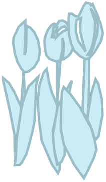
Universitat de València

A DECOMPOSITION THEOREM FOR FINITE MONOID ACTIONS

Centrum Wiskunde & Informatica

Amsterdam, 2014



Enric Cosme

Departament d'Àlgebra
Universitat de València

MONOID

Definition

A Monoid is tuple $(M, \cdot, 1)$ where M is a set, $\cdot$ is an associative binary operation and 1 is an element in M with the property:

$$1m = m1 = m$$

for all $m \in M$. We will usually write M for the sake of simplicity.

MONOID

Definition

A Monoid is tuple $(M, \cdot, 1)$ where M is a set, $\cdot$ is an associative binary operation and 1 is an element in M with the property:

$$1m = m1 = m$$

for all $m \in M$. We will usually write M for the sake of simplicity.

Basic examples of monoids

For a set X, $\mathcal{T}_X = \{f\colon f \text{ is a function from } X \text{ to } X\}$

MONOID

Definition

A Monoid is tuple $(M, \cdot, 1)$ where M is a set, $\cdot$ is an associative binary operation and 1 is an element in M with the property:

$$1m = m1 = m$$

for all $m \in M$. We will usually write M for the sake of simplicity.

Basic examples of monoids

For a set X, $\mathcal{T}_X = \{f \colon f \text{ is a function from } X \text{ to } X\}$

For a set A, the free monoid A^* over A.

GROUP

Definition

Let a, b be two elements of the monoid M. We say that b is the inverse of a if

$$ab = ba = 1$$

GROUP

Definition

Let a, b be two elements of the monoid M. We say that b is the inverse of a if

$$ab = ba = 1$$

We say that a monoid M is a group if every element $a \in M$ has an inverse. We usually denote groups by G.

GROUP

Definition

Let a, b be two elements of the monoid M. We say that b is the inverse of a if

$$ab = ba = 1$$

We say that a monoid M is a group if every element $a \in M$ has an inverse. We usually denote groups by G.

Basic examples of groups

For a set X, $\Sigma_X = \{f \colon f \text{ is a bijective function from } X \text{ to } X\}$

GROUP

Definition

Let a, b be two elements of the monoid M. We say that b is the inverse of a if

$$ab = ba = 1$$

We say that a monoid M is a group if every element $a \in M$ has an inverse. We usually denote groups by G.

Basic examples of groups

For a set X, $\Sigma_X = \{f \colon f$ is a bijective function from X to $X\}$

The integers with the sum $(\mathbb{Z}, +, 0)$.

ACTION

Definition

Let M be a monoid and let X be any set. We say that M acts on the left of X if there exists a mapping:

$$\begin{array}{cccc} : & M \times X & \longrightarrow & X \\ & (m, x) & \longmapsto & mx \end{array}$$

for which the following properties hold:

a1. For all $m_1, m_2 \in M$ and $x \in X$, $m_2(m_1x) = (m_2m_1)x$.

a2. For all $x \in X$, $1x = x$.

We will say that X is a left M-set.

ACTION

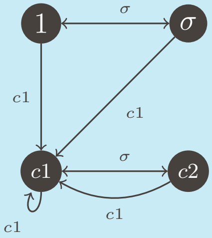
The natural action

Let M be any monoid. It can act on itself using the internal multiplication law on M:

$$\begin{array}{rccc} : & M \times M & \longrightarrow & M \\ & (m_1, m_2) & \longmapsto & m_1 m_2 \end{array}$$

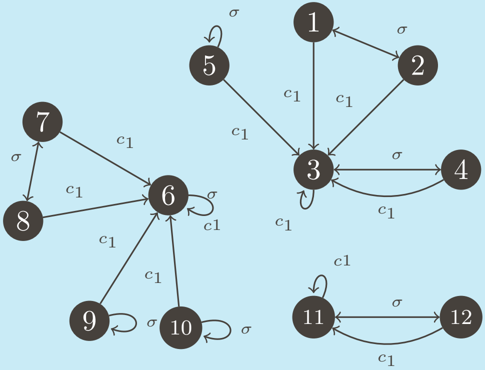
ACTIONS

The natural action of $\mathcal{T}_2$



ACTIONS

An arbitrary action of $\mathcal{T}_2$ on a set of 12 elements



M-MORPHISM

Definition

If X and Y are two M-sets, we define a M-morphism from X to Y to be a function $f : X \to Y$ such that

$$f(m \cdot x) = m \cdot f(x)$$

for all m in M and all $x \in X$.

