# Interval monoids

Jean Michel

University Paris Diderot

Berlin, tuesday 31st August 2021

# Interval monoids

Let $W$ be a group, and $R \subset W$ a finite subset which generates positively $W$; that is, any element $w \in W$ can be written $w = r_1 \cdots r_n$, with $r_i \in R$.

Then we define the $R$-length $l_R(w)$ as the minimum $n$ in such a decomposition of $w$. And we define a left divisibility relation $\leq_R$ on $W$ by

$$a \leq_R c \qquad \text{if and only if} \qquad l_R(a) + l_R(a^{-1}c) = l_R(c),$$

that is, we have a product $ab = c$ where lengths add.

Left divisibility is a partial order. We call a *left interval* a subset of $W$ stable by taking left divisors.

Symmetrically we can define right divisibility $c \geq_R a$ and call *balanced interval* a subset stable by taking left and right divisors.

Let $S$ be a balanced interval. We define the *interval monoid* $M(\mathbf{S})$ whose generators are a copy $\mathbf{S}$ of $S$ by the presentation

$$M(\mathbf{S}) = \langle \mathbf{S} \mid \mathbf{ab} = \mathbf{c} \text{ if } l_R(a) + l_R(b) = l_R(c) \text{ and } ab = c \rangle$$

# Interval monoids

Let $W$ be a group, and $R \subset W$ a finite subset which generates positively $W$; that is, any element $w \in W$ can be written $w = r_1 \cdots r_n$, with $r_i \in R$.
Then we define the $R$-length $l_R(w)$ as the minimum $n$ in such a decomposition of $w$. And we define a left divisibility relation $\leq_R$ on $W$ by

$$a \leq_R c \qquad \text{if and only if} \qquad l_R(a) + l_R(a^{-1}c) = l_R(c),$$

that is, we have a product $ab = c$ where lengths add.
Left divisibility is a partial order. We call a *left interval* a subset of $W$ stable by taking left divisors.
Symmetrically we can define right divisibility $c \geq_R a$ and call *balanced interval* a subset stable by taking left and right divisors.
Let $S$ be a balanced interval. We define the *interval monoid* $M(\mathbf{S})$ whose generators are a copy $\mathbf{S}$ of $S$ by the presentation

$$M(\mathbf{S}) = \langle \mathbf{S} \mid \mathbf{ab} = \mathbf{c} \text{ if } l_R(a) + l_R(b) = l_R(c) \text{ and } ab = c \rangle$$

# Interval monoids

Let $W$ be a group, and $R \subset W$ a finite subset which generates positively $W$; that is, any element $w \in W$ can be written $w = r_1 \cdots r_n$, with $r_i \in R$.

Then we define the $R$-length $l_R(w)$ as the minimum $n$ in such a decomposition of $w$. And we define a left divisibility relation $\leq_R$ on $W$ by

$$a \leq_R c \qquad \text{if and only if} \qquad l_R(a) + l_R(a^{-1}c) = l_R(c),$$

that is, we have a product $ab = c$ where lengths add.

Left divisibility is a partial order. We call a *left interval* a subset of $W$ stable by taking left divisors.

Symmetrically we can define right divisibility $c \geq_R a$ and call *balanced interval* a subset stable by taking left and right divisors.

Let $S$ be a balanced interval. We define the *interval monoid* $M(\mathbf{S})$ whose generators are a copy $\mathbf{S}$ of $S$ by the presentation

$$M(\mathbf{S}) = \langle \mathbf{S} \mid \mathbf{ab} = \mathbf{c} \text{ if } l_R(a) + l_R(b) = l_R(c) \text{ and } ab = c \rangle$$

# Interval monoids

Let $W$ be a group, and $R \subset W$ a finite subset which generates positively $W$; that is, any element $w \in W$ can be written $w = r_1 \cdots r_n$, with $r_i \in R$.
Then we define the $R$-length $l_R(w)$ as the minimum $n$ in such a decomposition of $w$. And we define a left divisibility relation $\leq_R$ on $W$ by

$$a \leq_R c \qquad \text{if and only if} \qquad l_R(a) + l_R(a^{-1}c) = l_R(c),$$

that is, we have a product $ab = c$ where lengths add.
Left divisibility is a partial order. We call a *left interval* a subset of $W$ stable by taking left divisors.
Symmetrically we can define right divisibility $c \geq_R a$ and call *balanced interval* a subset stable by taking left and right divisors.
Let $S$ be a balanced interval. We define the *interval monoid* $M(\mathbf{S})$ whose generators are a copy $\mathbf{S}$ of $S$ by the presentation

$$M(\mathbf{S}) = \langle \mathbf{S} \mid \mathbf{ab} = \mathbf{c} \text{ if } l_R(a) + l_R(b) = l_R(c) \text{ and } ab = c \rangle$$

# Interval monoids

Let $W$ be a group, and $R \subset W$ a finite subset which generates positively $W$; that is, any element $w \in W$ can be written $w = r_1 \cdots r_n$, with $r_i \in R$.
Then we define the $R$-length $l_R(w)$ as the minimum $n$ in such a decomposition of $w$. And we define a left divisibility relation $\leq_R$ on $W$ by

$$a \leq_R c \qquad \text{if and only if} \qquad l_R(a) + l_R(a^{-1}c) = l_R(c),$$

that is, we have a product $ab = c$ where lengths add.
Left divisibility is a partial order. We call a *left interval* a subset of $W$ stable by taking left divisors.
Symmetrically we can define right divisibility $c \geq_R a$ and call *balanced interval* a subset stable by taking left and right divisors.
Let $S$ be a balanced interval. We define the *interval monoid* $M(\mathbf{S})$ whose generators are a copy $\mathbf{S}$ of $S$ by the presentation

$$M(\mathbf{S}) = \langle \mathbf{S} \mid \mathbf{ab} = \mathbf{c} \text{ if } l_R(a) + l_R(b) = l_R(c) \text{ and } ab = c \rangle$$

# Interval monoids

Let $W$ be a group, and $R \subset W$ a finite subset which generates positively $W$; that is, any element $w \in W$ can be written $w = r_1 \cdots r_n$, with $r_i \in R$.

Then we define the $R$-length $l_R(w)$ as the minimum $n$ in such a decomposition of $w$. And we define a left divisibility relation $\leq_R$ on $W$ by

$$a \leq_R c \qquad \text{if and only if} \qquad l_R(a) + l_R(a^{-1}c) = l_R(c),$$

that is, we have a product $ab = c$ where lengths add.

Left divisibility is a partial order. We call a *left interval* a subset of $W$ stable by taking left divisors.

Symmetrically we can define right divisibility $c \geq_R a$ and call *balanced interval* a subset stable by taking left and right divisors.

Let $S$ be a balanced interval. We define the *interval monoid* $M(\mathbf{S})$ whose generators are a copy $\mathbf{S}$ of $S$ by the presentation

$$M(\mathbf{S}) = \langle \mathbf{S} \mid \mathbf{ab} = \mathbf{c} \text{ if } l_R(a) + l_R(b) = l_R(c) \text{ and } ab = c \rangle$$

# Garside interval monoids

**Theorem**

*If the interval $S \subset W$ is balanced and is a lattice for $\leq_R$ and $\geq_R$, then $M(\mathbf{S})$ has $\mathbf{S}$ as a Garside family.*

The lattice condition means that there are least common multiples and greatest common divisors for left and right divisibility.
For least common multiples we can allow a weakening: roughly, elements which have a common multiple have a least one.

Two applications are a construction of the Artin monoids and the dual monoids.

If $W, S$ is a finite Coxeter system, then $W$ is a lattice for $\leq_S$ and $\geq_S$ (called also the left and right weak Bruhat order). Then $M(\mathbf{W})$ is the Artin monoid attached to $W$. This can be extended to infinite Coxeter systems weakening the lcm axiom, thus getting a locally Garside monoid.

# Garside interval monoids

**Theorem**

*If the interval $S \subset W$ is balanced and is a lattice for $\leq_R$ and $\geq_R$, then $M(\mathbf{S})$ has $\mathbf{S}$ as a Garside family.*

The lattice condition means that there are least common multiples and greatest common divisors for left and right divisibility.
For least common multiples we can allow a weakening: roughly, elements which have a common multiple have a least one.

Two applications are a construction of the Artin monoids and the dual monoids.

If $W, S$ is a finite Coxeter system, then $W$ is a lattice for $\leq_S$ and $\geq_S$ (called also the left and right weak Bruhat order). Then $M(\mathbf{W})$ is the Artin monoid attached to $W$. This can be extended to infinite Coxeter systems weakening the lcm axiom, thus getting a locally Garside monoid.

# Garside interval monoids

**Theorem**

*If the interval $S \subset W$ is balanced and is a lattice for $\leq_R$ and $\geq_R$, then $M(\mathbf{S})$ has $\mathbf{S}$ as a Garside family.*

The lattice condition means that there are least common multiples and greatest common divisors for left and right divisibility.
For least common multiples we can allow a weakening: roughly, elements which have a common multiple have a least one.

Two applications are a construction of the Artin monoids and the dual monoids.

If $W, S$ is a finite Coxeter system, then $W$ is a lattice for $\leq_S$ and $\geq_S$ (called also the left and right weak Bruhat order). Then $M(\mathbf{W})$ is the Artin monoid attached to $W$. This can be extended to infinite Coxeter systems weakening the lcm axiom, thus getting a locally Garside monoid.

# Garside interval monoids

**Theorem**

*If the interval $S \subset W$ is balanced and is a lattice for $\leq_R$ and $\geq_R$, then $M(\mathbf{S})$ has $\mathbf{S}$ as a Garside family.*

The lattice condition means that there are least common multiples and greatest common divisors for left and right divisibility.
For least common multiples we can allow a weakening: roughly, elements which have a common multiple have a least one.

Two applications are a construction of the Artin monoids and the dual monoids.

If $W, S$ is a finite Coxeter system, then $W$ is a lattice for $\leq_S$ and $\geq_S$ (called also the left and right weak Bruhat order). Then $M(\mathbf{W})$ is the Artin monoid attached to $W$. This can be extended to infinite Coxeter systems weakening the lcm axiom, thus getting a locally Garside monoid.

# Garside interval monoids

**Theorem**

*If the interval $S \subset W$ is balanced and is a lattice for $\leq_R$ and $\geq_R$, then $M(\mathbf{S})$ has $\mathbf{S}$ as a Garside family.*

The lattice condition means that there are least common multiples and greatest common divisors for left and right divisibility.
For least common multiples we can allow a weakening: roughly, elements which have a common multiple have a least one.

Two applications are a construction of the Artin monoids and the dual monoids.

If $W, S$ is a finite Coxeter system, then $W$ is a lattice for $\leq_S$ and $\geq_S$ (called also the left and right weak Bruhat order). Then $M(\mathbf{W})$ is the Artin monoid attached to $W$. This can be extended to infinite Coxeter systems weakening the lcm axiom, thus getting a locally Garside monoid.

# Garside interval monoids

**Theorem**

*If the interval $S \subset W$ is balanced and is a lattice for $\leq_R$ and $\geq_R$, then $M(\mathbf{S})$ has $\mathbf{S}$ as a Garside family.*

The lattice condition means that there are least common multiples and greatest common divisors for left and right divisibility.
For least common multiples we can allow a weakening: roughly, elements which have a common multiple have a least one.

Two applications are a construction of the Artin monoids and the dual monoids.

If $W, S$ is a finite Coxeter system, then $W$ is a lattice for $\leq_S$ and $\geq_S$ (called also the left and right weak Bruhat order). Then $M(\mathbf{W})$ is the Artin monoid attached to $W$. This can be extended to infinite Coxeter systems weakening the lcm axiom, thus getting a locally Garside monoid.

# Garside interval monoids

**Theorem**

*If the interval $S \subset W$ is balanced and is a lattice for $\leq_R$ and $\geq_R$, then $M(\mathbf{S})$ has $\mathbf{S}$ as a Garside family.*

The lattice condition means that there are least common multiples and greatest common divisors for left and right divisibility.
For least common multiples we can allow a weakening: roughly, elements which have a common multiple have a least one.

Two applications are a construction of the Artin monoids and the dual monoids.

If $W, S$ is a finite Coxeter system, then $W$ is a lattice for $\leq_S$ and $\geq_S$ (called also the left and right weak Bruhat order). Then $M(\mathbf{W})$ is the Artin monoid attached to $W$. This can be extended to infinite Coxeter systems weakening the lcm axiom, thus getting a locally Garside monoid.

# Dual monoid

Let $V = \mathbb{C}^n$. A *complex reflection* is an element of $s \in \mathrm{GL}(V)$ of finite order, whose fixed points are an hyperplane (we say $s$ is a true reflection if it is of order $s^2 = 1$).

A finite complex reflection group is a finite subgroup $W \subset \mathrm{GL}(V)$ generated by complex reflections. We say $W$ is *irreducible* if the representation $V$ is. We say that the irreducible complex reflection group $W \subset \mathrm{GL}(V)$ is *well generated* if it can be generated by $n$ reflections (sometimes $n+1$ is necessary).

If $W$ is a well-generated finite complex reflection group, $R$ is the set of its reflections, $c$ is a Coxeter element (a product of the $n$ generators in some order), then the interval $S$ given by $\{x \in W \mid 1 \leq_R x \leq_R c\}$ is balanced, $S$ is a lattice for $\leq_R$ and $\geq_R$ and $M(\mathbf{S})$ is the *dual monoid* attached to $W$ and $c$.

# Dual monoid

Let $V = \mathbb{C}^n$. A *complex reflection* is an element of $s \in \mathrm{GL}(V)$ of finite order, whose fixed points are an hyperplane (we say $s$ is a true reflection if it is of order $s^2 = 1$).

A finite complex reflection group is a finite subgroup $W \subset \mathrm{GL}(V)$ generated by complex reflections. We say $W$ is *irreducible* if the representation $V$ is. We say that the irreducible complex reflection group $W \subset \mathrm{GL}(V)$ is *well generated* if it can be generated by $n$ reflections (sometimes $n+1$ is necessary).

