Document last updated Fri, Sep 13, 2024

# Abstract Algebra Notes
## Week 2 Wed, Sep 11, 2024

**Outline** ✱ Break before 8 pm

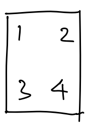
- Quiz 1
- If Blackboard doesn't say 100% for HW 01, you can make edit by Thurs & let me know
- Lecture:
  - symmetry group, symmetric group
  - groups from integers modulo n
  - Cayley table
  - New groups from old: Direct product, subgroup
- Group activity: problems for next week's HW & quiz

**Next week**

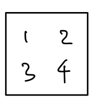
HW 02 Due Tues

Quiz @ start of class

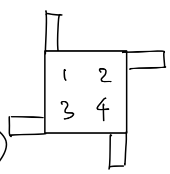
"Mattress groups"

rectangle (denoted $V_4$) 

: four transformations
- two rotations 0°, 180°
- two flips/reflections

square (denote $D_4$) 

: Eight transformations
- Rotations $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$
- four flips/reflections

Square w/ spikes (denote $\mathbb{Z}_4$) 

: Four rotations $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$

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

Write $g^n := \underbrace{g g \cdots g}_{n \text{ times}}$, $g^0 := e$

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

Exception: When the group operation is $+$,

we write $ng := \underbrace{g + \cdots + g}_{n \text{ times}}$, $0g := e$

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

Def The order of a group $G$, denoted by $|G|$, is the number of elts of $G$.

(Sec 3.2)

Def The order of an element $x$ of a group $G$, denoted by $|x|$, is the smallest positive integer $k$ such that $x^k = e$.

(Sec 4.1)

Ex: $|V_4| = 4$, $|D_4| = 8$

$|x| = 1$ iff $x = e$

$|\text{Rotation } 180°| = 2$, $|\text{Rotation } \frac{2\pi}{5}| = 5$

$|\text{Reflection}| = 2$

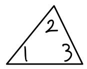
$\boxed{\text{Symmetries (see Sec 3.1 and 5.2)}}$

<u>Def</u> • A <u>symmetry</u> or <u>rigid motion</u> of a figure $\underline{X}$ in the plane $\mathbb{R}^2$ is a transformation $f: \mathbb{R}^2 \to \mathbb{R}^2$ that carries $\underline{X}$ onto $\underline{X}$ and preserves distances (meaning distance between $f(p)$ and $f(q)$ is the same as the distance between $p$ and $q$)

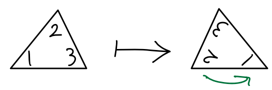
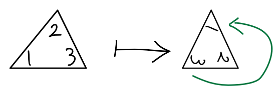
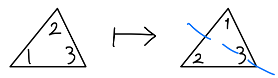
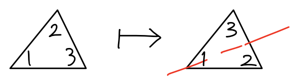
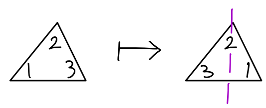
• If $\underline{X}$ is fixed, the set of all rigid motions together with composition $\circ$ is called the <u>symmetry group of $\underline{X}$</u>, $\text{Symmetry}(\underline{X})$

Warning: not the symmet<u>ric</u> group

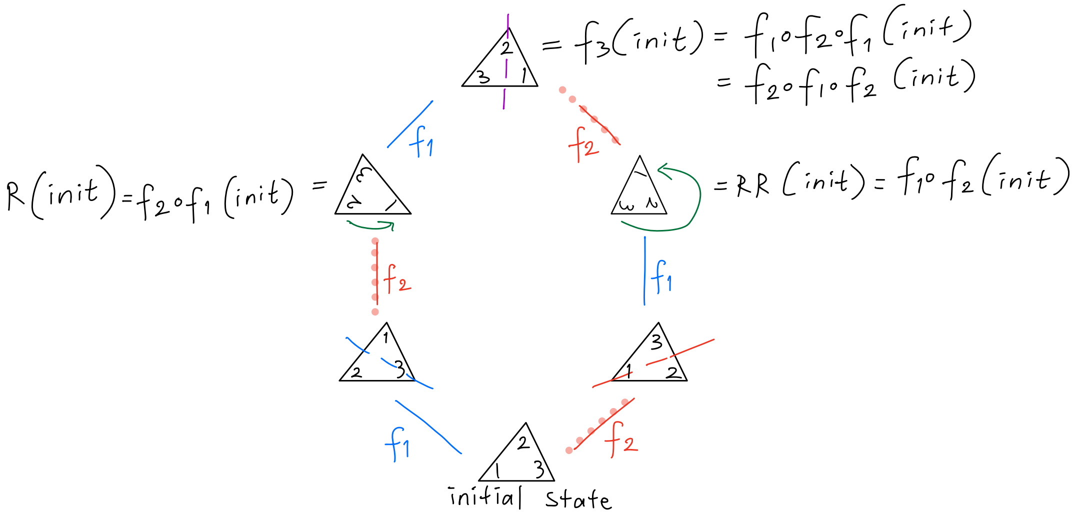
Ex (Symmetry group of a regular triangle)

