

Document last updated Sep 11 2025

Abstract Algebra Notes

Day 1, Sep 9, 2025

Outline examples of groups (symmetries) Ch 1

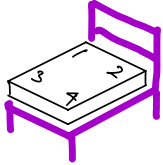
Group quiz 1

Groups: Def and examples Ch 2

Syllabus / Typesetting 01 (Overleaf.com)

* Break around 8 pm

The rectangle mattress group

Original position:  or

1	2
3	4

 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.

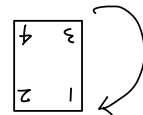
E.g: a 90° rotation and a $450^\circ = 360^\circ + 90^\circ$ rotation are considered equal.

Four possible transformations:

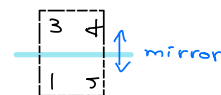
I. Do nothing (I for "Identity")

1	2
3	4

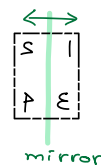
R. Rotate by 180° ("up" surface stays the same, head becomes foot end)



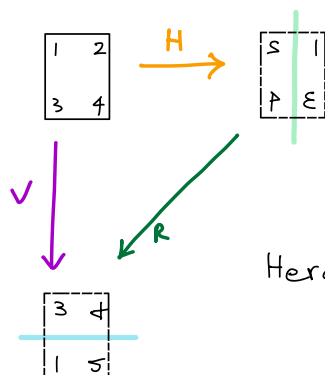
V. Vertical flip ("up" surface is flipped, head becomes foot end)



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



- 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

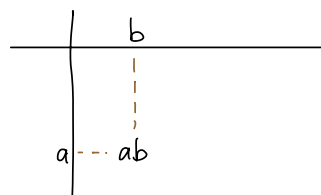
Here write $V = RH$

Operation table or Cayley table of the rectangle

mattress group.

\circ	I	H	V	R
I	I	H	V	R
H	H	I	R	V
V	V	R	I	H
R	R	V	H	I

Our convention is to read
row first & column second:



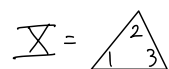
Symmetries

Def • A symmetry or rigid motion of a figure X in the plane \mathbb{R}^2 is a transformation $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ that carries X onto X and preserves distances (meaning distance between $f(p)$ and $f(q)$ is the same as the distance between p and q)
(see discussion on Ch 1 pg 34-36)

- Given a (plane) figure X , the set of all rigid motions together with composition \circ is called the symmetry group of X or the group of symmetries of X , denoted $\text{Symmetry}(X)$

Warning: not the symmetric group

Ex (Symmetry group of a regular triangle)



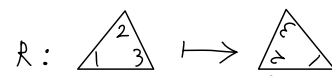
The labels are just to help us keep track

Six rigid motions / symmetries:

1) Identity

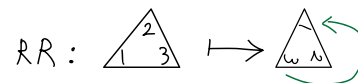
R_0

2) Counterclockwise rotation by $\frac{2\pi}{3}$



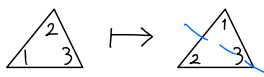
R_{120}

3) Counterclockwise rotation by $\frac{4\pi}{3}$

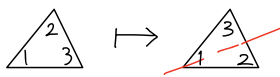


R_{240}

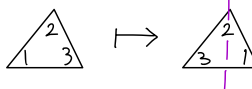
4) Negative slope mirror flip f_1 :



5) Positive slope mirror flip f_2 :



6) Vertical mirror flip f_3 :



(Start Group Quiz 1)

\circ	R_0	R_{120}	R_{240}	f_1	f_2	f_3
R_0	R_0	R_{120}	R_{240}	f_1	f_2	f_3
R_{120}	R_{120}	R_{240}	R_0	f_2	f_3	f_1
R_{240}	R_{240}	R_0	R_{120}	f_3	f_1	f_2
f_1	f_1	f_3	f_2	R_0	R_{240}	R_{120}
f_2	f_2	f_1	f_3	R_{120}	R_0	R_{240}
f_3	f_3	f_2	f_1	R_{240}	R_{120}	R_0


Def When X is a regular n -gon ($n \geq 3$),

Symmetry(X) is called the dihedral group D_n .

Prop D_n has $2n$ elements (rigid motions):

- n rotations: $\frac{2\pi}{n}, 2\frac{2\pi}{n}, \dots, (n-1)\frac{2\pi}{n}, 0$
- n flips

Ex • Above example is D_3 .

• Mercedes-Benz logo:  D_3

• Old Chrysler logo:  D_5

Shorthand:

"elt" means element

"iff" means if and only if

$$\mathbb{N} = \{n: n \text{ is a } \underline{\text{natural number}} \text{ (positive integer)}\} = \{1, 2, 3, \dots\}$$

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

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

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

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

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

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

Ch 2 Groups

The Cartesian product of sets A and B is a new set

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

Rem In general $A \times B \neq B \times A$

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

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

$$A \times C = \emptyset = C \times A$$

Def Let S be a set.

