ prime } p.\ p|m_0 \wedge p|n_0$

Let p_0 be such a prime. That is $m_0 = p_0 \cdot m_1$ and $n_0 = p_0 \cdot n_1$ for pos. int. m_1 and n_1.

Then $x = m_1/n_1$

and again

$$x = m_1/n_1 \Rightarrow (\exists \text{ prime } p.\ p \mid m_1 \text{ and } p \mid n_1)$$

So $\exists$ prime $p.\ p \mid m_1 \wedge p \mid n_1$

Say $p_1 \mid m_1$ and $p_1 \mid n_1$; so that $m_1 = p_1 \cdot m_2$ and $n_1 = p_1 \cdot n_2$ for pos. int m_2 and n_2.

Repeating the argument, we have

$$m_0 = p_0 \cdot m_1 = p_0 \cdot p_1 \cdot m_2 = \cdots = p_0 \cdot p_1 \cdots p_\ell \cdot m_{\ell+1}$$

$$\geq 2^\ell \quad \text{for all } \ell$$

In particular for $l = m_0$, we have

$$m_0 \geq 2^{m_0}$$

which is a contradiction $\boxtimes$.

Numbers

Objectives

- Get an appreciation for the abstract notion of number system, considering four examples: natural numbers, integers, rationals, and modular integers.
- Prove the correctness of three basic algorithms in the theory of numbers: the division algorithm, Euclid's algorithm, and the Extended Euclid's algorithm.
- Exemplify the use of the mathematical theory surrounding Euclid's Theorem and Fermat's Little Theorem in the context of public-key cryptography.
- To understand and be able to proficiently use the Principle of Mathematical Induction in its various forms.

Natural numbers

In the beginning there were the *natural numbers*

$$\mathbb{N} : \quad 0 \, , \quad 1 \, , \quad \ldots \, , \quad n \, , \quad n+1 \, , \quad \ldots$$

generated from *zero* by successive increment; that is, put in ML:

```
datatype
  N = zero | succ of N
```

The basic operations of this number system are:

- Addition

$$\underbrace{\overbrace{*\cdots*}^{m}\overbrace{*\cdots\cdots*}^{n}}_{m+n}$$

- Multiplication

$$m\left\{\overbrace{\begin{matrix} *\cdots\cdots\cdots\cdots* \\ \vdots \quad m\cdot n \quad \vdots \\ *\cdots\cdots\cdots\cdots* \end{matrix}}^{n}\right.$$

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*.

Commutative monoid laws

- Neutral element laws

$$\overbrace{\qquad}^{0}\overbrace{*\cdots\cdots*}^{n} = \overbrace{*\cdots\cdots*}^{n} = \overbrace{*\cdots\cdots*}^{n}\overbrace{\qquad}^{0}$$

- Associativity law

$$\overbrace{*\cdots**\cdots\cdots*}^{\ell+m}\overbrace{*\cdots\cdots*}^{n} = \overbrace{*\cdots*}^{\ell}\overbrace{*\cdots\cdots**\cdots\cdots*}^{m+n}$$

- Commutativity law

$$\overbrace{*\cdots*}^{m}\overbrace{*\cdots\cdots*}^{n} = \overbrace{*\cdots\cdots*}^{n}\overbrace{*\cdots*}^{m}$$

Monoids

Definition 43 *A* monoid *is an algebraic structure with*

- *a* neutral element*, say* e*,*
- *a* binary operation*, say* $\bullet$*,*

satisfying

- neutral element laws*:* $e \bullet x = x = x \bullet e$
- associativity law*:* $(x \bullet y) \bullet z = x \bullet (y \bullet z)$

It makes sense to write: $x \bullet y \bullet z$

Monoids

Definition 43 *A monoid is an algebraic structure with*

- *a neutral element, say e,*
- *a binary operation, say $\bullet$,*

satisfying

- *neutral element laws: $e \bullet x = x = x \bullet e$*
- *associativity law: $(x \bullet y) \bullet z = x \bullet (y \bullet z)$*

A monoid is commutative if:

- *commutativity: $x \bullet y = y \bullet x$*

is satisfied.