$\underline{X} =$  The labels are just to help us keep track

Six rigid motions / symmetries:

1) Identity
2) Counterclockwise rotation by $\frac{2\pi}{3}$ $R$: 
3) Counterclockwise rotation by $\frac{4\pi}{3}$ $RR$: 
4) Negative slope mirror flip $f_1$: 
5) Positive slope mirror flip $f_2$: 
6) Vertical mirror flip $f_3$: 

Compositions of $f_1$ and $f_2$ give us all other motions:




- This is a Cayley diagram for $D_3$ using just $f_1, f_2$.
- An (unoriented) edge means double-sided arrow, since $f_1^2 = f_2^2 = id$

**Def** When $X$ is a regular n-gon $(n \geqslant 3)$, Symmetry$(X)$ is called the dihedral group $D_n$.

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

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

**Ex** Above example is $D_3$.

Each of the 6 bijections $\{1,2,3\} \to \{1,2,3\}$ gives rise to a symmetry in $D_3$.

## Symmetric group on n letters (Sec 5.1)

**Def** A permutation of the set $\{1, 2, \ldots, n\}$ is a bijection from $\{1, 2, \ldots, n\}$ onto itself.

The set of permutations of $\{1, 2, \ldots, n\}$ is denoted $S_n$.

**Thm** The set $S_n$ together with function composition forms a group, and $|S_n| = n!$

**Proof** Exercise

**Notation:** $S_n$ is called the symmetric group on $\{1, \ldots, n\}$

**Two-row notation** $\sigma = \begin{bmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{bmatrix}$

\sigma

**One-line notation** $\sigma = \sigma(1)\,\sigma(2) \cdots \sigma(n)$

**Cycle notation** write $(j, \sigma(j), \sigma^2(j) \cdots)(k, \sigma(k), \sigma^2(k), \ldots)$

Ex ($S_7$) $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 1 & 3 & 6 & 5 & 7 \end{bmatrix}$ two-row

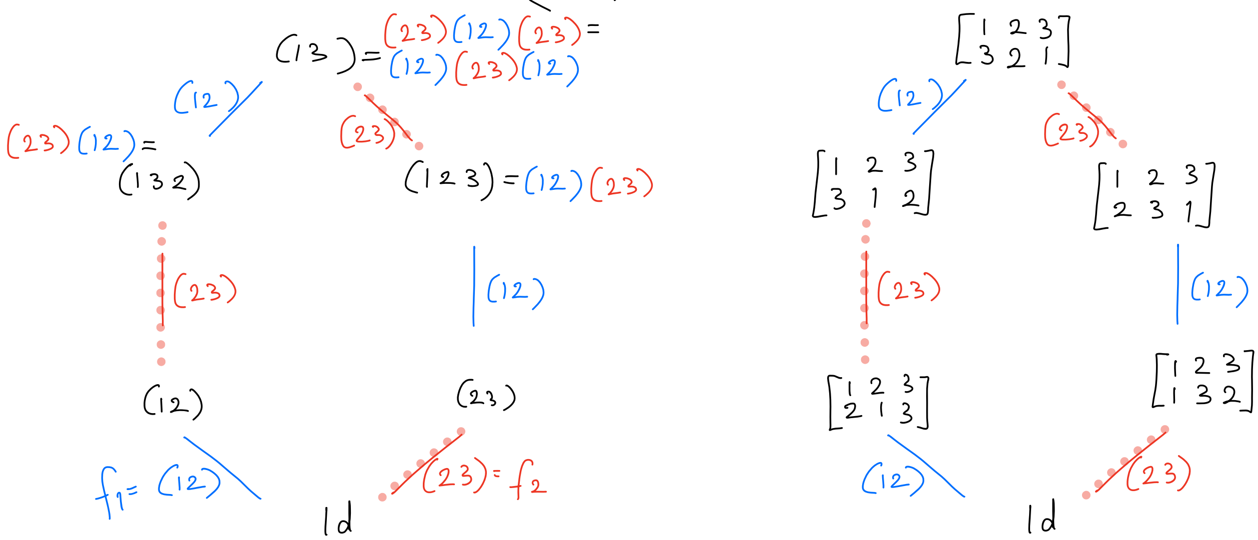
$\sigma = 2\ 4\ 1\ 3\ 6\ 5\ 7$ one-line

$\sigma = (1\ 2\ 3)(5\ 6)(7)$ or $(123)(56)$ cycle notation

if $\sigma(j) = j$, we don't need to write $j$ in cycle notation

A Cayley diagram for $S_3$ using just $(12)$ and $(23)$:

Compose right to left




Remark • $D_3$ and $S_3$ are "the same"

• In general, $D_n$ and $S_n$ are different because $|D_n| = 2n \neq n! = |S_n|$

Review equivalence relations & partitions (See Sec 1.2)
(extra notes)

Def A relation $R$ on a set $S$ is a subset of $S \times S$

Notation: write $xRy$ or $x \overset{R}{\sim} y$ instead of $(x,y) \in R$

Ex (a) $=$ is a relation on any set

Here $R = \{ (x,y) : x = y \}$

(b) $\neq$ is also a relation on any set

$R = \{ (x,y) : x \neq y \}$

(c) $\leq$ is a relation on $\mathbb{R}, \mathbb{Z}, \mathbb{Q}$ (also $<, \geq, >$)

$R = \{ (x,y) : x \leq y \}$

Def An equivalence relation on a set $S$ is a relation $\sim$ such that for all $x, y, z \in S$, we have:

1. $x \sim x$ (reflexive property)
2. if $x \sim y$ then $y \sim x$ (symmetric property)
3. if $x \sim y$ and $y \sim z$ then $x \sim z$ (transitive property)

Ex Which of these relations is an equivalence relation?

(a) $=$ ✓

(b) $\neq$ fails reflexive and transitive properties)

(c) $\leq$ fails (2)

(d) $<$ fails (1) and (2)

Ex Let $S = \{$ differentiable functions $f: \mathbb{R} \to \mathbb{R}\}$ (extra notes)

Define an equivalence relation on $S$ by

$$f \sim g$$

if $f' = g'$

Proof that $\sim$ satisfies properties 1 – 3:

1
2 } ✓

3 Suppose $f(x) \sim g(x)$ and $g(x) \sim h(x)$ \sim

Then $f'(x) = g'(x)$ and $g'(x) = h'(x)$.

From calculus we know that $f(x) - g(x) = C$ and $g(x) - h(x) = D$ for some constants $C, D$.

Then $f(x) - h(x) = f(x) - g(x) + g(x) - h(x)$

$$= C + D$$

So $f'(x) - h'(x) = (f-h)'(x) = 0$

Thus $f'(x) = h'(x)$, implying $f(x) \sim h(x)$

## Partitions

A partition $\mathcal{P}$ of a set $S$ is a collection of nonempty subsets

$X_1, X_2, X_3, \ldots$

such that each $x \in S$ is in exactly one of the subsets

Ex The partition of students for last week's group quiz

(extra notes)

**Ex** Some partitions of $\mathbb{Z}$

(a) A partition into two sets

$X_1 = \{2k+1 : k \in \mathbb{Z}\}$ odds

$X_2 = \{2k : k \in \mathbb{Z}\}$ evens

(b) A partition into three sets

$X_1 = \{3k+1 : k \in \mathbb{Z}\}$

$X_2 = \{3k+2 : k \in \mathbb{Z}\}$

$X_3 = \{3k : k \in \mathbb{Z}\}$

(c) A partition into infinitely many sets

$X_0 = \{0\}, \; X_1 = \{1,-1\}, \; X_2 = \{2,-2\}, \ldots, \; X_i = \{i,-i\}, \ldots$

**Def** Let $\sim$ be an equivalence relation on a set $S$, and $a \in S$.

Define the equivalence class of $a$ to be

$$[a] = \{ b \in S : b \sim a \}$$

Defining an equivalence relation on $S$ is "the same" as defining a partition on $S$ :

**Thm** • If $\sim$ is an equivalence relation on $S$, then the equivalence classes partition $S$.

• Conversely, if $\mathcal{P} = \{X_i\}_{i \in I}$ is a partition of $S$, then there is an equivalence relation on $S$ with equivalence classes $X_i$.

## Integers modulo n (see Sec 3.1)

Recall Def:

Let $n \in \mathbb{N}$. Integers $a, b \in \mathbb{Z}$ are <u>congruent modulo n</u> (or a is <u>congruent to</u> b mod n) if

$$n \mid (b-a),$$

that is, $b - a = nk$ for some $k \in \mathbb{Z}$.

Notation: $a \equiv b \pmod{n}$

This is an equivalence relation on $\mathbb{Z}$.

