Mathematics for Computer Scientists 2 (G52MC2)

L09 : Some algebra

Thorsten Altenkirch

School of Computer Science
University of Nottingham

November 11, 2009

Monoids

- $(\mathbb{N}, +, 0)$ is a **monoid**, i.e. it satisfies the following properties:

$$\begin{array}{rcll} 0 + m & = & m & \texttt{plus\_0\_l} \\ n + 0 & = & n & \texttt{plus\_0\_r} \\ m + (n + p) & = & (m + n) + p & \texttt{plus\_assoc} \end{array}$$

- It is actually a **commutative** monoid:

$$m + n \quad = \quad n + m \quad \texttt{plus\_comm}$$

- In a commutative monoid left and right neutrality are equivalent.
- Do you know a non-commutative monoid?

Semirings

- $(\mathbb{N}, +, 0, \times, 1)$ is a **semiring**: Both $(\mathbb{N}, +, 0)$ and $(\mathbb{N}, \times, 1)$ are monoids and

$$
\begin{array}{rcll}
0 \times n & = & 0 & \texttt{mult\_0\_r} \\
n \times 0 & = & 0 & \texttt{mult\_0\_l} \\
(m + n) \times p & = & m \times p + n \times p & \texttt{mult\_plus\_distr\_r} \\
m \times (n + p) & = & m \times n + m \times p & \texttt{mult\_plus\_distr\_l}
\end{array}
$$

- Indeed, $(\mathbb{N}, +, 0, \times, 1)$ is a **commutative monoids**, because $(\mathbb{N}, +, 0)$ and $(\mathbb{N}, \times, 1)$ are commutative semigroups.
- In a commutative semiring left and right distributivity are equivalent.
- Why is this *semi* (greek for half)?

Groups, rings and ...

- $(\mathbb{Z}, +, 0, -(\_))$ is a **group** because $(\mathbb{Z}, +, 0)$ is a monoid and every element has inverses:

$$\begin{array}{rcll} -m + m & = & 0 & \text{left inverse} \\ m + -m & = & 0 & \text{right inverse} \end{array}$$

- $(\mathbb{Z}, +, 0, -(\_), \times, 1)$ is a **ring** because $(\mathbb{Z}, +, 0, \times, 1)$ is a semiring and $(\mathbb{Z}, +, 0, -(\_))$ is a group.
- Can $\times$ be turned into a group, too? What are examples? How is this structure called?