Document last updated Mon, Sep 30, 2024

Abstract Algebra Notes

Week 1 Wed, Sep 4, 2024

Outline

Names & icebreaker

First examples of groups and Cayley graphs

Groups: Def and examples (Judson Sec 3.1)

Group quiz 1

Syllabus / HW 01 (Overleaf.com)

* Break around 8 pm

Shorthand:

elt → element

iff → if and only if

$\mathbb{N} = \{n : n \text{ is a natural numbers}\} = \{1, 2, 3, \ldots\}$

$\mathbb{Z} = \{n : n \text{ is an integer}\} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

$\mathbb{Q} = \{r : r \text{ is a rational number}\}$

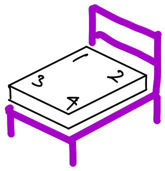
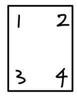
$= \{\frac{p}{q} : p, q \in \mathbb{Z} \text{ where } q \neq 0\}$

$\mathbb{R} = \{x : x \text{ is a real number}\}$

$\mathbb{C} = \{z : z \text{ is a complex number}\}$

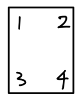
$= \{a + bi : a, b \in \mathbb{R}\}$

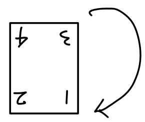
The mattress group G_1

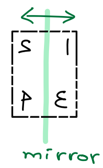
Original position:  or  for convenience

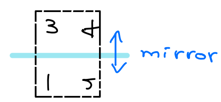
We want to remove this mattress from the frame, move it in some way, then fit it back into the frame. We're only interested in the net effect.

Four possible transformations:

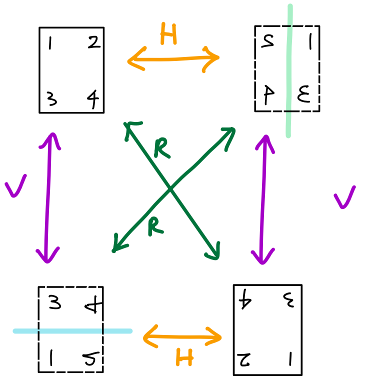
I. Do nothing (I for "Identity") 

R. Rotate by 180° ("up" surface stays the same, head becomes foot end) 

H. Horizontal flip ("up" surface is flipped, head end stays the same) 

V. Vertical flip ("up" surface is flipped, head becomes foot end) 

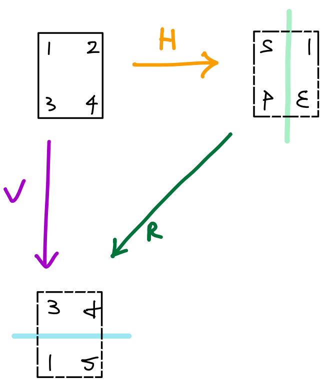
Visualize how these transformations relate to one another in a Cayley graph:



- The four vertices are the 4 states of the mattress
- Arrows are transformations

Remark

- Here all arrows are double-sided because doing R (or H or V) twice is the same as doing nothing (I).
- Instead of doing a vertical flip (harder in practice), you can do H and then R (or R then H) and achieve the same result.



Our textbook convention:
Read from right to left
like function composition

Here write $V = RH$ and say "the diagram commutes"

2-light switch group G_2

Starting state: both light switches are off ○○

Four possible transformations:

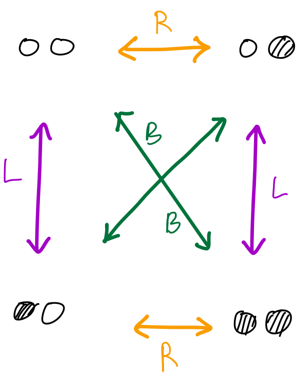
I. Do nothing ○○

R. Flip right switch ○●

L. Flip left switch ●○

B. Flip both switches ●●

Cayley diagram

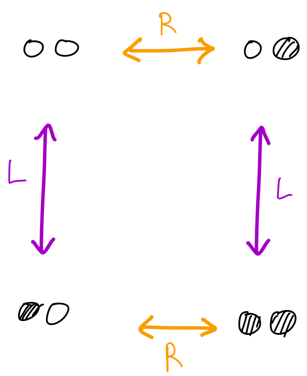


Remark

- The mattress group G_1 and 2-light switch group G_2 are superficially different, but they have the same structure (we say "G_1 and G_2 are isomorphic as groups")

- Any group w/ the same structure as G_1 and G_2 is called the Klein 4-group, denoted by V_4 because the word for four in German starts w/ "V".