If $W$ is a well-generated finite complex reflection group, $R$ is the set of its reflections, $c$ is a Coxeter element (a product of the $n$ generators in some order), then the interval $S$ given by $\{x \in W \mid 1 \leq_R x \leq_R c\}$ is balanced, $S$ is a lattice for $\leq_R$ and $\geq_R$ and $M(\mathbf{S})$ is the *dual monoid* attached to $W$ and $c$.

# Dual monoid

Let $V = \mathbb{C}^n$. A *complex reflection* is an element of $s \in \mathrm{GL}(V)$ of finite order, whose fixed points are an hyperplane (we say $s$ is a true reflection if it is of order $s^2 = 1$).
A finite complex reflection group is a finite subgroup $W \subset \mathrm{GL}(V)$ generated by complex reflections. We say $W$ is *irreducible* if the representation $V$ is. We say that the irreducible complex reflection group $W \subset \mathrm{GL}(V)$ is *well generated* if it can be generated by $n$ reflections (sometimes $n+1$ is necessary).

If $W$ is a well-generated finite complex reflection group, $R$ is the set of its reflections, $c$ is a Coxeter element (a product of the $n$ generators in some order), then the interval $S$ given by $\{x \in W \mid 1 \leq_R x \leq_R c\}$ is balanced, $S$ is a lattice for $\leq_R$ and $\geq_R$ and $M(\mathbf{S})$ is the *dual monoid* attached to $W$ and $c$.

# Dual monoid

Let $V = \mathbb{C}^n$. A *complex reflection* is an element of $s \in \mathrm{GL}(V)$ of finite order, whose fixed points are an hyperplane (we say $s$ is a true reflection if it is of order $s^2 = 1$).
A finite complex reflection group is a finite subgroup $W \subset \mathrm{GL}(V)$ generated by complex reflections. We say $W$ is *irreducible* if the representation $V$ is. We say that the irreducible complex reflection group $W \subset \mathrm{GL}(V)$ is *well generated* if it can be generated by $n$ reflections (sometimes $n+1$ is necessary).

If $W$ is a well-generated finite complex reflection group, $R$ is the set of its reflections, $c$ is a Coxeter element (a product of the $n$ generators in some order), then the interval $S$ given by $\{x \in W \mid 1 \leq_R x \leq_R c\}$ is balanced, $S$ is a lattice for $\leq_R$ and $\geq_R$ and $M(\mathbf{S})$ is the *dual monoid* attached to $W$ and $c$.

# Dual monoid

Let $V = \mathbb{C}^n$. A *complex reflection* is an element of $s \in \mathrm{GL}(V)$ of finite order, whose fixed points are an hyperplane (we say $s$ is a true reflection if it is of order $s^2 = 1$).
A finite complex reflection group is a finite subgroup $W \subset \mathrm{GL}(V)$ generated by complex reflections. We say $W$ is *irreducible* if the representation $V$ is. We say that the irreducible complex reflection group $W \subset \mathrm{GL}(V)$ is *well generated* if it can be generated by $n$ reflections (sometimes $n+1$ is necessary).

If $W$ is a well-generated finite complex reflection group, $R$ is the set of its reflections, $c$ is a Coxeter element (a product of the $n$ generators in some order), then the interval $S$ given by $\{x \in W \mid 1 \leq_R x \leq_R c\}$ is balanced, $S$ is a lattice for $\leq_R$ and $\geq_R$ and $M(\mathbf{S})$ is the *dual monoid* attached to $W$ and $c$.

# Dual monoid

Let $V = \mathbb{C}^n$. A *complex reflection* is an element of $s \in \mathrm{GL}(V)$ of finite order, whose fixed points are an hyperplane (we say $s$ is a true reflection if it is of order $s^2 = 1$).
A finite complex reflection group is a finite subgroup $W \subset \mathrm{GL}(V)$ generated by complex reflections. We say $W$ is *irreducible* if the representation $V$ is. We say that the irreducible complex reflection group $W \subset \mathrm{GL}(V)$ is *well generated* if it can be generated by $n$ reflections (sometimes $n+1$ is necessary).

If $W$ is a well-generated finite complex reflection group, $R$ is the set of its reflections, $c$ is a Coxeter element (a product of the $n$ generators in some order), then the interval $S$ given by $\{x \in W \mid 1 \leq_R x \leq_R c\}$ is balanced, $S$ is a lattice for $\leq_R$ and $\geq_R$ and $M(\mathbf{S})$ is the *dual monoid* attached to $W$ and $c$.

# Dual monoid

Let $V = \mathbb{C}^n$. A *complex reflection* is an element of $s \in \mathrm{GL}(V)$ of finite order, whose fixed points are an hyperplane (we say $s$ is a true reflection if it is of order $s^2 = 1$).
A finite complex reflection group is a finite subgroup $W \subset \mathrm{GL}(V)$ generated by complex reflections. We say $W$ is *irreducible* if the representation $V$ is. We say that the irreducible complex reflection group $W \subset \mathrm{GL}(V)$ is *well generated* if it can be generated by $n$ reflections (sometimes $n+1$ is necessary).

If $W$ is a well-generated finite complex reflection group, $R$ is the set of its reflections, $c$ is a Coxeter element (a product of the $n$ generators in some order), then the interval $S$ given by $\{x \in W \mid 1 \leq_R x \leq_R c\}$ is balanced, $S$ is a lattice for $\leq_R$ and $\geq_R$ and $M(\mathbf{S})$ is the *dual monoid* attached to $W$ and $c$.

# Dual monoid

Let $V = \mathbb{C}^n$. A *complex reflection* is an element of $s \in \mathrm{GL}(V)$ of finite order, whose fixed points are an hyperplane (we say $s$ is a true reflection if it is of order $s^2 = 1$).
A finite complex reflection group is a finite subgroup $W \subset \mathrm{GL}(V)$ generated by complex reflections. We say $W$ is *irreducible* if the representation $V$ is. We say that the irreducible complex reflection group $W \subset \mathrm{GL}(V)$ is *well generated* if it can be generated by $n$ reflections (sometimes $n+1$ is necessary).

If $W$ is a well-generated finite complex reflection group, $R$ is the set of its reflections, $c$ is a Coxeter element (a product of the $n$ generators in some order), then the interval $S$ given by $\{x \in W \mid 1 \leq_R x \leq_R c\}$ is balanced, $S$ is a lattice for $\leq_R$ and $\geq_R$ and $M(\mathbf{S})$ is the *dual monoid* attached to $W$ and $c$.

# Germs

Intervals in a group define *germs*, where germs are sets which model subsets of a monoid.

**Definition**

A germ is a set $S$ with a partially defined multiplication $(a, b) \mapsto a \cdot b, S^2 \to S$.

Usually we require germs to be *left associative*, that is:

*If $g \cdot h$ and $f \cdot (g \cdot h)$ are defined, then $f \cdot g$ and $(f \cdot g) \cdot h$ are also defined, and $f \cdot (g \cdot h) = (f \cdot g) \cdot h$.*

There is similarly a *right associativity* condition.
A germ defines a monoid

$$M(S) = \langle S \mid ab = c \text{ if } a \cdot b \text{ is defined and } a \cdot b = c \rangle$$

# Germs

Intervals in a group define *germs*, where germs are sets which model subsets of a monoid.

**Definition**

A germ is a set $S$ with a partially defined multiplication $(a, b) \mapsto a \cdot b, S^2 \to S$.

Usually we require germs to be *left associative*, that is:

*If $g \cdot h$ and $f \cdot (g \cdot h)$ are defined, then $f \cdot g$ and $(f \cdot g) \cdot h$ are also defined, and $f \cdot (g \cdot h) = (f \cdot g) \cdot h$.*

There is similarly a *right associativity* condition.
A germ defines a monoid

$$M(S) = \langle S \mid ab = c \text{ if } a \cdot b \text{ is defined and } a \cdot b = c \rangle$$

# Germs

Intervals in a group define *germs*, where germs are sets which model subsets of a monoid.

**Definition**

A germ is a set $S$ with a partially defined multiplication $(a, b) \mapsto a \cdot b, S^2 \to S$.

Usually we require germs to be *left associative*, that is:

*If $g \cdot h$ and $f \cdot (g \cdot h)$ are defined, then $f \cdot g$ and $(f \cdot g) \cdot h$ are also defined, and $f \cdot (g \cdot h) = (f \cdot g) \cdot h$.*

There is similarly a *right associativity* condition.
A germ defines a monoid

$$M(S) = \langle S \mid ab = c \text{ if } a \cdot b \text{ is defined and } a \cdot b = c \rangle$$

# Germs

Intervals in a group define *germs*, where germs are sets which model subsets of a monoid.

**Definition**

A germ is a set $S$ with a partially defined multiplication $(a, b) \mapsto a \cdot b, S^2 \to S$.

Usually we require germs to be *left associative*, that is:

*If $g \cdot h$ and $f \cdot (g \cdot h)$ are defined, then $f \cdot g$ and $(f \cdot g) \cdot h$ are also defined, and $f \cdot (g \cdot h) = (f \cdot g) \cdot h$.*

There is similarly a *right associativity* condition.

A germ defines a monoid

$$M(S) = \langle S \mid ab = c \text{ if } a \cdot b \text{ is defined and } a \cdot b = c \rangle$$

# Germs

Intervals in a group define *germs*, where germs are sets which model subsets of a monoid.

**Definition**

A germ is a set $S$ with a partially defined multiplication $(a, b) \mapsto a \cdot b, S^2 \to S$.

Usually we require germs to be *left associative*, that is:

*If $g \cdot h$ and $f \cdot (g \cdot h)$ are defined, then $f \cdot g$ and $(f \cdot g) \cdot h$ are also defined, and $f \cdot (g \cdot h) = (f \cdot g) \cdot h$.*

There is similarly a *right associativity* condition.
A germ defines a monoid

$$M(S) = \langle S \mid ab = c \text{ if } a \cdot b \text{ is defined and } a \cdot b = c \rangle$$

## Proposition (Embedding)

*A left associative germ $S$ embeds into $M(S)$ as a subset stable under right divisors.*

### Sketch of proof.

$M(S)$ identifies with $S^*$ (the sequences $(s_1, \ldots, s_n)$ with $s_i \in S$) modulo the relations $(s_i, \ldots, s_i, s_{i+1}, s_n) \equiv (s_i, \ldots, s_i \cdot s_{i+1}, s_n)$. We define a partial map $\iota : M(S) \to S$ by $\iota((s_1, \ldots, s_n)) = s$ if $(s_1, \ldots, s_n) \equiv (s)$. Left associativity shows that $\iota$ is well defined. The composition $s \mapsto (s) \mapsto \iota((s))$ is the identity so $s \to (s)$ is injective.
Similarly left associativity shows that $\iota$ is defined for a right divisor (a final subsequence). □

We say that a germ is *left-cancellative* if $f \cdot g$ and $f \cdot g'$ defined and equal implies $g = g'$.
An balanced interval in a group is automatically a right and left associative and right and left cancellative germ.

## Proposition (Embedding)

*A left associative germ $S$ embeds into $M(S)$ as a subset stable under right divisors.*

## Sketch of proof.

$M(S)$ identifies with $S^*$ (the sequences $(s_1, \ldots, s_n)$ with $s_i \in S$) modulo the relations $(s_i, \ldots, s_i, s_{i+1}, s_n) \equiv (s_i, \ldots, s_i \cdot s_{i+1}, s_n)$. We define a partial map $\iota : M(S) \to S$ by $\iota((s_1, \ldots, s_n)) = s$ if $(s_1, \ldots, s_n) \equiv (s)$. Left associativity shows that $\iota$ is well defined. The composition $s \mapsto (s) \mapsto \iota((s))$ is the identity so $s \to (s)$ is injective.

Similarly left associativity shows that $\iota$ is defined for a right divisor (a final subsequence). □

We say that a germ is *left-cancellative* if $f \cdot g$ and $f \cdot g'$ defined and equal implies $g = g'$.

An balanced interval in a group is automatically a right and left associative and right and left cancellative germ.

## Proposition (Embedding)

*A left associative germ $S$ embeds into $M(S)$ as a subset stable under right divisors.*

## Sketch of proof.

$M(S)$ identifies with $S^*$ (the sequences $(s_1, \ldots, s_n)$ with $s_i \in S$) modulo the relations $(s_i, \ldots, s_i, s_{i+1}, s_n) \equiv (s_i, \ldots, s_i \cdot s_{i+1}, s_n)$. We define a partial map $\iota : M(S) \to S$ by $\iota((s_1, \ldots, s_n)) = s$ if $(s_1, \ldots, s_n) \equiv (s)$. Left associativity shows that $\iota$ is well defined. The composition $s \mapsto (s) \mapsto \iota((s))$ is the identity so $s \to (s)$ is injective.

Similarly left associativity shows that $\iota$ is defined for a right divisor (a final subsequence). □

We say that a germ is *left-cancellative* if $f \cdot g$ and $f \cdot g'$ defined and equal implies $g = g'$.

An balanced interval in a group is automatically a right and left associative and right and left cancellative germ.

## Proposition (Embedding)

*A left associative germ $S$ embeds into $M(S)$ as a subset stable under right divisors.*

## Sketch of proof.

$M(S)$ identifies with $S^*$ (the sequences $(s_1, \ldots, s_n)$ with $s_i \in S$) modulo the relations $(s_i, \ldots, s_i, s_{i+1}, s_n) \equiv (s_i, \ldots, s_i \cdot s_{i+1}, s_n)$. We define a partial map $\iota : M(S) \to S$ by $\iota((s_1, \ldots, s_n)) = s$ if $(s_1, \ldots, s_n) \equiv (s)$. Left associativity shows that $\iota$ is well defined. The composition $s \mapsto (s) \mapsto \iota((s))$ is the identity so $s \to (s)$ is injective.