If f is bijective, we will say that the actions are equivalent.

CONGRUENCES

Definition

Let X be an M-set. A relation $\Theta \subseteq X \times X$ is called left stable if for each $x, y \in X$ and $m \in M$, the condition

$$x \Theta y \quad \text{implies} \quad mx \Theta my$$

A left congruence is any equivalence relation that is left stable.

CONGRUENCES

Definition

Let X be an M-set. A relation $\Theta \subseteq X \times X$ is called left stable if for each $x, y \in X$ and $m \in M$, the condition

$$x \Theta y \quad \text{implies} \quad mx \Theta my$$

A left congruence is any equivalence relation that is left stable.

One can define a natural left action on the quotient X/Θ in terms of the action defined on X in such a way that the canonical surjection $\pi_\Theta : X \to X/\Theta$ is an M-epimorphism. Moreover, this allow us to obtain a 1st Isomorphism Theorem on M-sets.

TYPES OF ACTIONS

Definition

Let X be an M-set. The action is said to be:

- Transitive; If for each $x, y \in X$, there is an element $m \in M$ with $mx = y$.

TYPES OF ACTIONS

Definition

Let X be an M-set. The action is said to be:

- Transitive; If for each $x, y \in X$, there is an element $m \in M$ with $mx = y$.
- Cyclic; If there exists an element $x \in X$ such that $Mx = X$.

TYPES OF ACTIONS

Definition

Let X be an M-set. The action is said to be:

- Transitive; If for each $x, y \in X$, there is an element $m \in M$ with $mx = y$.
- Cyclic; If there exists an element $x \in X$ such that $Mx = X$.
- Quasi-transitive; If X is not the coproduct of two proper invariant subsets.

TYPES OF ACTIONS

Definition

Let X be an M-set. The action is said to be:

- Transitive; If for each $x, y \in X$, there is an element $m \in M$ with $mx = y$.
- Cyclic; If there exists an element $x \in X$ such that $Mx = X$.
- Quasi-transitive; If X is not the coproduct of two proper invariant subsets.

The following implications hold:

$$\text{Transitive} \quad \Rightarrow \quad \text{Cyclic} \quad \Rightarrow \quad \text{Quasi-transitive}$$

TYPES OF ACTIONS

Definition

Let X be an M-set. The action is said to be:

Transitive; If for each $x, y \in X$, there is an element $m \in M$ with $mx = y$.

Cyclic; If there exists an element $x \in X$ such that $Mx = X$.

Quasi-transitive; If X is not the coproduct of two proper invariant subsets.

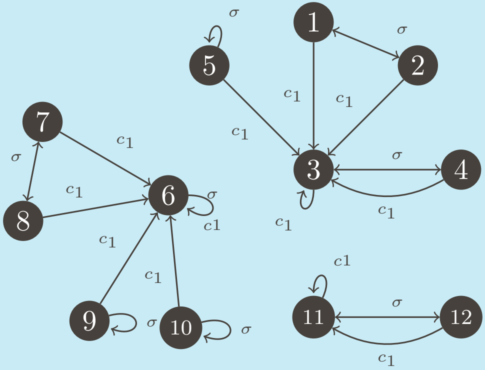
The following implications hold:

$$\text{Transitive} \quad \Rightarrow \quad \text{Cyclic} \quad \Rightarrow \quad \text{Quasi-transitive}$$

They all coincide when we work with group actions.

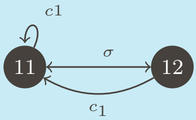
TYPES OF ACTIONS

An arbitrary action of $\mathcal{T}_2$ on a set of 12 elements



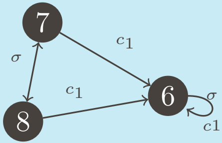
TYPES OF ACTIONS

A transitive action



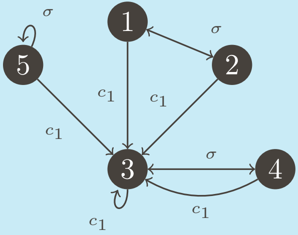
TYPES OF ACTIONS

A cyclic action



TYPES OF ACTIONS

A quasi-transitive action



BUILDING BLOCKS

Theorem

Let X and Y be two M-sets. Then the following statements are equivalent:

i. $X \cong Y$

ii. There exists a bijection $h : \pi_0(X) \to \pi_0(Y)$ from the set of quasi-transitive subsets of X to the set of quasi-transitive subsets of Y that relates equivalent actions, that is to say, for each $X' \in \pi_0(X)$, the action of M on X' is equivalent to the action of M on $h(X')$.