- Since $B = RL$, we can get to all states using just R and L, so another possible Cayley diagram for G_2 is



$\boxed{\text{Exercise}}$ Consider a variation of the mattress group where the mattress is square.

Now you can also rotate by $90°$ and $270°$, and do more types of flips.

a) List all possible transformations.

b) Try to draw a Cayley diagram using just flips.

Groups: Sec 3.2 Def & Examples

Recall (See Sec 1.2)

The <u>Cartesian product</u> of sets A and B is a new set

$$A \times B = \{ \underbrace{(a,b)}_{\text{tuple or ordered pair}} : a \in A \text{ and } b \in B \}$$

<u>Rem</u> In general $A \times B \neq B \times A$

Ex: $A = \{x, y\}$, $B = \{1,2,3\}$, $C = \varnothing$

$$A \times B = \{(x,1), (x,2), (x,3), (y,1), (y,2), (y,3)\}$$

$$A \times C = \varnothing = C \times A$$

<u>Def</u> Let S be a set.

A <u>binary operation</u> $*$ on S is a function

$$\begin{aligned} S \times S &\longrightarrow S \\ (a,b) &\longmapsto a * b \end{aligned}$$

Depending on the operation, we may write $*$ as

$+, \cdot, \circ$, or a different symbol, or no symbol at all.

Ex: (1) $+, -, \cdot$ are binary operations on $\mathbb{Z}$

(2) $\div$ is a binary operation on $\mathbb{Q} \setminus \{0\}$ and $\mathbb{R} \setminus \{0\}$

(3) $+$ is a binary operation on $\mathbb{N}$

(4) $-$ is not a binary operation on $\mathbb{N}$

(5) Matrix addition and matrix multiplication are binary operations on $Mat_n(\mathbb{R}) \stackrel{\text{def}}{=} \{n \times n \text{ matrices w/ real entries}\}$

(6) $a * b \stackrel{\text{def}}{=} a$ is a binary operation on $\mathbb{R}$

(7) $a * b \stackrel{\text{def}}{=} a + b + ab$ —"— on $\mathbb{R}$

Rem A binary operation is simply a method (or formula) for combining an ordered pair from S to yield a new elt of S.

This property is called closure

Below is an example for how to use this word in a sentence:

Claim $\div$ is not a binary operation on $\mathbb{Z}$.

Proof The set $\mathbb{Z}$ is not closed under the operation $\div$.
For example, $5 \div 4 \notin \mathbb{Z}$.

Def Let $*$ be a binary operation on S

① $*$ is called associative if

$$(a * b) * c = a * (b * c)$$

for all $a, b, c \in S$

German word for identity: Einheit

② An element $e \in S$ is called an identity element for $*$ if

$$e * a = a \quad \text{and} \quad a * e = a$$

for all $a \in S$

③ If e is an identity element for $*$ on S, and $a, b \in S$, and

$$a * b = e \quad \text{and} \quad b * a = e,$$

then b is called an inverse of a under $*$

④ $*$ is called commutative if

$$a * b = b * a$$

for all $a, b \in S$

Ex (1) $+$ on $\mathbb{Z}$

associative, commutative
has identity elt 0
Every $n \in \mathbb{Z}$ has inverse $-n$

(2) $\cdot$ on $\mathbb{Z}$

associative, commutative
has identity elt 1
The elt 1 has inverse 1
The elt -1 has inverse -1
No other $n \in \mathbb{Z}$ has an inverse