Similarly left associativity shows that $\iota$ is defined for a right divisor (a final subsequence). □

We say that a germ is *left-cancellative* if $f \cdot g$ and $f \cdot g'$ defined and equal implies $g = g'$.

An balanced interval in a group is automatically a right and left associative and right and left cancellative germ.

## Proposition (Embedding)

*A left associative germ $S$ embeds into $M(S)$ as a subset stable under right divisors.*

## Sketch of proof.

$M(S)$ identifies with $S^*$ (the sequences $(s_1, \ldots, s_n)$ with $s_i \in S$) modulo the relations $(s_i, \ldots, s_i, s_{i+1}, s_n) \equiv (s_i, \ldots, s_i \cdot s_{i+1}, s_n)$. We define a partial map $\iota : M(S) \to S$ by $\iota((s_1, \ldots, s_n)) = s$ if $(s_1, \ldots, s_n) \equiv (s)$. Left associativity shows that $\iota$ is well defined. The composition $s \mapsto (s) \mapsto \iota((s))$ is the identity so $s \to (s)$ is injective.

Similarly left associativity shows that $\iota$ is defined for a right divisor (a final subsequence). □

We say that a germ is *left-cancellative* if $f \cdot g$ and $f \cdot g'$ defined and equal implies $g = g'$.

An balanced interval in a group is automatically a right and left associative and right and left cancellative germ.

**Proposition (Embedding)**

*A left associative germ $S$ embeds into $M(S)$ as a subset stable under right divisors.*

**Sketch of proof.**

$M(S)$ identifies with $S^*$ (the sequences $(s_1, \ldots, s_n)$ with $s_i \in S$) modulo the relations $(s_i, \ldots, s_i, s_{i+1}, s_n) \equiv (s_i, \ldots, s_i \cdot s_{i+1}, s_n)$. We define a partial map $\iota : M(S) \to S$ by $\iota((s_1, \ldots, s_n)) = s$ if $(s_1, \ldots, s_n) \equiv (s)$. Left associativity shows that $\iota$ is well defined. The composition $s \mapsto (s) \mapsto \iota((s))$ is the identity so $s \to (s)$ is injective.
Similarly left associativity shows that $\iota$ is defined for a right divisor (a final subsequence). $\square$

We say that a germ is *left-cancellative* if $f \cdot g$ and $f \cdot g'$ defined and equal implies $g = g'$.
An balanced interval in a group is automatically a right and left associative and right and left cancellative germ.

### Proposition (Embedding)

*A left associative germ $S$ embeds into $M(S)$ as a subset stable under right divisors.*

### Sketch of proof.

$M(S)$ identifies with $S^*$ (the sequences $(s_1, \ldots, s_n)$ with $s_i \in S$) modulo the relations $(s_i, \ldots, s_i, s_{i+1}, s_n) \equiv (s_i, \ldots, s_i \cdot s_{i+1}, s_n)$. We define a partial map $\iota : M(S) \to S$ by $\iota((s_1, \ldots, s_n)) = s$ if $(s_1, \ldots, s_n) \equiv (s)$. Left associativity shows that $\iota$ is well defined. The composition $s \mapsto (s) \mapsto \iota((s))$ is the identity so $s \to (s)$ is injective.
Similarly left associativity shows that $\iota$ is defined for a right divisor (a final subsequence). □

We say that a germ is *left-cancellative* if $f \cdot g$ and $f \cdot g'$ defined and equal implies $g = g'$.

An balanced interval in a group is automatically a right and left associative and right and left cancellative germ.

**Proposition (Embedding)**

*A left associative germ $S$ embeds into $M(S)$ as a subset stable under right divisors.*

**Sketch of proof.**

$M(S)$ identifies with $S^*$ (the sequences $(s_1, \ldots, s_n)$ with $s_i \in S$) modulo the relations $(s_i, \ldots, s_i, s_{i+1}, s_n) \equiv (s_i, \ldots, s_i \cdot s_{i+1}, s_n)$. We define a partial map $\iota : M(S) \to S$ by $\iota((s_1, \ldots, s_n)) = s$ if $(s_1, \ldots, s_n) \equiv (s)$. Left associativity shows that $\iota$ is well defined. The composition $s \mapsto (s) \mapsto \iota((s))$ is the identity so $s \to (s)$ is injective.
Similarly left associativity shows that $\iota$ is defined for a right divisor (a final subsequence). □

We say that a germ is *left-cancellative* if $f \cdot g$ and $f \cdot g'$ defined and equal implies $g = g'$.
An balanced interval in a group is automatically a right and left associative and right and left cancellative germ.

# When is $M(S)$ Garside?

**Proposition**

*A Garside family $S$ in a monoid $M$ defines a germ such that $M = M(S)$.*

**Proof.**

We have to prove that two elements of $M$ are equal by applying relations of the form $ab = c$, where $a, b, c$ in $S$. This is clear since one goes from any decomposition $s_1 \cdots s_n$ of an element to a normal form by a finite number of equalities $s_1 s_2 = H(s_1 s_2) T(s_1 s_2)$ which can be written themselves $H(s_1 s_2) = s_1 t$ and $s_2 = t T(s_1 s_2)$. □

In the above proof appears the functions on $S^2$ given by $(s_1, s_2) \mapsto H(s_1 s_2)$ and $(s_1, s_2) \mapsto T(s_1 s_2)$. Let us see that such functions are always defined for an interval $S$ as in Theorem 1.

# When is $M(S)$ Garside?

**Proposition**

*A Garside family $S$ in a monoid $M$ defines a germ such that $M = M(S)$.*

**Proof.**

We have to prove that two elements of $M$ are equal by applying relations of the form $ab = c$, where $a, b, c$ in $S$. This is clear since one goes from any decomposition $s_1 \cdots s_n$ of an element to a normal form by a finite number of equalities $s_1 s_2 = H(s_1 s_2) T(s_1 s_2)$ which can be written themselves $H(s_1 s_2) = s_1 t$ and $s_2 = t T(s_1 s_2)$. □

In the above proof appears the functions on $S^2$ given by $(s_1, s_2) \mapsto H(s_1 s_2)$ and $(s_1, s_2) \mapsto T(s_1 s_2)$. Let us see that such functions are always defined for an interval $S$ as in Theorem 1.

# When is $M(S)$ Garside?

**Proposition**

*A Garside family $S$ in a monoid $M$ defines a germ such that $M = M(S)$.*

**Proof.**

We have to prove that two elements of $M$ are equal by applying relations of the form $ab = c$, where $a, b, c$ in $S$. This is clear since one goes from any decomposition $s_1 \cdots s_n$ of an element to a normal form by a finite number of equalities $s_1 s_2 = H(s_1 s_2) T(s_1 s_2)$ which can be written themselves $H(s_1 s_2) = s_1 t$ and $s_2 = t T(s_1 s_2)$. □

In the above proof appears the functions on $S^2$ given by $(s_1, s_2) \mapsto H(s_1 s_2)$ and $(s_1, s_2) \mapsto T(s_1 s_2)$. Let us see that such functions are always defined for an interval $S$ as in Theorem 1.

# When is $M(S)$ Garside?

**Proposition**

*A Garside family $S$ in a monoid $M$ defines a germ such that $M = M(S)$.*

**Proof.**

We have to prove that two elements of $M$ are equal by applying relations of the form $ab = c$, where $a, b, c$ in $S$. This is clear since one goes from any decomposition $s_1 \cdots s_n$ of an element to a normal form by a finite number of equalities $s_1 s_2 = H(s_1 s_2)T(s_1 s_2)$ which can be written themselves $H(s_1 s_2) = s_1 t$ and $s_2 = tT(s_1 s_2)$. □

In the above proof appears the functions on $S^2$ given by $(s_1, s_2) \mapsto H(s_1 s_2)$ and $(s_1, s_2) \mapsto T(s_1 s_2)$. Let us see that such functions are always defined for an interval $S$ as in Theorem 1.

# When is $M(S)$ Garside?

**Proposition**

*A Garside family $S$ in a monoid $M$ defines a germ such that $M = M(S)$.*

**Proof.**

We have to prove that two elements of $M$ are equal by applying relations of the form $ab = c$, where $a, b, c$ in $S$. This is clear since one goes from any decomposition $s_1 \cdots s_n$ of an element to a normal form by a finite number of equalities $s_1 s_2 = H(s_1 s_2)T(s_1 s_2)$ which can be written themselves $H(s_1 s_2) = s_1 t$ and $s_2 = tT(s_1 s_2)$. □

In the above proof appears the functions on $S^2$ given by $(s_1, s_2) \mapsto H(s_1 s_2)$ and $(s_1, s_2) \mapsto T(s_1 s_2)$. Let us see that such functions are always defined for an interval $S$ as in Theorem 1.

## Proposition (Head)

*Let $S$ be a germ which is left-associative, left-cancellative, has right lcms and is right Noetherian (no infinite bounded chains for left divisibility). Then given $x, y \in S$, there is a unique maximal $z$ (for divisibility) which left-divides $y$ and such that $x \cdot z$ is defined.*

### Proof.

If $z_1$ and $z_2$ are two left divisors of $y$ such that $x \cdot z_1$ and $x \cdot z_2$ are defined, then these elements have a right lcm which can be written $x \cdot z_3$ (by stability under right divisors). And by left cancellability we find that $z_3$ is a lcm of $z_1$ and $z_2$ (and left-divides $y$). By right Noetherianity the sequence $z_1, \ldots, z_n$ will become stationary when considering more elements $z_i$, converging to a $z$ satisfying the requirements. □

We note that in the above proof the property needed is that if $x \cdot z_1$ and $x \cdot z_2$ are defined and $z_1, z_2$ have a common multiple then they have a right-lcm $z_3$ and $x \cdot z_3$ is defined.

**Proposition (Head)**

*Let $S$ be a germ which is left-associative, left-cancellative, has right lcms and is right Noetherian (no infinite bounded chains for left divisibility). Then given $x, y \in S$, there is a unique maximal $z$ (for divisibility) which left-divides $y$ and such that $x \cdot z$ is defined.*

Proof.

If $z_1$ and $z_2$ are two left divisors of $y$ such that $x \cdot z_1$ and $x \cdot z_2$ are defined, then these elements have a right lcm which can be written $x \cdot z_3$ (by stability under right divisors). And by left cancellability we find that $z_3$ is a lcm of $z_1$ and $z_2$ (and left-divides $y$). By right Noetherianity the sequence $z_1, \ldots, z_n$ will become stationary when considering more elements $z_i$, converging to a $z$ satisfying the requirements. □

We note that in the above proof the property needed is that if $x \cdot z_1$ and $x \cdot z_2$ are defined and $z_1, z_2$ have a common multiple then they have a right-lcm $z_3$ and $x \cdot z_3$ is defined.

## Proposition (Head)

*Let $S$ be a germ which is left-associative, left-cancellative, has right lcms and is right Noetherian (no infinite bounded chains for left divisibility). Then given $x, y \in S$, there is a unique maximal $z$ (for divisibility) which left-divides $y$ and such that $x \cdot z$ is defined.*

## Proof.

If $z_1$ and $z_2$ are two left divisors of $y$ such that $x \cdot z_1$ and $x \cdot z_2$ are defined, then these elements have a right lcm which can be written $x \cdot z_3$ (by stability under right divisors). And by left cancellability we find that $z_3$ is a lcm of $z_1$ and $z_2$ (and left-divides $y$). By right Noetherianity the sequence $z_1, \ldots, z_n$ will become stationary when considering more elements $z_i$, converging to a $z$ satisfying the requirements. □

We note that in the above proof the property needed is that if $x \cdot z_1$ and $x \cdot z_2$ are defined and $z_1, z_2$ have a common multiple then they have a right-lcm $z_3$ and $x \cdot z_3$ is defined.

## Proposition (Head)

*Let $S$ be a germ which is left-associative, left-cancellative, has right lcms and is right Noetherian (no infinite bounded chains for left divisibility). Then given $x, y \in S$, there is a unique maximal $z$ (for divisibility) which left-divides $y$ and such that $x \cdot z$ is defined.*

## Proof.

If $z_1$ and $z_2$ are two left divisors of $y$ such that $x \cdot z_1$ and $x \cdot z_2$ are defined, then these elements have a right lcm which can be written $x \cdot z_3$ (by stability under right divisors). And by left cancellability we find that $z_3$ is a lcm of $z_1$ and $z_2$ (and left-divides $y$). By right Noetherianity the sequence $z_1, \ldots, z_n$ will become stationary when considering more elements $z_i$, converging to a $z$ satisfying the requirements. □

We note that in the above proof the property needed is that if $x \cdot z_1$ and $x \cdot z_2$ are defined and $z_1, z_2$ have a common multiple then they have a right-lcm $z_3$ and $x \cdot z_3$ is defined.

## Proposition (Head)

*Let $S$ be a germ which is left-associative, left-cancellative, has right lcms and is right Noetherian (no infinite bounded chains for left divisibility). Then given $x, y \in S$, there is a unique maximal $z$ (for divisibility) which left-divides $y$ and such that $x \cdot z$ is defined.*

## Proof.

If $z_1$ and $z_2$ are two left divisors of $y$ such that $x \cdot z_1$ and $x \cdot z_2$ are defined, then these elements have a right lcm which can be written $x \cdot z_3$ (by stability under right divisors). And by left cancellability we find that $z_3$ is a lcm of $z_1$ and $z_2$ (and left-divides $y$). By right Noetherianity the sequence $z_1, \ldots, z_n$ will become stationary when considering more elements $z_i$, converging to a $z$ satisfying the requirements. □

We note that in the above proof the property needed is that if $x \cdot z_1$ and $x \cdot z_2$ are defined and $z_1, z_2$ have a common multiple then they have a right-lcm $z_3$ and $x \cdot z_3$ is defined.