BUILDING BLOCKS

So far we have seen that the usual definitions of transitivity on group actions are useless to monoid actions.

Quasi-transitive actions are the building blocks for monoid actions, but they are still difficult to handle. Instead, cyclic actions are the easiest actions to work with.

DECOMPOSITION THEOREM

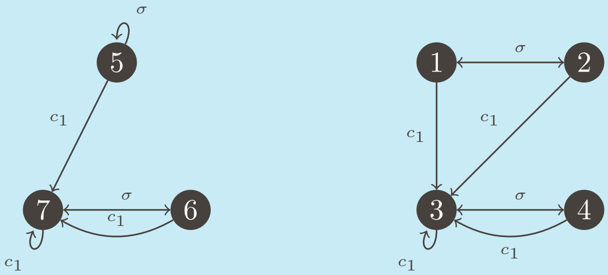
Definition

Let X and Y be two M-sets. Assume that they both have non-empty invariant subsets which are equivalent to an M-set W. Then we can consider the amalgamated sum of X and Y relative to W. It is again an M-set which will be denoted by:

$$X \amalg_W Y$$

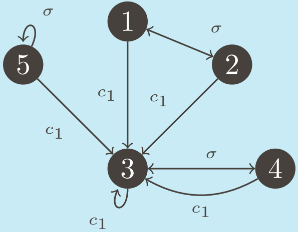
DECOMPOSITION THEOREM

Amalgamated Sum



DECOMPOSITION THEOREM

Amalgamated Sum



DECOMPOSITION THEOREM

Theorem

Let X be a finite M-set. Assume that the action of M on X is quasi-transitive. Then there are invariant subsets W, Y, Z of X such that:

i. W is a common non-empty invariant subset of both Y and Z.
ii. Y is a cyclic M-set.
iii. Z is a quasi-transitive M-set.
iv. $X \cong Y \amalg_W Z$

DECOMPOSITION THEOREM

Theorem

Let X be a finite M-set. Assume that the action of M on X is quasi-transitive. Then there are invariant subsets W, Y, Z of X such that:

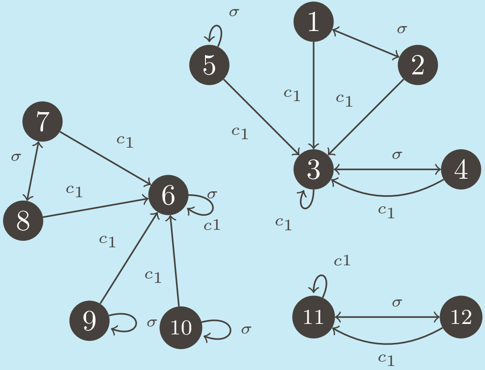
i. W is a common non-empty invariant subset of both Y and Z.
ii. Y is a cyclic M-set.
iii. Z is a quasi-transitive M-set.
iv. $X \cong Y \amalg_W Z$

Corollary

Every finite quasi-transitive M-set can be written as an amalgamated sum of cyclic M-sets.

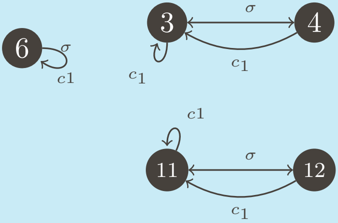
DECOMPOSITION THEOREM

An arbitrary action of $\mathcal{T}_2$ on a set of 12 elements



DECOMPOSITION THEOREM

W invariant subsets



DECOMPOSITION THEOREM

Corollary

Let X be a finite quasi-transitive M-set that is not cyclic. Then the W subset that appears in the decomposition theorem is isomorphic to a quotient of the greatest proper left-ideal contained in M.

BIBLIOGRAPHY

- J. Climent Vidal,
  Teoría de Conjuntos,
  Lecture Notes, Universitat de València, 2010.
- R. Jansana,
  Orders, Lattices and Boolean Algebras,
  Lecture Notes, Universitat de Barcelona, 2010-11.
- M. Kilp, U. Knauer, A.V. Mikhalev,
  Monoids, Acts and Categories,
  Walter de Gruyter, Berlin, 2000.
- B. Steinberg,
  A Theory of Transformation Monoids: Combinatorics and Representation Theory,
  eprint arXiv:1004.2982, 2010.