Visual Algebra

Lecture 1.6: The formal definition of a group

Dr. Matthew Macauley

School of Mathematical & Statistical Sciences
Clemson University
South Carolina, USA
http://www.math.clemson.edu/~macaule/

Forbidden Cayley tables?

Last time, we finished with two Latin squares on a set of five elements.

These are tables where every element appears in every row and column once.

There is even an identity element e.

	e	a	b	c	d
e	e	a	b	c	d
a	a	c	d	b	e
b	b	d	a	e	c
c	c	b	e	d	a
d	d	e	c	a	b

	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	d	e	a	c
c	c	b	d	e	a
d	d	c	a	b	e

Question

Are these Cayley tables of a group? If not, what goes wrong?

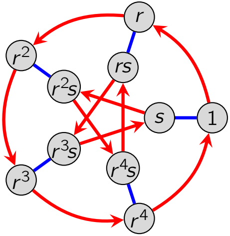
More generally: *Can we use a Latin square to define an abstract group?*

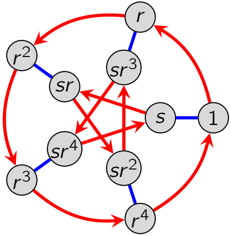
Forbidden Cayley graphs?

Motivated by symmetries, we began by calling members of a group "actions."

Then we encountered Q_8, and it wasn't clear that there even is an underlying action.

It is natural to ask: *Can we use a Cayley graph to define an abstract group?*





Consider $r^2s = sr$, and the blue-red path. This takes 10 iterations from any node to return.

But that would imply that $G = \langle sr \rangle$, and every cyclic group must be abelian. *(Why?)*

As before, we can try to write a presentation from this graph:

$$G = \big\langle r, s \mid r^5 = s^2 = 1,\ rs = sr^3,\ r^2s = sr,\ r^3s = sr^4,\ r^4s = sr^2 \big\rangle$$

Question. *What group is this?*

Binary operations and associativity

The previous slide is a cautionary tale for why we need a formal definition.

A group is a set of elements satisfying a few properties.

Combining elements can be done with a binary operation, e.g., $+$, $-$, $\cdot$, and $\div$.

Definition

If $*$ is a binary operation on a set S, then $s * t \in S$ for all $s, t \in S$. In this case, we say that S is closed under the operation $*$.

Alternatively, we say that $*$ is a binary operation on S.

Definition

A binary operation $*$ on S is associative if

$$a * (b * c) = (a * b) * c, \qquad \text{for all } a, b, c \in S.$$

Associative basically means *parentheses are permitted anywhere, but required nowhere*.

For example, addition and multiplication are associative, but subtraction and division are not:

$$4 - (1 - 2) \neq (4 - 1) - 2, \qquad 4/(1/2) \neq (4/1)/2.$$

The formal definition of a group

We are now ready to formally define a group.

Definition

A group is a set G satisfying the following properties:

1. There is an associative binary operation $*$ on G.
2. There is an identity element $e \in G$. That is, $e * g = g = g * e$ for all $g \in G$.
3. Every element $g \in G$ has an inverse, g^{-1}, satisfying $g * g^{-1} = e = g^{-1} * g$.

Remarks

- Depending on context, the binary operation may be denoted by $*$, $\cdot$, $+$, or $\circ$.
- We frequently omit the symbol and write, e.g., xy for $x * y$.
- We only use $+$ if G is abelian. Thus, $g + h = h + g$ (always), but in general, $gh \neq hg$.
- Uniqueness of the identity and inverses is *not* built into this definition. However, it's an easy exercise to establish.

A few simple properties

Let's verify uniqueness of the identity and inverses.

Theorem

Every element of a group has a unique inverse.

Verification

Let g be an element of a group G. By definition, it has at least one inverse.

Suppose that h and k are both inverses of g. This means that $gh = hg = e$ and $gk = kg = e$. It suffices to show that $h = k$. Indeed,

$$h = he = h(gk) = (hg)k = ek = k,$$

which is what we needed to show. $\square$

The technique of the following is similar.

Theorem

Every group has a unique identity element.

Revisiting our Latin squares

	e	a	b	c	d
e	e	a	b	c	d
a	a	c	d	b	e
b	b	d	a	e	c
c	c	b	e	d	a
d	d	e	c	a	b

	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	d	e	a	c
c	c	b	d	e	a
d	d	c	a	b	e

The table on the left describes a group $\mathbb{Z}_5 := \{0, 1, 2, 3, 4\}$ under addition modulo 5:

$$e = 0, \qquad a = 1, \qquad b = 3, \qquad c = 2, \qquad d = 4.$$

The table on the right fails associativity:

$$(a * b) * d = c * d = a, \qquad a * (b * d) = a * c = d.$$

Due to *F.W. Light's associativity test*, there is no shortcut for determining whether the binary operation in a Latin square is associative.

Specifically, the worst-case running time is $O(n^3)$, the number of (a, b, c)-triples.