## Proposition (Head)

*Let $S$ be a germ which is left-associative, left-cancellative, has right lcms and is right Noetherian (no infinite bounded chains for left divisibility). Then given $x, y \in S$, there is a unique maximal $z$ (for divisibility) which left-divides $y$ and such that $x \cdot z$ is defined.*

## Proof.

If $z_1$ and $z_2$ are two left divisors of $y$ such that $x \cdot z_1$ and $x \cdot z_2$ are defined, then these elements have a right lcm which can be written $x \cdot z_3$ (by stability under right divisors). And by left cancellability we find that $z_3$ is a lcm of $z_1$ and $z_2$ (and left-divides $y$). By right Noetherianity the sequence $z_1, \ldots, z_n$ will become stationary when considering more elements $z_i$, converging to a $z$ satisfying the requirements. □

We note that in the above proof the property needed is that if $x \cdot z_1$ and $x \cdot z_2$ are defined and $z_1, z_2$ have a common multiple then they have a right-lcm $z_3$ and $x \cdot z_3$ is defined.

We will denote $H_2(x, y)$ the element $x \cdot z$ defined in the previous proposition. We will also denote $T_2(x, y)$ the element $z' \in S$ such that $y = z \cdot z'$. In $M(S)$ we have $xy = H_2(x, y) T_2(x, y)$.

We will prove that $M(S)$ has $S$ as a Garside family by constructing a head function. But there is a technical complication: to show $M(S)$ is cancellable we will have to define simultaneously a tail function. We first show

**Proposition ($H$ and $T$)**

*Let $S$ be a germ which is left-associative, left-cancellative and has functions $H_2$ and $T_2$ as in Proposition (Head). Then there are unique functions $H : M(S) \to S$ and $T : M(S) \to M(S)$ such that for $x, y \in S$ we have $H(xy) = H_2(x, y)$ and $T(xy) = T_2(x, y)$, and which for any $a, b \in M(S)$ satisfy*

$$H(ab) = H(aH(b))$$
$$T(ab) = T(aH(b))T(b)$$

*Further, $H(x)$ is the maximal left divisor of $x$ which is in $S$.*

We will denote $H_2(x, y)$ the element $x \cdot z$ defined in the previous proposition. We will also denote $T_2(x, y)$ the element $z' \in S$ such that $y = z \cdot z'$. In $M(S)$ we have $xy = H_2(x, y) T_2(x, y)$.

We will prove that $M(S)$ has $S$ as a Garside family by constructing a head function. But there is a technical complication: to show $M(S)$ is cancellable we will have to define simultaneously a tail function. We first show

### Proposition ($H$ and $T$)

*Let $S$ be a germ which is left-associative, left-cancellative and has functions $H_2$ and $T_2$ as in Proposition (Head). Then there are unique functions $H : M(S) \to S$ and $T : M(S) \to M(S)$ such that for $x, y \in S$ we have $H(xy) = H_2(x, y)$ and $T(xy) = T_2(x, y)$, and which for any $a, b \in M(S)$ satisfy*

$$H(ab) = H(aH(b))$$
$$T(ab) = T(aH(b))T(b)$$

*Further, $H(x)$ is the maximal left divisor of $x$ which is in $S$.*

We will denote $H_2(x,y)$ the element $x \cdot z$ defined in the previous proposition. We will also denote $T_2(x,y)$ the element $z' \in S$ such that $y = z \cdot z'$. In $M(S)$ we have $xy = H_2(x,y)T_2(x,y)$.

We will prove that $M(S)$ has $S$ as a Garside family by constructing a head function. But there is a technical complication: to show $M(S)$ is cancellable we will have to define simultaneously a tail function. We first show

**Proposition ($H$ and $T$)**

*Let $S$ be a germ which is left-associative, left-cancellative and has functions $H_2$ and $T_2$ as in Proposition (Head). Then there are unique functions $H : M(S) \to S$ and $T : M(S) \to M(S)$ such that for $x, y \in S$ we have $H(xy) = H_2(x,y)$ and $T(xy) = T_2(x,y)$, and which for any $a, b \in M(S)$ satisfy*

$$H(ab) = H(aH(b))$$
$$T(ab) = T(aH(b))T(b)$$

*Further, $H(x)$ is the maximal left divisor of $x$ which is in $S$.*

We will denote $H_2(x,y)$ the element $x \cdot z$ defined in the previous proposition. We will also denote $T_2(x,y)$ the element $z' \in S$ such that $y = z \cdot z'$. In $M(S)$ we have $xy = H_2(x,y)T_2(x,y)$.
We will prove that $M(S)$ has $S$ as a Garside family by constructing a head function. But there is a technical complication: to show $M(S)$ is cancellable we will have to define simultaneously a tail function. We first show

**Proposition ($H$ and $T$)**

*Let $S$ be a germ which is left-associative, left-cancellative and has functions $H_2$ and $T_2$ as in Proposition (Head). Then there are unique functions $H : M(S) \to S$ and $T : M(S) \to M(S)$ such that for $x, y \in S$ we have $H(xy) = H_2(x,y)$ and $T(xy) = T_2(x,y)$, and which for any $a, b \in M(S)$ satisfy*

$$H(ab) = H(aH(b))$$
$$T(ab) = T(aH(b))T(b)$$

*Further, $H(x)$ is the maximal left divisor of $x$ which is in $S$.*

We will denote $H_2(x, y)$ the element $x \cdot z$ defined in the previous proposition. We will also denote $T_2(x, y)$ the element $z' \in S$ such that $y = z \cdot z'$. In $M(S)$ we have $xy = H_2(x, y)T_2(x, y)$.
We will prove that $M(S)$ has $S$ as a Garside family by constructing a head function. But there is a technical complication: to show $M(S)$ is cancellable we will have to define simultaneously a tail function. We first show

## Proposition ($H$ and $T$)

*Let $S$ be a germ which is left-associative, left-cancellative and has functions $H_2$ and $T_2$ as in Proposition (Head). Then there are unique functions $H : M(S) \to S$ and $T : M(S) \to M(S)$ such that for $x, y \in S$ we have $H(xy) = H_2(x, y)$ and $T(xy) = T_2(x, y)$, and which for any $a, b \in M(S)$ satisfy*

$$H(ab) = H(aH(b))$$
$$T(ab) = T(aH(b))T(b)$$

*Further, $H(x)$ is the maximal left divisor of $x$ which is in $S$.*

We will denote $H_2(x, y)$ the element $x \cdot z$ defined in the previous proposition. We will also denote $T_2(x, y)$ the element $z' \in S$ such that $y = z \cdot z'$. In $M(S)$ we have $xy = H_2(x, y)T_2(x, y)$.
We will prove that $M(S)$ has $S$ as a Garside family by constructing a head function. But there is a technical complication: to show $M(S)$ is cancellable we will have to define simultaneously a tail function. We first show

**Proposition ($H$ and $T$)**

*Let $S$ be a germ which is left-associative, left-cancellative and has functions $H_2$ and $T_2$ as in Proposition (Head). Then there are unique functions $H : M(S) \to S$ and $T : M(S) \to M(S)$ such that for $x, y \in S$ we have $H(xy) = H_2(x, y)$ and $T(xy) = T_2(x, y)$, and which for any $a, b \in M(S)$ satisfy*

$$H(ab) = H(aH(b))$$
$$T(ab) = T(aH(b))T(b)$$

*Further, $H(x)$ is the maximal left divisor of $x$ which is in $S$.*

We will denote $H_2(x,y)$ the element $x \cdot z$ defined in the previous proposition. We will also denote $T_2(x,y)$ the element $z' \in S$ such that $y = z \cdot z'$. In $M(S)$ we have $xy = H_2(x,y)T_2(x,y)$.
We will prove that $M(S)$ has $S$ as a Garside family by constructing a head function. But there is a technical complication: to show $M(S)$ is cancellable we will have to define simultaneously a tail function. We first show

## Proposition ($H$ and $T$)

*Let $S$ be a germ which is left-associative, left-cancellative and has functions $H_2$ and $T_2$ as in Proposition (Head). Then there are unique functions $H : M(S) \to S$ and $T : M(S) \to M(S)$ such that for $x, y \in S$ we have $H(xy) = H_2(x,y)$ and $T(xy) = T_2(x,y)$, and which for any $a, b \in M(S)$ satisfy*

$$H(ab) = H(aH(b))$$
$$T(ab) = T(aH(b))T(b)$$

*Further, $H(x)$ is the maximal left divisor of $x$ which is in $S$.*

As before, we identify elements of $M(S)$ to elements of $S^*$ modulo $\equiv$. We define $H$ and $T$ on such sequences by induction on the number of terms, by setting

- $H(()) = 1$
- $H((s)) = s$
- $H(s_1, \dots, s_n) = H_2(s_1, H((s_2, \dots, s_n))$

and

- $T(()) = T((s)) = 1$
- $T(s_1, \dots, s_n) = T_2(s_1, H((s_2, \dots, s_n)))T((s_2, \dots, s_n))$.

We have to show that these definitions are compatible with $\equiv$ and satisfy the equations of Proposition ($H$ and $T$).
We first show that $H_2$ and $T_2$ as defined on $S^2$ satisfy the equations of Proposition ($H$ and $T$)

As before, we identify elements of $M(S)$ to elements of $S^*$ modulo $\equiv$. We define $H$ and $T$ on such sequences by induction on the number of terms, by setting

- $H(()) = 1$
- $H((s)) = s$
- $H(s_1, \ldots, s_n) = H_2(s_1, H((s_2, \ldots, s_n))$

and

- $T(()) = T((s)) = 1$
- $T(s_1, \ldots, s_n) = T_2(s_1, H((s_2, \ldots, s_n)))\, T((s_2, \ldots, s_n))$.

We have to show that these definitions are compatible with $\equiv$ and satisfy the equations of Proposition ($H$ and $T$).
We first show that $H_2$ and $T_2$ as defined on $S^2$ satisfy the equations of Proposition ($H$ and $T$)

As before, we identify elements of $M(S)$ to elements of $S^*$ modulo $\equiv$. We define $H$ and $T$ on such sequences by induction on the number of terms, by setting

- $H(()) = 1$
- $H((s)) = s$
- $H(s_1, \ldots, s_n) = H_2(s_1, H((s_2, \ldots, s_n)))$

and

- $T(()) = T((s)) = 1$
- $T(s_1, \ldots, s_n) = T_2(s_1, H((s_2, \ldots, s_n)))T((s_2, \ldots, s_n))$.

We have to show that these definitions are compatible with $\equiv$ and satisfy the equations of Proposition ($H$ and $T$).
We first show that $H_2$ and $T_2$ as defined on $S^2$ satisfy the equations of Proposition ($H$ and $T$)

As before, we identify elements of $M(S)$ to elements of $S^*$ modulo $\equiv$. We define $H$ and $T$ on such sequences by induction on the number of terms, by setting

- $H(()) = 1$
- $H((s)) = s$
- $H(s_1, \ldots, s_n) = H_2(s_1, H((s_2, \ldots, s_n))$

and

- $T(()) = T((s)) = 1$
- $T(s_1, \ldots, s_n) = T_2(s_1, H((s_2, \ldots, s_n)))T((s_2, \ldots, s_n))$.

We have to show that these definitions are compatible with $\equiv$ and satisfy the equations of Proposition ($H$ and $T$).

We first show that $H_2$ and $T_2$ as defined on $S^2$ satisfy the equations of Proposition ($H$ and $T$)

As before, we identify elements of $M(S)$ to elements of $S^*$ modulo $\equiv$. We define $H$ and $T$ on such sequences by induction on the number of terms, by setting

- $H(()) = 1$
- $H((s)) = s$
- $H(s_1, \ldots, s_n) = H_2(s_1, H((s_2, \ldots, s_n))$

and

- $T(()) = T((s)) = 1$
- $T(s_1, \ldots, s_n) = T_2(s_1, H((s_2, \ldots, s_n)))T((s_2, \ldots, s_n))$.

We have to show that these definitions are compatible with $\equiv$ and satisfy the equations of Proposition ($H$ and $T$).

We first show that $H_2$ and $T_2$ as defined on $S^2$ satisfy the equations of Proposition ($H$ and $T$)

As before, we identify elements of $M(S)$ to elements of $S^*$ modulo $\equiv$. We define $H$ and $T$ on such sequences by induction on the number of terms, by setting

- $H(()) = 1$
- $H((s)) = s$
- $H(s_1, \ldots, s_n) = H_2(s_1, H((s_2, \ldots, s_n))$

and

- $T(()) = T((s)) = 1$
- $T(s_1, \ldots, s_n) = T_2(s_1, H((s_2, \ldots, s_n)))T((s_2, \ldots, s_n))$.

We have to show that these definitions are compatible with $\equiv$ and satisfy the equations of Proposition ($H$ and $T$).
We first show that $H_2$ and $T_2$ as defined on $S^2$ satisfy the equations of Proposition ($H$ and $T$)

## Lemma (Equations for $H_2$ and $T_2$)

1. $H_2(x \cdot y, z) = H_2(x, H_2(y, z))$
2. $T_2(x \cdot y, z) = T_2(x, H_2(y, z))\, T_2(y, z)$

### Proof.

Define $u$ by $H_2(x \cdot y, z) = x \cdot y \cdot u$ and $v$ by $H_2(y, z) = y \cdot v$. By definition of $H_2(y, z)$ we have $y \cdot u \preccurlyeq H_2(y, z)$ where $\preccurlyeq$ is the divisibility relation in $S$. As $x \cdot y \cdot u$ is defined, this in turn implies $x \cdot y \cdot u \preccurlyeq H_2(x, H_2(y, z))$. Define $w$ by $x \cdot y \cdot u \cdot w = H_2(x, H_2(y, z))$. It follows that $u \cdot w \preccurlyeq v \preccurlyeq z$ and the maximality of $u$ shows that $w = 1$ which shows (i).
We show now (ii). By definition of $T_2$, since $H_2(x, H_2(y, z)) = x \cdot y \cdot u$, we have $y \cdot u \cdot T_2(x, H_2(y, z)) = H_2(y, z) = y \cdot v$, whence $u \cdot T_2(x, H_2(y, z)) = v$. Similarly, since $H_2(y, z) = y \cdot v$ we have $v \cdot T_2(y, z) = z$. Thus $u \cdot T_2(x, H_2(y, z)) \cdot T_2(y, z) = z$. But since $H_2(x \cdot y, z) = x \cdot y \cdot u$ we have $u \cdot T_2(x \cdot y, z) = z$ whence the result simplifying by $u$. □

Lemma (Equations for $H_2$ and $T_2$)

1. $H_2(x \cdot y, z) = H_2(x, H_2(y, z))$
2. $T_2(x \cdot y, z) = T_2(x, H_2(y, z))\, T_2(y, z)$

Proof.