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

- Monoid laws

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

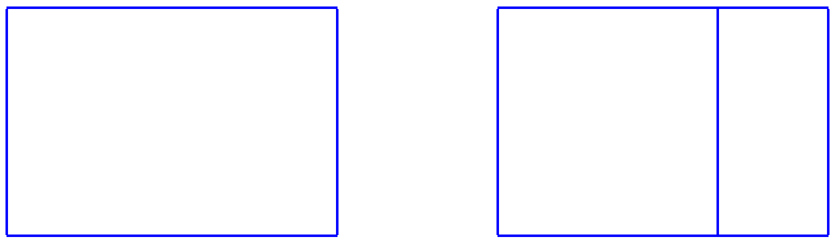
- Commutativity law

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

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

- Distributive laws

$$
\begin{aligned}
l \cdot 0 &= 0 \\
l \cdot (m+n) &= l \cdot m + l \cdot n
\end{aligned}
$$



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

Semirings

Definition 44 *A* semiring *(or* rig*) is an algebraic structure with*

- *a* commutative monoid *structure, say* $(0, \oplus)$*,*
- *a* monoid structure*, say* $(1, \otimes)$*,*

satifying the distributivity laws*:*

- $0 \otimes x = 0 = x \otimes 0$
- $x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$, $(y \oplus z) \otimes x = (y \otimes x) \oplus (z \otimes x)$

A semiring is commutative *whenever* $\otimes$ *is.*

Cancellation

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,

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

Definition 45 *A binary operation* $\bullet$ *allows* cancellation *by an element* c

- on the left*: if* $c \bullet x = c \bullet y$ *implies* $x = y$
- on the right*: if* $x \bullet c = y \bullet c$ *implies* $x = y$

Example: The append operation on lists allows cancellation by any list on both the left and the right.

Inverses

Definition 46 *For a monoid with a neutral element* e *and a binary operation* $\bullet$*, and element* x *is said to admit an*

- inverse on the left *if there exists an element* ℓ *such that* $\ell \bullet x = e$
- inverse on the right *if there exists an element* r *such that* $x \bullet r = e$
- inverse *if it admits both left and right inverses*

$\Downarrow$ cancellation: suppose x has left inverse ℓ

Then $x \cdot y = x \cdot z \Rightarrow y = z$

Because if $x \cdot y = x \cdot z$ Then

$\ell \cdot x \cdot y = \ell \cdot x \cdot z$ and so

$e \cdot y = e \cdot z$ and we are done.

Inverses

Definition 46 *For a monoid with a neutral element* e *and a binary operation* $\bullet$*, and element* x *is said to admit an*

- inverse on the left *if there exists an element* ℓ *such that* $\ell \bullet x = e$
- inverse on the right *if there exists an element* r *such that* $x \bullet r = e$
- inverse *if it admits both left and right inverses*

Proposition 47 *For a monoid* $(e, \bullet)$ *if an element admits an inverse then its left and right inverses are equal.*

PROOF: ($\Rightarrow$) By definition

($\Leftarrow$) Say x has left inverse ℓ and right inverse r.

RTP: $\ell = r$.

$$\ell = \ell \cdot e = \ell \cdot (x \cdot r) = (\ell \cdot x) \cdot r = e \cdot r = r \qquad \boxtimes$$

$$e = x \cdot r \qquad\qquad \ell \cdot x = e$$

Groups

Definition 49 *A* group *is a monoid in which every element has an inverse.*

An Abelian group *is a group for which the monoid is commutative.*

Inverses

Definition 50

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* $x \cdot y = 1$*.*

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*.

Rings

Definition 51 *A* ring *is a semiring* $(0, \oplus, 1, \otimes)$ *in which the commutative monoid* $(0, \oplus)$ *is a group.*

A ring is commutative *if so is the monoid* $(1, \otimes)$.

Fields

Definition 52 *A* field *is a commutative ring in which every element besides* 0 *has a reciprocal (that is, and inverse with respect to* $\otimes$*).*