A binary operation $*$ 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 $\text{Mat}_n(\mathbb{R}) \stackrel{\text{def}}{=} \{n \times n \text{ matrices w/ real entries}\}$

(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 \star be a binary operation on S

① \star is called associative if

$$(a \star b) \star c = a \star (b \star c)$$

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

German word for identity: *Einheit*

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

$$e \star a = a \text{ and } a \star e = a$$

for all $a \in S$

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

$$a \star b = e \text{ and } b \star a = e,$$

then b is called an inverse of a under \star

④ \star is called commutative if

$$a \star b = b \star a$$

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 $5-(1-1)=5$

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

associative, commutative

has identity elt 1

Every $r \in \mathbb{Q} \setminus \{0\}$ has an inverse $\frac{1}{r}$

\rightarrow (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 $\text{Mat}_n(\mathbb{R})$

associative, not commutative when $n \geq 2$

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

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

Def A group (G, \star) is a set G together 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 .

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

Def

- A group (G, \star) is called abelian (or commutative) if $a \star b = b \star a$ for all $a, b \in G$.
- It is called non-abelian (or non-commutative) if there is some pair of elements a, b for which $ab \neq ba$.

Ex of abelian groups

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

(2) $\{\text{Even integers}\}$ 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 mult \times

(4) $\text{Mat}_2(\mathbb{R})$ is an abelian group under matrix addition
(identity is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$)

(5) "Square mattress group" (D_4) is not abelian.

(6) "Rectangle mattress group" (V_4) is abelian

2.2 Properties of groups

Remark Identity and inverses are unique:

Thm In a group, there is only one identity element (see Thm 2.1)

Pf Suppose both e and e' are identities of G .

Then, by def of identity, we have

1. $ae = a$ for all a in G , and

2. $e'a = a$ for all a in G .

Since e' is in G , (part 1) tells us $e'e = e'$.

Since e is in G , (part 2) tells us $e'e = e$.

Thus e and e' are both equal to $e'e$ and so $e = e'$. \square

Thm (see Thm 2.2 "right and left cancellation laws")

Let a, b, c be elts of a group G .

① (Right cancellation law) $\overset{\text{on the right}}{ba = ca}$ implies $b = c$

② (Left cancellation law) $ab = ac$ implies $b = c$

Pf ①
(done in class)

Suppose $ba = ca$. Let a' be an inverse of a .

Multiply on the right by a' : $(ba)a' = (ca)a'$

By associativity, we have $b(aa') = c(aa')$


Since $aa' = e$, we have $be = ce$

Thus $b = c$.

Remark The cancellation property tells us that, in a Cayley table for a group, every group elt occurs exactly once in each row and column.

Why?

Thm (see Thm 2.3)

Each element a in a group G has a unique inverse,
 meaning there is only one

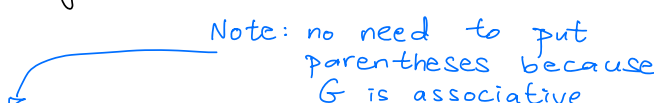
I.e. for each element a in G , there is a unique element b in G such that $ab = ba = e$.

Pf Exercise

Rem In view of the previous theorem, we can talk about "the inverse" of an element g in a group.

Notation : g^{-1}

Notation G group, $g \in G$, $n \in \mathbb{N}$

Write $g^n := \underbrace{g g \cdots g}_{n \text{ times}}$,


$$g^0 := e$$

$$g^{-n} := (g^{-1})^n = \underbrace{g^{-1} g^{-1} \cdots g^{-1}}_{n \text{ times}}$$

$$\text{Ex: } g^{-4} = (g^{-1})^4 = g^{-1} g^{-1} g^{-1} g^{-1}$$

Theorem: $g^m g^n = g^{m+n}$ and $(g^m)^n = g^{mn}$
(Laws of exponent)

Warning: in general $(ab)^n \neq a^n b^n$

Exception: When the group operation is $+$,

we write $-g$ for the inverse of g (instead of g^{-1})

$$ng := \underbrace{g + \dots + g}_{n \text{ times}},$$

$$0g := e$$

$$-ng := n(-g) = \underbrace{(-g) + (-g) + \dots + (-g)}_{n \text{ times}}$$

Thm ("socks - shoes" property) (see Thm 2.4)

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

$$\textcircled{1} (ab)^{-1} = b^{-1}a^{-1}$$

$$\textcircled{2} (a^{-1})^{-1} = a \quad (\text{see Ch 2 exercise 26})$$

Proof $\textcircled{1} (ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = ae a^{-1} = aa^{-1} = e,$

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

But a previous theorem tells us that inverses are unique.

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

$\textcircled{2}$ Exercise

Q: What would be an analogy for $(abc)^{-1} = c^{-1}b^{-1}a^{-1}$?

$$GL_n(\mathbb{R}) \stackrel{\text{def}}{=} \{ M \in \text{Mat}_n(\mathbb{R}) : \overbrace{M \text{ is invertible}}^{\det(M) \neq 0 \text{ iff}} \}$$

is called the general linear group of degree n over \mathbb{R}

Fact $(GL_n(\mathbb{R}), \text{matrix mult})$ is a (non-abelian) group.
if $n \geq 2$

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

• 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:

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

— end of doc —