Define $u$ by $H_2(x \cdot y, z) = x \cdot y \cdot u$ and $v$ by $H_2(y, z) = y \cdot v$. By definition of $H_2(y, z)$ we have $y \cdot u \preccurlyeq H_2(y, z)$ where $\preccurlyeq$ is the divisibility relation in $S$. As $x \cdot y \cdot u$ is defined, this in turn implies $x \cdot y \cdot u \preccurlyeq H_2(x, H_2(y, z))$. Define $w$ by $x \cdot y \cdot u \cdot w = H_2(x, H_2(y, z))$. It follows that $u \cdot w \preccurlyeq v \preccurlyeq z$ and the maximality of $u$ shows that $w = 1$ which shows (i).
We show now (ii). By definition of $T_2$, since $H_2(x, H_2(y, z)) = x \cdot y \cdot u$, we have $y \cdot u \cdot T_2(x, H_2(y, z)) = H_2(y, z) = y \cdot v$, whence $u \cdot T_2(x, H_2(y, z)) = v$. Similarly, since $H_2(y, z) = y \cdot v$ we have $v \cdot T_2(y, z) = z$. Thus $u \cdot T_2(x, H_2(y, z)) \cdot T_2(y, z) = z$. But since $H_2(x \cdot y, z) = x \cdot y \cdot u$ we have $u \cdot T_2(x \cdot y, z) = z$ whence the result simplifying by $u$. □

**Lemma (Equations for $H_2$ and $T_2$)**

1. $H_2(x \cdot y, z) = H_2(x, H_2(y, z))$
2. $T_2(x \cdot y, z) = T_2(x, H_2(y, z))\, T_2(y, z)$

**Proof.**

Define $u$ by $H_2(x \cdot y, z) = x \cdot y \cdot u$ and $v$ by $H_2(y, z) = y \cdot v$. By definition of $H_2(y, z)$ we have $y \cdot u \preccurlyeq H_2(y, z)$ where $\preccurlyeq$ is the divisibility relation in $S$. As $x \cdot y \cdot u$ is defined, this in turn implies $x \cdot y \cdot u \preccurlyeq H_2(x, H_2(y, z))$. Define $w$ by $x \cdot y \cdot u \cdot w = H_2(x, H_2(y, z))$. It follows that $u \cdot w \preccurlyeq v \preccurlyeq z$ and the maximality of $u$ shows that $w = 1$ which shows (i).

We show now (ii). By definition of $T_2$, since $H_2(x, H_2(y, z)) = x \cdot y \cdot u$, we have $y \cdot u \cdot T_2(x, H_2(y, z)) = H_2(y, z) = y \cdot v$, whence $u \cdot T_2(x, H_2(y, z)) = v$. Similarly, since $H_2(y, z) = y \cdot v$ we have $v \cdot T_2(y, z) = z$. Thus $u \cdot T_2(x, H_2(y, z)) \cdot T_2(y, z) = z$. But since $H_2(x \cdot y, z) = x \cdot y \cdot u$ we have $u \cdot T_2(x \cdot y, z) = z$ whence the result simplifying by $u$. □

## Lemma (Equations for $H_2$ and $T_2$)

1. $H_2(x \cdot y, z) = H_2(x, H_2(y, z))$
2. $T_2(x \cdot y, z) = T_2(x, H_2(y, z))\, T_2(y, z)$

## Proof.

Define $u$ by $H_2(x \cdot y, z) = x \cdot y \cdot u$ and $v$ by $H_2(y, z) = y \cdot v$. By definition of $H_2(y, z)$ we have $y \cdot u \preccurlyeq H_2(y, z)$ where $\preccurlyeq$ is the divisibility relation in $S$. As $x \cdot y \cdot u$ is defined, this in turn implies $x \cdot y \cdot u \preccurlyeq H_2(x, H_2(y, z))$. Define $w$ by $x \cdot y \cdot u \cdot w = H_2(x, H_2(y, z))$. It follows that $u \cdot w \preccurlyeq v \preccurlyeq z$ and the maximality of $u$ shows that $w = 1$ which shows (i).

We show now (ii). By definition of $T_2$, since $H_2(x, H_2(y, z)) = x \cdot y \cdot u$, we have $y \cdot u \cdot T_2(x, H_2(y, z)) = H_2(y, z) = y \cdot v$, whence $u \cdot T_2(x, H_2(y, z)) = v$. Similarly, since $H_2(y, z) = y \cdot v$ we have $v \cdot T_2(y, z) = z$. Thus $u \cdot T_2(x, H_2(y, z)) \cdot T_2(y, z) = z$. But since $H_2(x \cdot y, z) = x \cdot y \cdot u$ we have $u \cdot T_2(x \cdot y, z) = z$ whence the result simplifying by $u$. $\square$

### Lemma (Equations for $H_2$ and $T_2$)

1. $H_2(x \cdot y, z) = H_2(x, H_2(y, z))$
2. $T_2(x \cdot y, z) = T_2(x, H_2(y, z))\, T_2(y, z)$

### Proof.

Define $u$ by $H_2(x \cdot y, z) = x \cdot y \cdot u$ and $v$ by $H_2(y, z) = y \cdot v$. By definition of $H_2(y, z)$ we have $y \cdot u \preccurlyeq H_2(y, z)$ where $\preccurlyeq$ is the divisibility relation in $S$. As $x \cdot y \cdot u$ is defined, this in turn implies $x \cdot y \cdot u \preccurlyeq H_2(x, H_2(y, z))$. Define $w$ by $x \cdot y \cdot u \cdot w = H_2(x, H_2(y, z))$. It follows that $u \cdot w \preccurlyeq v \preccurlyeq z$ and the maximality of $u$ shows that $w = 1$ which shows (i).
We show now (ii). By definition of $T_2$, since $H_2(x, H_2(y, z)) = x \cdot y \cdot u$, we have $y \cdot u \cdot T_2(x, H_2(y, z)) = H_2(y, z) = y \cdot v$, whence $u \cdot T_2(x, H_2(y, z)) = v$. Similarly, since $H_2(y, z) = y \cdot v$ we have $v \cdot T_2(y, z) = z$. Thus $u \cdot T_2(x, H_2(y, z)) \cdot T_2(y, z) = z$. But since $H_2(x \cdot y, z) = x \cdot y \cdot u$ we have $u \cdot T_2(x \cdot y, z) = z$ whence the result simplifying by $u$. □

## Lemma (Equations for $H_2$ and $T_2$)

1. $H_2(x \cdot y, z) = H_2(x, H_2(y, z))$
2. $T_2(x \cdot y, z) = T_2(x, H_2(y, z))\, T_2(y, z)$

## Proof.

Define $u$ by $H_2(x \cdot y, z) = x \cdot y \cdot u$ and $v$ by $H_2(y, z) = y \cdot v$. By definition of $H_2(y, z)$ we have $y \cdot u \preccurlyeq H_2(y, z)$ where $\preccurlyeq$ is the divisibility relation in $S$. As $x \cdot y \cdot u$ is defined, this in turn implies $x \cdot y \cdot u \preccurlyeq H_2(x, H_2(y, z))$. Define $w$ by $x \cdot y \cdot u \cdot w = H_2(x, H_2(y, z))$. It follows that $u \cdot w \preccurlyeq v \preccurlyeq z$ and the maximality of $u$ shows that $w = 1$ which shows (i).

We show now (ii). By definition of $T_2$, since $H_2(x, H_2(y, z)) = x \cdot y \cdot u$, we have $y \cdot u \cdot T_2(x, H_2(y, z)) = H_2(y, z) = y \cdot v$, whence $u \cdot T_2(x, H_2(y, z)) = v$. Similarly, since $H_2(y, z) = y \cdot v$ we have $v \cdot T_2(y, z) = z$. Thus $u \cdot T_2(x, H_2(y, z)) \cdot T_2(y, z) = z$. But since $H_2(x \cdot y, z) = x \cdot y \cdot u$ we have $u \cdot T_2(x \cdot y, z) = z$ whence the result simplifying by $u$. □

## Lemma (Equations for $H_2$ and $T_2$)

1. $H_2(x \cdot y, z) = H_2(x, H_2(y, z))$
2. $T_2(x \cdot y, z) = T_2(x, H_2(y, z))\, T_2(y, z)$

## Proof.

Define $u$ by $H_2(x \cdot y, z) = x \cdot y \cdot u$ and $v$ by $H_2(y, z) = y \cdot v$. By definition of $H_2(y, z)$ we have $y \cdot u \preccurlyeq H_2(y, z)$ where $\preccurlyeq$ is the divisibility relation in $S$. As $x \cdot y \cdot u$ is defined, this in turn implies $x \cdot y \cdot u \preccurlyeq H_2(x, H_2(y, z))$. Define $w$ by $x \cdot y \cdot u \cdot w = H_2(x, H_2(y, z))$. It follows that $u \cdot w \preccurlyeq v \preccurlyeq z$ and the maximality of $u$ shows that $w = 1$ which shows (i).

We show now (ii). By definition of $T_2$, since $H_2(x, H_2(y, z)) = x \cdot y \cdot u$, we have $y \cdot u \cdot T_2(x, H_2(y, z)) = H_2(y, z) = y \cdot v$, whence $u \cdot T_2(x, H_2(y, z)) = v$. Similarly, since $H_2(y, z) = y \cdot v$ we have $v \cdot T_2(y, z) = z$. Thus $u \cdot T_2(x, H_2(y, z)) \cdot T_2(y, z) = z$. But since $H_2(x \cdot y, z) = x \cdot y \cdot u$ we have $u \cdot T_2(x \cdot y, z) = z$ whence the result simplifying by $u$. □

Lemma (Equations for $H_2$ and $T_2$)

1. $H_2(x \cdot y, z) = H_2(x, H_2(y, z))$
2. $T_2(x \cdot y, z) = T_2(x, H_2(y, z))\, T_2(y, z)$

Proof.

Define $u$ by $H_2(x \cdot y, z) = x \cdot y \cdot u$ and $v$ by $H_2(y, z) = y \cdot v$. By definition of $H_2(y, z)$ we have $y \cdot u \preccurlyeq H_2(y, z)$ where $\preccurlyeq$ is the divisibility relation in $S$. As $x \cdot y \cdot u$ is defined, this in turn implies $x \cdot y \cdot u \preccurlyeq H_2(x, H_2(y, z))$. Define $w$ by $x \cdot y \cdot u \cdot w = H_2(x, H_2(y, z))$. It follows that $u \cdot w \preccurlyeq v \preccurlyeq z$ and the maximality of $u$ shows that $w = 1$ which shows (i).
We show now (ii). By definition of $T_2$, since $H_2(x, H_2(y, z)) = x \cdot y \cdot u$, we have $y \cdot u \cdot T_2(x, H_2(y, z)) = H_2(y, z) = y \cdot v$, whence $u \cdot T_2(x, H_2(y, z)) = v$. Similarly, since $H_2(y, z) = y \cdot v$ we have $v \cdot T_2(y, z) = z$. Thus $u \cdot T_2(x, H_2(y, z)) \cdot T_2(y, z) = z$. But since $H_2(x \cdot y, z) = x \cdot y \cdot u$ we have $u \cdot T_2(x \cdot y, z) = z$ whence the result simplifying by $u$. □

**Lemma (Equations for $H_2$ and $T_2$)**

1. $H_2(x \cdot y, z) = H_2(x, H_2(y, z))$
2. $T_2(x \cdot y, z) = T_2(x, H_2(y, z))\, T_2(y, z)$

**Proof.**

Define $u$ by $H_2(x \cdot y, z) = x \cdot y \cdot u$ and $v$ by $H_2(y, z) = y \cdot v$. By definition of $H_2(y, z)$ we have $y \cdot u \preccurlyeq H_2(y, z)$ where $\preccurlyeq$ is the divisibility relation in $S$. As $x \cdot y \cdot u$ is defined, this in turn implies $x \cdot y \cdot u \preccurlyeq H_2(x, H_2(y, z))$. Define $w$ by $x \cdot y \cdot u \cdot w = H_2(x, H_2(y, z))$. It follows that $u \cdot w \preccurlyeq v \preccurlyeq z$ and the maximality of $u$ shows that $w = 1$ which shows (i).

We show now (ii). By definition of $T_2$, since $H_2(x, H_2(y, z)) = x \cdot y \cdot u$, we have $y \cdot u \cdot T_2(x, H_2(y, z)) = H_2(y, z) = y \cdot v$, whence $u \cdot T_2(x, H_2(y, z)) = v$. Similarly, since $H_2(y, z) = y \cdot v$ we have $v \cdot T_2(y, z) = z$. Thus $u \cdot T_2(x, H_2(y, z)) \cdot T_2(y, z) = z$. But since $H_2(x \cdot y, z) = x \cdot y \cdot u$ we have $u \cdot T_2(x \cdot y, z) = z$ whence the result simplifying by $u$. □

# Compatibility with $\equiv$

To check that the definition of $H$ is compatible with $\equiv$, by induction it is enough to check what happens when $s_1$ is a product, that is to check that $H_2(s_1 \cdot s_1', H((s_2, \ldots s_n))) = H_2(s_1, H_2(s_1', H((s_2, \ldots, s_n))))$ which is (i) of Lemma (Equations for $H_2$ and $T_2$).