(3) $-$ on $\mathbb{Z}$

not associative, ex: $(5-1)-1=3$ but $5-(1-1)=5$

(4) $\cdot$ on $\mathbb{Q}\setminus\{0\}$

associative, commutative
has identity elt 1
Every $r \in \mathbb{Q}\setminus\{0\}$ has an inverse $\frac{1}{r}$

(5) $\div$ on $\mathbb{Q}$

not associative, ex: $(30 \div 5) \div 2 = 3$ but $30 \div (5 \div 2) = 12$

(6) $\cdot$ Matrix multp on $Mat_n(\mathbb{R})$

associative, not commutative when $n \geq 2$

identity is $\begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$, the identity matrix

$M \in Mat_n(\mathbb{R})$ has an inverse iff $\det(M) \neq 0$

We might refer to a group as G when the operation $\star$ is implicit

Def A group $(G, \star)$ is a set G w/ a binary operation $\star$ on G such that

1. $\star$ is associative
2. there is an identity elt e for $\star$
3. Each elt $a \in G$ has an inverse under $\star$.

Remark Identity and inverses are unique:

Prop Suppose $\star$ is an associative binary operation on a set S.

1. If there is an identity elt e for $\star$ in S, then e is unique.
2. If a has an inverse under $\star$, then this inverse is unique.

usual notation for inverse of a : a^{-1}

(when the binary operation is $+$, we might write the inverse of a as $-a$, not a^{-1})

Proof ① Prove / read text (Prop 3.17)

② Suppose b and c are inverses of a under $\star$.

Then $ab = ba = e$ and $ac = ca = e$.

(We want to show $b = c$)

since $\star$ is associative

$$b = be = b(ac) = (ba)c = ec = c$$

by assumption above

since e is an identity elt

Prop ("Socks - shoes" property)

Let $(G, *)$ be a group, and $a, b \in G$.

① $(ab)^{-1} = b^{-1}a^{-1}$

② $(a^{-1})^{-1} = a$

Proof ① $ab(b^{-1}a^{-1}) = aea^{-1} = aa^{-1} = e$ and

similarly, $(b^{-1}a^{-1})ab = b^{-1}eb = b^{-1}b = e$,

So $b^{-1}a^{-1}$ is an inverse of ab.

But the previous proposition tells us that inverses are unique.

Hence $(ab)^{-1} = b^{-1}a^{-1}$!

② Prove / read text (Prop 3.20)

Def A group $(G, *)$ is called **abelian** (or commutative) if $*$ is commutative.

Ex of abelian groups

(1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are abelian groups under $+$

(2) $\{$Even integers$\}$ is an abelian group under $+$

(3) $\mathbb{Q}^{\times} = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^{\times} = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^{\times} = \mathbb{C} \setminus \{0\}$ are abelian groups under $\cdot$

(4) $\mathrm{Mat}_2(\mathbb{R})$ is an abelian group under matrix addition

(identity is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$)

$$GL_n(\mathbb{R}) \overset{\text{def}}{=} \{ M \in Mat_n(\mathbb{R}) : \underbrace{A \text{ is invertible}}_{\text{iff } \boxed{\det(M) \neq 0}} \}$$

is called the <u>general</u> <u>linear group</u> of degree n over $\mathbb{R}$

<u>Fact</u> $(GL_n(\mathbb{R}),$ matrix multp$)$ is a (non-abelian if $n \geqslant 2$) group.

<u>Proof that $GL_2(\mathbb{R})$ is a non-abelian group under matrix multiplication:</u>

- Proving closure:

  Matrix multp is a binary operation because if $A, B \in GL_2(\mathbb{R})$

  then $\det(A) \neq 0$ and $\det(B) \neq 0$,

  so $\det(AB) = (\det A)(\det B) \neq 0$

  Hence $AB \in GL_2(\mathbb{R})$.

- Proving properties of a group
  1. Matrix multiplication is associative
  2. $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity elt
  3. Each $M \in GL_n(\mathbb{R})$ has an inverse $M^{-1} \in GL_n(\mathbb{R})$.

- To prove that a binary operation is non-commutative, it is enough to find two elements which do not commute:

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \neq \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad \square$$

— the end —