We show that $H$ is a $S$-head ($H(x)$ is the maximal left divisor in $S$ of $x$): if $s$ is a divisor in $S$ of $x$, then $x$ may be represented by a sequence $(s, \ldots)$ and the definition shows that $s$ left-divides $H(x)$. Finally it is easy by induction on the length of a sequence for $x$ that $H(xy) = H(xH(y))$.

Similarly to check that the definition of $T$ is compatible with $\equiv$ boils to $T_2(s_1 \cdot s_1', H((s_2, \ldots, s_n))) = T_2(s_1, H_2(s_1', H((s_2, \ldots, s_n))))T_2(s_1', H((s_2, \ldots, s_n)))$ which is (ii) of Lemma (Equations for $H_2$ and $T_2$), and similarly induction on the length of a sequence shows the equation for $T$.

# Compatibility with $\equiv$

To check that the definition of $H$ is compatible with $\equiv$, by induction it is enough to check what happens when $s_1$ is a product, that is to check that $H_2(s_1 \cdot s_1', H((s_2, \ldots s_n))) = H_2(s_1, H_2(s_1', H((s_2, \ldots, s_n))))$ which is (i) of Lemma (Equations for $H_2$ and $T_2$).

We show that $H$ is a $S$-head ($H(x)$ is the maximal left divisor in $S$ of $x$): if $s$ is a divisor in $S$ of $x$, then $x$ may be represented by a sequence $(s, \ldots)$ and the definition shows that $s$ left-divides $H(x)$. Finally it is easy by induction on the length of a sequence for $x$ that $H(xy) = H(xH(y))$.

Similarly to check that the definition of $T$ is compatible with $\equiv$ boils to $T_2(s_1 \cdot s_1', H((s_2, \ldots, s_n))) = T_2(s_1, H_2(s_1', H((s_2, \ldots, s_n))))T_2(s_1', H((s_2, \ldots, s_n)))$ which is (ii) of Lemma (Equations for $H_2$ and $T_2$), and similarly induction on the length of a sequence shows the equation for $T$.

# Compatibility with $\equiv$

To check that the definition of $H$ is compatible with $\equiv$, by induction it is enough to check what happens when $s_1$ is a product, that is to check that $H_2(s_1 \cdot s_1', H((s_2, \ldots s_n))) = H_2(s_1, H_2(s_1', H((s_2, \ldots, s_n))))$ which is (i) of Lemma (Equations for $H_2$ and $T_2$).
We show that $H$ is a $S$-head ($H(x)$ is the maximal left divisor in $S$ of $x$): if $s$ is a divisor in $S$ of $x$, then $x$ may be represented by a sequence $(s, \ldots)$ and the definition shows that $s$ left-divides $H(x)$.
Finally it is easy by induction on the length of a sequence for $x$ that $H(xy) = H(xH(y))$.
Similarly to check that the definition of $T$ is compatible with $\equiv$ boils to $T_2(s_1 \cdot s_1', H((s_2, \ldots, s_n))) = T_2(s_1, H_2(s_1', H((s_2, \ldots, s_n))))T_2(s_1', H((s_2, \ldots, s_n)))$ which is (ii) of Lemma (Equations for $H_2$ and $T_2$), and similarly induction on the length of a sequence shows the equation for $T$.

# Compatibility with $\equiv$

To check that the definition of $H$ is compatible with $\equiv$, by induction it is enough to check what happens when $s_1$ is a product, that is to check that
$H_2(s_1 \cdot s_1', H((s_2, \ldots s_n))) = H_2(s_1, H_2(s_1', H((s_2, \ldots, s_n))))$ which is (i) of Lemma (Equations for $H_2$ and $T_2$).
We show that $H$ is a $S$-head ($H(x)$ is the maximal left divisor in $S$ of $x$): if $s$ is a divisor in $S$ of $x$, then $x$ may be represented by a sequence $(s, \ldots)$ and the definition shows that $s$ left-divides $H(x)$.
Finally it is easy by induction on the length of a sequence for $x$ that $H(xy) = H(xH(y))$.
Similarly to check that the definition of $T$ is compatible with $\equiv$ boils to $T_2(s_1 \cdot s_1', H((s_2, \ldots, s_n))) =$
$T_2(s_1, H_2(s_1', H((s_2, \ldots, s_n))))T_2(s_1', H((s_2, \ldots, s_n)))$ which is (ii) of Lemma (Equations for $H_2$ and $T_2$), and similarly induction on the length of a sequence shows the equation for $T$.

# Compatibility with $\equiv$

To check that the definition of $H$ is compatible with $\equiv$, by induction it is enough to check what happens when $s_1$ is a product, that is to check that $H_2(s_1 \cdot s_1', H((s_2, \dots s_n))) = H_2(s_1, H_2(s_1', H((s_2, \dots, s_n))))$ which is (i) of Lemma (Equations for $H_2$ and $T_2$).
We show that $H$ is a $S$-head ($H(x)$ is the maximal left divisor in $S$ of $x$): if $s$ is a divisor in $S$ of $x$, then $x$ may be represented by a sequence $(s, \dots)$ and the definition shows that $s$ left-divides $H(x)$.
Finally it is easy by induction on the length of a sequence for $x$ that $H(xy) = H(xH(y))$.
Similarly to check that the definition of $T$ is compatible with $\equiv$ boils to $T_2(s_1 \cdot s_1', H((s_2, \dots, s_n))) = T_2(s_1, H_2(s_1', H((s_2, \dots, s_n))))T_2(s_1', H((s_2, \dots, s_n)))$ which is (ii) of Lemma (Equations for $H_2$ and $T_2$), and similarly induction on the length of a sequence shows the equation for $T$.

# Cancellability

We now show how Proposition ($H$ and $T$) implies that $M(S)$ is left-cancellative. It shows first that for $x \in M(S)$ any $y$ such that $x = H(x)y$ is the unique element $T(x)$. We show this by induction on the number of terms of $x \in S^*$. We have $T(x) = T(H(x)y) = T(H(x)H(y))T(y) = T_2(H(x), H(y))T(y) = H(y)T(y)$, the last equality since $H(x) = H(H(x)H(y)) = H_2(H(x), H(y))$, and by induction $H(y)T(y) = y$.

This implies general cancellability: we want to show that an equality $ab = ac$ in $M(S)$ implies $b = c$. Since $a$ is a product of elements of $S$ it is enough to consider the case whare $a \in S$. Let $x = ab = ac$. We have $H(x) = H(ab) = H(aH(b)) = H_2(a, H(b))$ $= a \cdot b_1$ where $b_1$ divides $b$ thus $b = b_1 b_2$ and $x = (a \cdot b_1)b_2$ where $H(x) = a \cdot b_1$ and thus $T(x) = b_2$. We can write similarly $x = (a \cdot c_1)c_2$. By cancellability in $S$ we get $b_1 = c_1$ and $b_2 = c_2 = T(x)$ thus $b = b_1 b_2 = c_1 c_2 = c$.

$H$ is a $S$-head ($H(x)$ is a maximal divisor of $x$ in $S$), $S$ generates $M(S)$ and is stable by right divisor: $S$ is a Garside family in $M(S)$.

# Cancellability

We now show how Proposition ($H$ and $T$) implies that $M(S)$ is left-cancellative. It shows first that for $x \in M(S)$ any $y$ such that $x = H(x)y$ is the unique element $T(x)$. We show this by induction on the number of terms of $x \in S^*$. We have $T(x) = T(H(x)y) = T(H(x)H(y))T(y) = T_2(H(x), H(y))T(y) = H(y)T(y)$, the last equality since $H(x) = H(H(x)H(y)) = H_2(H(x), H(y))$, and by induction $H(y)T(y) = y$.

This implies general cancellability: we want to show that an equality $ab = ac$ in $M(S)$ implies $b = c$. Since $a$ is a product of elements of $S$ it is enough to consider the case whare $a \in S$. Let $x = ab = ac$. We have $H(x) = H(ab) = H(aH(b)) = H_2(a, H(b))$ $= a \cdot b_1$ where $b_1$ divides $b$ thus $b = b_1 b_2$ and $x = (a \cdot b_1)b_2$ where $H(x) = a \cdot b_1$ and thus $T(x) = b_2$. We can write similarly $x = (a \cdot c_1)c_2$. By cancellability in $S$ we get $b_1 = c_1$ and $b_2 = c_2 = T(x)$ thus $b = b_1 b_2 = c_1 c_2 = c$.

$H$ is a $S$-head ($H(x)$ is a maximal divisor of $x$ in $S$), $S$ generates $M(S)$ and is stable by right divisor: $S$ is a Garside family in $M(S)$.

# Cancellability

We now show how Proposition ($H$ and $T$) implies that $M(S)$ is left-cancellative. It shows first that for $x \in M(S)$ any $y$ such that $x = H(x)y$ is the unique element $T(x)$. We show this by induction on the number of terms of $x \in S^*$. We have $T(x) = T(H(x)y) = T(H(x)H(y))T(y) = T_2(H(x), H(y))T(y) = H(y)T(y)$, the last equality since $H(x) = H(H(x)H(y)) = H_2(H(x), H(y))$, and by induction $H(y)T(y) = y$.

This implies general cancellability: we want to show that an equality $ab = ac$ in $M(S)$ implies $b = c$. Since $a$ is a product of elements of $S$ it is enough to consider the case whare $a \in S$. Let $x = ab = ac$. We have $H(x) = H(ab) = H(aH(b)) = H_2(a, H(b)) = a \cdot b_1$ where $b_1$ divides $b$ thus $b = b_1 b_2$ and $x = (a \cdot b_1)b_2$ where $H(x) = a \cdot b_1$ and thus $T(x) = b_2$. We can write similarly $x = (a \cdot c_1)c_2$. By cancellability in $S$ we get $b_1 = c_1$ and $b_2 = c_2 = T(x)$ thus $b = b_1 b_2 = c_1 c_2 = c$.

$H$ is a $S$-head ($H(x)$ is a maximal divisor of $x$ in $S$), $S$ generates $M(S)$ and is stable by right divisor: $S$ is a Garside family in $M(S)$.

# Cancellability

We now show how Proposition ($H$ and $T$) implies that $M(S)$ is left-cancellative. It shows first that for $x \in M(S)$ any $y$ such that $x = H(x)y$ is the unique element $T(x)$. We show this by induction on the number of terms of $x \in S^*$. We have $T(x) = T(H(x)y) = T(H(x)H(y))T(y) = T_2(H(x), H(y))T(y) = H(y)T(y)$, the last equality since $H(x) = H(H(x)H(y)) = H_2(H(x), H(y))$, and by induction $H(y)T(y) = y$.

This implies general cancellability: we want to show that an equality $ab = ac$ in $M(S)$ implies $b = c$. Since $a$ is a product of elements of $S$ it is enough to consider the case whare $a \in S$. Let $x = ab = ac$. We have $H(x) = H(ab) = H(aH(b)) = H_2(a, H(b))$ $= a \cdot b_1$ where $b_1$ divides $b$ thus $b = b_1 b_2$ and $x = (a \cdot b_1)b_2$ where $H(x) = a \cdot b_1$ and thus $T(x) = b_2$. We can write similarly $x = (a \cdot c_1)c_2$. By cancellability in $S$ we get $b_1 = c_1$ and $b_2 = c_2 = T(x)$ thus $b = b_1 b_2 = c_1 c_2 = c$.

$H$ is a $S$-head ($H(x)$ is a maximal divisor of $x$ in $S$), $S$ generates $M(S)$ and is stable by right divisor: $S$ is a Garside family in $M(S)$.

# Cancellability

We now show how Proposition ($H$ and $T$) implies that $M(S)$ is left-cancellative. It shows first that for $x \in M(S)$ any $y$ such that $x = H(x)y$ is the unique element $T(x)$. We show this by induction on the number of terms of $x \in S^*$. We have $T(x) = T(H(x)y) = T(H(x)H(y))T(y) = T_2(H(x), H(y))T(y) = H(y)T(y)$, the last equality since $H(x) = H(H(x)H(y)) = H_2(H(x), H(y))$, and by induction $H(y)T(y) = y$.

This implies general cancellability: we want to show that an equality $ab = ac$ in $M(S)$ implies $b = c$. Since $a$ is a product of elements of $S$ it is enough to consider the case whare $a \in S$. Let $x = ab = ac$. We have $H(x) = H(ab) = H(aH(b)) = H_2(a, H(b))$ $= a \cdot b_1$ where $b_1$ divides $b$ thus $b = b_1 b_2$ and $x = (a \cdot b_1)b_2$ where $H(x) = a \cdot b_1$ and thus $T(x) = b_2$. We can write similarly $x = (a \cdot c_1)c_2$. By cancellability in $S$ we get $b_1 = c_1$ and $b_2 = c_2 = T(x)$ thus $b = b_1 b_2 = c_1 c_2 = c$.

$H$ is a $S$-head ($H(x)$ is a maximal divisor of $x$ in $S$), $S$ generates $M(S)$ and is stable by right divisor: $S$ is a Garside family in $M(S)$.

# Cancellability

We now show how Proposition ($H$ and $T$) implies that $M(S)$ is left-cancellative. It shows first that for $x \in M(S)$ any $y$ such that $x = H(x)y$ is the unique element $T(x)$. We show this by induction on the number of terms of $x \in S^*$. We have $T(x) = T(H(x)y) = T(H(x)H(y))T(y) = T_2(H(x), H(y))T(y) = H(y)T(y)$, the last equality since $H(x) = H(H(x)H(y)) = H_2(H(x), H(y))$, and by induction $H(y)T(y) = y$.

This implies general cancellability: we want to show that an equality $ab = ac$ in $M(S)$ implies $b = c$. Since $a$ is a product of elements of $S$ it is enough to consider the case whare $a \in S$. Let $x = ab = ac$. We have $H(x) = H(ab) = H(aH(b)) = H_2(a, H(b))$ $= a \cdot b_1$ where $b_1$ divides $b$ thus $b = b_1 b_2$ and $x = (a \cdot b_1)b_2$ where $H(x) = a \cdot b_1$ and thus $T(x) = b_2$. We can write similarly $x = (a \cdot c_1)c_2$. By cancellability in $S$ we get $b_1 = c_1$ and $b_2 = c_2 = T(x)$ thus $b = b_1 b_2 = c_1 c_2 = c$.

$H$ is a $S$-head ($H(x)$ is a maximal divisor of $x$ in $S$), $S$ generates $M(S)$ and is stable by right divisor: $S$ is a Garside family in $M(S)$.

# Cancellability

We now show how Proposition ($H$ and $T$) implies that $M(S)$ is left-cancellative. It shows first that for $x \in M(S)$ any $y$ such that $x = H(x)y$ is the unique element $T(x)$. We show this by induction on the number of terms of $x \in S^*$. We have $T(x) = T(H(x)y) = T(H(x)H(y))T(y) = T_2(H(x), H(y))T(y) = H(y)T(y)$, the last equality since $H(x) = H(H(x)H(y)) = H_2(H(x), H(y))$, and by induction $H(y)T(y) = y$.

This implies general cancellability: we want to show that an equality $ab = ac$ in $M(S)$ implies $b = c$. Since $a$ is a product of elements of $S$ it is enough to consider the case whare $a \in S$. Let $x = ab = ac$. We have $H(x) = H(ab) = H(aH(b)) = H_2(a, H(b)) = a \cdot b_1$ where $b_1$ divides $b$ thus $b = b_1 b_2$ and $x = (a \cdot b_1)b_2$ where $H(x) = a \cdot b_1$ and thus $T(x) = b_2$. We can write similarly $x = (a \cdot c_1)c_2$. By cancellability in $S$ we get $b_1 = c_1$ and $b_2 = c_2 = T(x)$ thus $b = b_1 b_2 = c_1 c_2 = c$.

$H$ is a $S$-head ($H(x)$ is a maximal divisor of $x$ in $S$), $S$ generates $M(S)$ and is stable by right divisor: $S$ is a Garside family in $M(S)$.

# Cancellability

We now show how Proposition ($H$ and $T$) implies that $M(S)$ is left-cancellative. It shows first that for $x \in M(S)$ any $y$ such that $x = H(x)y$ is the unique element $T(x)$. We show this by induction on the number of terms of $x \in S^*$. We have $T(x) = T(H(x)y) = T(H(x)H(y))T(y) = T_2(H(x), H(y))T(y) = H(y)T(y)$, the last equality since $H(x) = H(H(x)H(y)) = H_2(H(x), H(y))$, and by induction $H(y)T(y) = y$.

This implies general cancellability: we want to show that an equality $ab = ac$ in $M(S)$ implies $b = c$. Since $a$ is a product of elements of $S$ it is enough to consider the case whare $a \in S$. Let $x = ab = ac$. We have $H(x) = H(ab) = H(aH(b)) = H_2(a, H(b))$ $= a \cdot b_1$ where $b_1$ divides $b$ thus $b = b_1 b_2$ and $x = (a \cdot b_1)b_2$ where $H(x) = a \cdot b_1$ and thus $T(x) = b_2$. We can write similarly $x = (a \cdot c_1)c_2$. By cancellability in $S$ we get $b_1 = c_1$ and $b_2 = c_2 = T(x)$ thus $b = b_1 b_2 = c_1 c_2 = c$.

$H$ is a $S$-head ($H(x)$ is a maximal divisor of $x$ in $S$), $S$ generates $M(S)$ and is stable by right divisor: $S$ is a Garside family in $M(S)$.

## Proposition (check common multiple on generators)

*In a group $W$ generated positively by $R$, let $S$ be an interval stable under left and right divisors and assume any $r, r' \in R$ which have a common multiple have a least common multiple. Then any $s, s'$ in $S$ which have a common multiple have a least common multiple.*

## Proof.

The proof is by induction on $l_R(s) + l_R(s')$. If $l_R(s) = l_R(s') = 1$ we are at the start of the induction. Otherwise one of them, say $s$ is a product $s = s_1 s_2$. Assume $s, s'$ have a common multiple $sh$. Then $sh$ is a common multiple of $s_1$ and $s'$ so by induction they have a least common multiple $s_1 h_1$. Now $h_1$ and $s_2$ have a common multiple $s_2 h$, so by induction have a least common multiple $s_2 h_2$. Then $s_1 s_2 h_2$ is a least common multiple of $s$ and $s'$. □

## Proposition (check common multiple on generators)

*In a group $W$ generated positively by $R$, let $S$ be an interval stable under left and right divisors and assume any $r, r' \in R$ which have a common multiple have a least common multiple. Then any $s, s'$ in $S$ which have a common multiple have a least common multiple.*

### Proof.

The proof is by induction on $l_R(s) + l_R(s')$. If $l_R(s) = l_R(s') = 1$ we are at the start of the induction. Otherwise one of them, say $s$ is a product $s = s_1 s_2$. Assume $s, s'$ have a common multiple $sh$. Then $sh$ is a common multiple of $s_1$ and $s'$ so by induction they have a least common multiple $s_1 h_1$. Now $h_1$ and $s_2$ have a common multiple $s_2 h$, so by induction have a least common multiple $s_2 h_2$. Then $s_1 s_2 h_2$ is a least common multiple of $s$ and $s'$. □

## Proposition (check common multiple on generators)

*In a group $W$ generated positively by $R$, let $S$ be an interval stable under left and right divisors and assume any $r, r' \in R$ which have a common multiple have a least common multiple. Then any $s, s'$ in $S$ which have a common multiple have a least common multiple.*

## Proof.

The proof is by induction on $l_R(s) + l_R(s')$. If $l_R(s) = l_R(s') = 1$ we are at the start of the induction. Otherwise one of them, say $s$ is a product $s = s_1 s_2$. Assume $s, s'$ have a common multiple $sh$. Then $sh$ is a common multiple of $s_1$ and $s'$ so by induction they have a least common multiple $s_1 h_1$. Now $h_1$ and $s_2$ have a common multiple $s_2 h$, so by induction have a least common multiple $s_2 h_2$. Then $s_1 s_2 h_2$ is a least common multiple of $s$ and $s'$. □

### Proposition (check common multiple on generators)

*In a group $W$ generated positively by $R$, let $S$ be an interval stable under left and right divisors and assume any $r, r' \in R$ which have a common multiple have a least common multiple. Then any $s, s'$ in $S$ which have a common multiple have a least common multiple.*

### Proof.

The proof is by induction on $l_R(s) + l_R(s')$. If $l_R(s) = l_R(s') = 1$ we are at the start of the induction. Otherwise one of them, say $s$ is a product $s = s_1 s_2$. Assume $s, s'$ have a common multiple $sh$. Then $sh$ is a common multiple of $s_1$ and $s'$ so by induction they have a least common multiple $s_1 h_1$. Now $h_1$ and $s_2$ have a common multiple $s_2 h$, so by induction have a least common multiple $s_2 h_2$. Then $s_1 s_2 h_2$ is a least common multiple of $s$ and $s'$. □

## Proposition (check common multiple on generators)

*In a group $W$ generated positively by $R$, let $S$ be an interval stable under left and right divisors and assume any $r, r' \in R$ which have a common multiple have a least common multiple. Then any $s, s'$ in $S$ which have a common multiple have a least common multiple.*

## Proof.

The proof is by induction on $l_R(s) + l_R(s')$. If $l_R(s) = l_R(s') = 1$ we are at the start of the induction. Otherwise one of them, say $s$ is a product $s = s_1 s_2$. Assume $s, s'$ have a common multiple $sh$. Then $sh$ is a common multiple of $s_1$ and $s'$ so by induction they have a least common multiple $s_1 h_1$. Now $h_1$ and $s_2$ have a common multiple $s_2 h$, so by induction have a least common multiple $s_2 h_2$. Then $s_1 s_2 h_2$ is a least common multiple of $s$ and $s'$. $\square$

## Proposition (check common multiple on generators)

*In a group $W$ generated positively by $R$, let $S$ be an interval stable under left and right divisors and assume any $r, r' \in R$ which have a common multiple have a least common multiple. Then any $s, s'$ in $S$ which have a common multiple have a least common multiple.*

## Proof.

The proof is by induction on $l_R(s) + l_R(s')$. If $l_R(s) = l_R(s') = 1$ we are at the start of the induction. Otherwise one of them, say $s$ is a product $s = s_1 s_2$. Assume $s, s'$ have a common multiple $sh$. Then $sh$ is a common multiple of $s_1$ and $s'$ so by induction they have a least common multiple $s_1 h_1$. Now $h_1$ and $s_2$ have a common multiple $s_2 h$, so by induction have a least common multiple $s_2 h_2$. Then $s_1 s_2 h_2$ is a least common multiple of $s$ and $s'$. □

## Proposition (check common multiple on generators)

*In a group $W$ generated positively by $R$, let $S$ be an interval stable under left and right divisors and assume any $r, r' \in R$ which have a common multiple have a least common multiple. Then any $s, s'$ in $S$ which have a common multiple have a least common multiple.*

## Proof.

The proof is by induction on $l_R(s) + l_R(s')$. If $l_R(s) = l_R(s') = 1$ we are at the start of the induction. Otherwise one of them, say $s$ is a product $s = s_1 s_2$. Assume $s, s'$ have a common multiple $sh$. Then $sh$ is a common multiple of $s_1$ and $s'$ so by induction they have a least common multiple $s_1 h_1$. Now $h_1$ and $s_2$ have a common multiple $s_2 h$, so by induction have a least common multiple $s_2 h_2$. Then $s_1 s_2 h_2$ is a least common multiple of $s$ and $s'$. □

## Proposition (check extend on generators)

*In a group $W$ generated positively by $R$, let $S$ be an interval stable under left and right divisors and assume that for any $f \in S$ and any $r, r' \in R$ which have a common multiple and for which $fr$ and $fr'$ are in $S$ then $f \operatorname{right-lcm}(r, r') \in S$. Then for any $s, s'$ in $S$ which have a common multiple and for which $fs$ and $fs'$ are in $S$ then $f \operatorname{right-lcm}(s, s') \in S$.*

**Proof.**

The previous proposition was the particular case where $f = 1$. The proof is similarly by induction on $l_R(s) + l_R(s')$, but this time we keep track of the property of elements $fs_1h_1$, $fs_1s_2h_2$ to be in $S$. This is left as an exercise. □

The previous two propositions reduce the check for existence of least common multiples to generators.

## Proposition (check extend on generators)

*In a group $W$ generated positively by $R$, let $S$ be an interval stable under left and right divisors and assume that for any $f \in S$ and any $r, r' \in R$ which have a common multiple and for which $fr$ and $fr'$ are in $S$ then $f\,\mathrm{right\text{-}lcm}(r, r') \in S$. Then for any $s, s'$ in $S$ which have a common multiple and for which $fs$ and $fs'$ are in $S$ then $f\,\mathrm{right\text{-}lcm}(s, s') \in S$.*

**Proof.**

The previous proposition was the particular case where $f = 1$. The proof is similarly by induction on $l_R(s) + l_R(s')$, but this time we keep track of the property of elements $fs_1h_1$, $fs_1s_2h_2$ to be in $S$. This is left as an exercise. □

The previous two propositions reduce the check for existence of least common multiples to generators.

## Proposition (check extend on generators)

*In a group $W$ generated positively by $R$, let $S$ be an interval stable under left and right divisors and assume that for any $f \in S$ and any $r, r' \in R$ which have a common multiple and for which $fr$ and $fr'$ are in $S$ then $f\,\mathrm{right\text{-}lcm}(r, r') \in S$. Then for any $s, s'$ in $S$ which have a common multiple and for which $fs$ and $fs'$ are in $S$ then $f\,\mathrm{right\text{-}lcm}(s, s') \in S$.*

## Proof.

The previous proposition was the particular case where $f = 1$. The proof is similarly by induction on $l_R(s) + l_R(s')$, but this time we keep track of the property of elements $fs_1h_1$, $fs_1s_2h_2$ to be in $S$. This is left as an exercise. □

The previous two propositions reduce the check for existence of least common multiples to generators.

## Proposition (check extend on generators)

*In a group $W$ generated positively by $R$, let $S$ be an interval stable under left and right divisors and assume that for any $f \in S$ and any $r, r' \in R$ which have a common multiple and for which $fr$ and $fr'$ are in $S$ then $f\,\mathrm{right\text{-}lcm}(r, r') \in S$. Then for any $s, s'$ in $S$ which have a common multiple and for which $fs$ and $fs'$ are in $S$ then $f\,\mathrm{right\text{-}lcm}(s, s') \in S$.*

## Proof.

The previous proposition was the particular case where $f = 1$. The proof is similarly by induction on $l_R(s) + l_R(s')$, but this time we keep track of the property of elements $fs_1h_1$, $fs_1s_2h_2$ to be in $S$. This is left as an exercise. □

The previous two propositions reduce the check for existence of least common multiples to generators.

## Proposition (check extend on generators)

*In a group $W$ generated positively by $R$, let $S$ be an interval stable under left and right divisors and assume that for any $f \in S$ and any $r, r' \in R$ which have a common multiple and for which $fr$ and $fr'$ are in $S$ then $f\,\mathrm{right\text{-}lcm}(r, r') \in S$. Then for any $s, s'$ in $S$ which have a common multiple and for which $fs$ and $fs'$ are in $S$ then $f\,\mathrm{right\text{-}lcm}(s, s') \in S$.*

## Proof.

The previous proposition was the particular case where $f = 1$. The proof is similarly by induction on $l_R(s) + l_R(s')$, but this time we keep track of the property of elements $fs_1h_1$, $fs_1s_2h_2$ to be in $S$. This is left as an exercise. □

The previous two propositions reduce the check for existence of least common multiples to generators.

## Proposition (check extend on generators)

*In a group $W$ generated positively by $R$, let $S$ be an interval stable under left and right divisors and assume that for any $f \in S$ and any $r, r' \in R$ which have a common multiple and for which $fr$ and $fr'$ are in $S$ then $f\,\mathrm{right\text{-}lcm}(r, r') \in S$. Then for any $s, s'$ in $S$ which have a common multiple and for which $fs$ and $fs'$ are in $S$ then $f\,\mathrm{right\text{-}lcm}(s, s') \in S$.*

## Proof.

The previous proposition was the particular case where $f = 1$. The proof is similarly by induction on $l_R(s) + l_R(s')$, but this time we keep track of the property of elements $fs_1h_1$, $fs_1s_2h_2$ to be in $S$. This is left as an exercise. □

The previous two propositions reduce the check for existence of least common multiples to generators.

## Proposition ($I$-reduced element)

*Let $(W, S)$ be a Coxeter system, and let $W_I$ be a parabolic subgroup for $I \subset S$. In any coset $W_I w$ there is a unique element $x$ of minimal length, characterized by the equivalent properties:*

- $l_S(v) + l_S(x) = l_S(vx)$ *for any* $v \in W_I$.
- $x$ *is not divisible on the left by any* $i \in I$ $(l_S(ix) = l_S(x) + 1)$.

Assume $s, s' \in S$ have a common multiple $w$ and write $w = vx$ where $x$ is the minimal element in $W_I w$ for $I = \{s, s'\}$. By assumption $l_S(svx) = l_S(vx) - 1$. We cannot have $l_S(sv) = l_S(v) + 1$ by the first item since the lengths add. It follows that $v \in W_I$ is a common multiple of $s, s'$. Now in the dihedral group $W_I$ the generators have a common multiple if and only if $W_I$ is finite and it is the longest element of $\Delta_{s,s'}$ of $W_I$, thus unique. For the property (extend by generators) we want that if $l_S(ws) = l_S(w+1)$ and $l_S(ws') = l_S(w+1)$ then $l_S(w\Delta_{s,s'}) = l_S(w) + l_S(\Delta_{s,s'})$. This is a consequence of the equivalence of the two items in the proposition.

## Proposition ($I$-reduced element)

*Let $(W,S)$ be a Coxeter system, and let $W_I$ be a parabolic subgroup for $I \subset S$. In any coset $W_I w$ there is a unique element $x$ of minimal length, characterized by the equivalent properties:*

- $l_S(v) + l_S(x) = l_S(vx)$ *for any* $v \in W_I$.
- $x$ *is not divisible on the left by any* $i \in I$ $(l_S(ix) = l_S(x) + 1)$.

Assume $s, s' \in S$ have a common multiple $w$ and write $w = vx$ where $x$ is the minimal element in $W_I w$ for $I = \{s, s'\}$. By assumption $l_S(svx) = l_S(vx) - 1$. We cannot have $l_S(sv) = l_S(v) + 1$ by the first item since the lengths add. It follows that $v \in W_I$ is a common multiple of $s, s'$. Now in the dihedral group $W_I$ the generators have a common multiple if and only if $W_I$ is finite and it is the longest element of $\Delta_{s,s'}$ of $W_I$, thus unique. For the property (extend by generators) we want that if $l_S(ws) = l_S(w+1)$ and $l_S(ws') = l_S(w+1)$ then $l_S(w\Delta_{s,s'}) = l_S(w) + l_S(\Delta_{s,s'})$. This is a consequence of the equivalence of the two items in the proposition.

## Proposition ($I$-reduced element)

*Let $(W, S)$ be a Coxeter system, and let $W_I$ be a parabolic subgroup for $I \subset S$. In any coset $W_I w$ there is a unique element $x$ of minimal length, characterized by the equivalent properties:*

- $l_S(v) + l_S(x) = l_S(vx)$ *for any* $v \in W_I$.
- $x$ *is not divisible on the left by any* $i \in I$ $(l_S(ix) = l_S(x) + 1)$.

Assume $s, s' \in S$ have a common multiple $w$ and write $w = vx$ where $x$ is the minimal element in $W_I w$ for $I = \{s, s'\}$. By assumption $l_S(svx) = l_S(vx) - 1$. We cannot have $l_S(sv) = l_S(v) + 1$ by the first item since the lengths add. It follows that $v \in W_I$ is a common multiple of $s, s'$. Now in the dihedral group $W_I$ the generators have a common multiple if and only if $W_I$ is finite and it is the longest element of $\Delta_{s,s'}$ of $W_I$, thus unique.

For the property (extend by generators) we want that if $l_S(ws) = l_S(w+1)$ and $l_S(ws') = l_S(w+1)$ then $l_S(w\Delta_{s,s'}) = l_S(w) + l_S(\Delta_{s,s'})$. This is a consequence of the equivalence of the two items in the proposition.

## Proposition ($I$-reduced element)

*Let $(W, S)$ be a Coxeter system, and let $W_I$ be a parabolic subgroup for $I \subset S$. In any coset $W_I w$ there is a unique element $x$ of minimal length, characterized by the equivalent properties:*

- $l_S(v) + l_S(x) = l_S(vx)$ *for any* $v \in W_I$.
- $x$ *is not divisible on the left by any* $i \in I$ ($l_S(ix) = l_S(x) + 1$).

Assume $s, s' \in S$ have a common multiple $w$ and write $w = vx$ where $x$ is the minimal element in $W_I w$ for $I = \{s, s'\}$. By assumption $l_S(svx) = l_S(vx) - 1$. We cannot have $l_S(sv) = l_S(v) + 1$ by the first item since the lengths add. It follows that $v \in W_I$ is a common multiple of $s, s'$. Now in the dihedral group $W_I$ the generators have a common multiple if and only if $W_I$ is finite and it is the longest element of $\Delta_{s,s'}$ of $W_I$, thus unique. For the property (extend by generators) we want that if $l_S(ws) = l_S(w + 1)$ and $l_S(ws') = l_S(w + 1)$ then $l_S(w\Delta_{s,s'}) = l_S(w) + l_S(\Delta_{s,s'})$. This is a consequence of the equivalence of the two items in the proposition.

## Proposition ($I$-reduced element)

*Let $(W, S)$ be a Coxeter system, and let $W_I$ be a parabolic subgroup for $I \subset S$. In any coset $W_I w$ there is a unique element $x$ of minimal length, characterized by the equivalent properties:*

- $l_S(v) + l_S(x) = l_S(vx)$ *for any* $v \in W_I$.
- $x$ *is not divisible on the left by any* $i \in I$ *(*$l_S(ix) = l_S(x) + 1$*).*

Assume $s, s' \in S$ have a common multiple $w$ and write $w = vx$ where $x$ is the minimal element in $W_I w$ for $I = \{s, s'\}$. By assumption $l_S(svx) = l_S(vx) - 1$. We cannot have $l_S(sv) = l_S(v) + 1$ by the first item since the lengths add. It follows that $v \in W_I$ is a common multiple of $s, s'$. Now in the dihedral group $W_I$ the generators have a common multiple if and only if $W_I$ is finite and it is the longest element of $\Delta_{s,s'}$ of $W_I$, thus unique. For the property (extend by generators) we want that if $l_S(ws) = l_S(w + 1)$ and $l_S(ws') = l_S(w + 1)$ then $l_S(w\Delta_{s,s'}) = l_S(w) + l_S(\Delta_{s,s'})$. This is a consequence of the equivalence of the two items in the proposition.

## Proposition ($I$-reduced element)

*Let $(W, S)$ be a Coxeter system, and let $W_I$ be a parabolic subgroup for $I \subset S$. In any coset $W_I w$ there is a unique element $x$ of minimal length, characterized by the equivalent properties:*

- $l_S(v) + l_S(x) = l_S(vx)$ *for any* $v \in W_I$.
- $x$ *is not divisible on the left by any* $i \in I$ $(l_S(ix) = l_S(x) + 1)$.

Assume $s, s' \in S$ have a common multiple $w$ and write $w = vx$ where $x$ is the minimal element in $W_I w$ for $I = \{s, s'\}$. By assumption $l_S(svx) = l_S(vx) - 1$. We cannot have $l_S(sv) = l_S(v) + 1$ by the first item since the lengths add. It follows that $v \in W_I$ is a common multiple of $s, s'$. Now in the dihedral group $W_I$ the generators have a common multiple if and only if $W_I$ is finite and it is the longest element of $\Delta_{s,s'}$ of $W_I$, thus unique. For the property (extend by generators) we want that if $l_S(ws) = l_S(w + 1)$ and $l_S(ws') = l_S(w + 1)$ then $l_S(w\Delta_{s,s'}) = l_S(w) + l_S(\Delta_{s,s'})$. This is a consequence of the equivalence of the two items in the proposition.

## Proposition ($I$-reduced element)

*Let $(W, S)$ be a Coxeter system, and let $W_I$ be a parabolic subgroup for $I \subset S$. In any coset $W_I w$ there is a unique element $x$ of minimal length, characterized by the equivalent properties:*

- $l_S(v) + l_S(x) = l_S(vx)$ *for any* $v \in W_I$.
- $x$ *is not divisible on the left by any* $i \in I$ ($l_S(ix) = l_S(x) + 1$).

Assume $s, s' \in S$ have a common multiple $w$ and write $w = vx$ where $x$ is the minimal element in $W_I w$ for $I = \{s, s'\}$. By assumption $l_S(svx) = l_S(vx) - 1$. We cannot have $l_S(sv) = l_S(v) + 1$ by the first item since the lengths add. It follows that $v \in W_I$ is a common multiple of $s, s'$. Now in the dihedral group $W_I$ the generators have a common multiple if and only if $W_I$ is finite and it is the longest element of $\Delta_{s,s'}$ of $W_I$, thus unique. For the property (extend by generators) we want that if $l_S(ws) = l_S(w + 1)$ and $l_S(ws') = l_S(w + 1)$ then $l_S(w\Delta_{s,s'}) = l_S(w) + l_S(\Delta_{s,s'})$. This is a consequence of the equivalence of the two items in the proposition.

## Proposition ($I$-reduced element)

*Let $(W, S)$ be a Coxeter system, and let $W_I$ be a parabolic subgroup for $I \subset S$. In any coset $W_I w$ there is a unique element $x$ of minimal length, characterized by the equivalent properties:*

- $l_S(v) + l_S(x) = l_S(vx)$ *for any* $v \in W_I$.
- $x$ *is not divisible on the left by any* $i \in I$ *(*$l_S(ix) = l_S(x) + 1$*).*

Assume $s, s' \in S$ have a common multiple $w$ and write $w = vx$ where $x$ is the minimal element in $W_I w$ for $I = \{s, s'\}$. By assumption $l_S(svx) = l_S(vx) - 1$. We cannot have $l_S(sv) = l_S(v) + 1$ by the first item since the lengths add. It follows that $v \in W_I$ is a common multiple of $s, s'$. Now in the dihedral group $W_I$ the generators have a common multiple if and only if $W_I$ is finite and it is the longest element of $\Delta_{s,s'}$ of $W_I$, thus unique.

For the property (extend by generators) we want that if $l_S(ws) = l_S(w + 1)$ and $l_S(ws') = l_S(w + 1)$ then $l_S(w\Delta_{s,s'}) = l_S(w) + l_S(\Delta_{s,s'})$. This is a consequence of the equivalence of the two items in the proposition.

## Proposition ($I$-reduced element)

*Let $(W, S)$ be a Coxeter system, and let $W_I$ be a parabolic subgroup for $I \subset S$. In any coset $W_I w$ there is a unique element $x$ of minimal length, characterized by the equivalent properties:*

- $l_S(v) + l_S(x) = l_S(vx)$ *for any* $v \in W_I$.
- $x$ *is not divisible on the left by any* $i \in I$ *(*$l_S(ix) = l_S(x) + 1$*).*

Assume $s, s' \in S$ have a common multiple $w$ and write $w = vx$ where $x$ is the minimal element in $W_I w$ for $I = \{s, s'\}$. By assumption $l_S(svx) = l_S(vx) - 1$. We cannot have $l_S(sv) = l_S(v) + 1$ by the first item since the lengths add. It follows that $v \in W_I$ is a common multiple of $s, s'$. Now in the dihedral group $W_I$ the generators have a common multiple if and only if $W_I$ is finite and it is the longest element of $\Delta_{s,s'}$ of $W_I$, thus unique. For the property (extend by generators) we want that if $l_S(ws) = l_S(w + 1)$ and $l_S(ws') = l_S(w + 1)$ then $l_S(w\Delta_{s,s'}) = l_S(w) + l_S(\Delta_{s,s'})$. This is a consequence of the equivalence of the two items in the proposition.

## Proposition ($I$-reduced element)

*Let $(W,S)$ be a Coxeter system, and let $W_I$ be a parabolic subgroup for $I \subset S$. In any coset $W_I w$ there is a unique element $x$ of minimal length, characterized by the equivalent properties:*

- $l_S(v) + l_S(x) = l_S(vx)$ *for any* $v \in W_I$.
- $x$ *is not divisible on the left by any* $i \in I$ *(*$l_S(ix) = l_S(x) + 1$*).*

Assume $s, s' \in S$ have a common multiple $w$ and write $w = vx$ where $x$ is the minimal element in $W_I w$ for $I = \{s, s'\}$. By assumption $l_S(svx) = l_S(vx) - 1$. We cannot have $l_S(sv) = l_S(v) + 1$ by the first item since the lengths add. It follows that $v \in W_I$ is a common multiple of $s, s'$. Now in the dihedral group $W_I$ the generators have a common multiple if and only if $W_I$ is finite and it is the longest element of $\Delta_{s,s'}$ of $W_I$, thus unique. For the property (extend by generators) we want that if $l_S(ws) = l_S(w+1)$ and $l_S(ws') = l_S(w+1)$ then $l_S(w\Delta_{s,s'}) = l_S(w) + l_S(\Delta_{s,s'})$. This is a consequence of the equivalence of the two items in the proposition.