$a \in [b]$ iff $a \equiv b \pmod{n}$ iff $[a] = [b]$

When $n=2$: there are two equivalence classes

$$\{\ldots, -2, 0, 2, 4, \ldots\} = [0] = [4]$$

and $$\{\ldots, -1, 1, 3, 5, \ldots\} = [1] = [57]$$

When $n=3$: there are three equivalence classes

$$\{\ldots, -3, 0, 3, 6, 9, \ldots\} = [0] = [123]$$

$$\{\ldots, -2, 1, 4, 7, 10, \ldots\} = [1] = [7]$$

$$\{\ldots, -1, 2, 5, 8, 11, \ldots\} = [2] = [8]$$

<u>Def</u> Let $\mathbb{Z}_n$ be the set of all equivalence classes.
integers mod n

$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ or $\{0, 1, \ldots, n-1\}$ when the context is clear

Alternative notation: $\mathbb{Z}/n$, $\mathbb{Z}/n\mathbb{Z}$ (will make sense in Ch 6)

**Def** Two binary operations on $\mathbb{Z}_n$:

① Addition modulo n $\quad [a]+[b] \overset{\text{def}}{=} [a+b]$

② Multiplication modulo n $\quad [a]\cdot[b] \overset{\text{def}}{=} [ab]$

**Remark** Both are well-defined, meaning that the def doesn't depend on your choice of representative of the class.

That is, we need to show that:

if $[a]=[a']$ and $[b]=[b']$, then

① $[a]+[b]=[a']+[b']$ and

② $[a]\cdot[b]=[a']\cdot[b']$

To show these, recall that

$$\left.\begin{array}{l} \text{if } a\equiv a' \pmod n \text{ and } b\equiv b' \pmod n \text{ then} \\ ① \ a+b\equiv a'+b' \pmod n \\ ② \ a\cdot b\equiv a'\cdot b' \pmod n \end{array}\right\} \text{(proposition)}$$

So, if $[a]=[a']$ and $[b]=[b']$, then

① $[a]+[b] \overset{\text{def}}{=} [a+b] \overset{\text{prop}}{=} [a'+b'] \overset{\text{def}}{=} [a']+[b']$

② $[a]\cdot[b] \overset{\text{def}}{=} [a\cdot b] \overset{\text{prop}}{=} [a'\cdot b'] \overset{\text{def}}{=} [a']\cdot[b']$

**Prop** $(\mathbb{Z}_n, +)$ is an abelian group:

1. $+$ is associative
2. $[0]$ is the identity
3. The inverse of $[a]$ is $[-a]$
4. Addition modulo $n$ is commutative

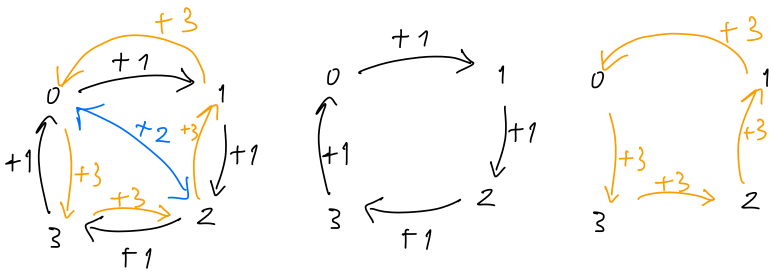
**Ex** The group $\mathbb{Z}_4 = \{0,1,2,3\}$ under $+$ can be described in an operation table (called Cayley table for group)

| + | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

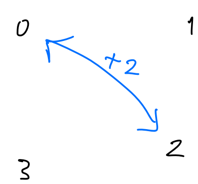
main diagonal

**Remark** The Cayley table is symmetric across the main diagonal. This tells us $(\mathbb{Z}_4, +)$ is abelian.

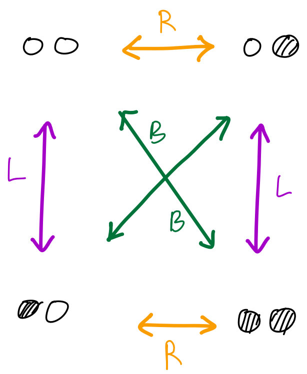
Cayley graphs for $(\mathbb{Z}_4, +)$:




NOT a Cayley graph:



Back to the 2-light switch group $G$




$e :=$ do nothing transformation

Table for $(G, \star)$

| $\star$ | $e$ | $R$ | $L$ | $B$ |
|---|---|---|---|---|
| $e$ | $e$ | $R$ | $L$ | $B$ |
| $R$ | $R$ | $e$ | $B$ | $L$ |
| $L$ | $L$ | $B$ | $e$ | $R$ |
| $B$ | $B$ | $L$ | $R$ | $e$ |

Remark From the tables, we see that $(\mathbb{Z}_4, +)$ and $(G, \star)$ have "different structure" (for ex, see main diagonal)

So $G$ is not the Klein 4-group

**Prop** Multiplication modulo $n$ is an associative binary operation w/ identity $[1]$.

**Ex** Operation table for $\mathbb{Z}_4$ under $\cdot$ is below.

| $\cdot$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

Note: No 1 in these rows, meaning 0 and 2 have no inverses

**Remark** $(\mathbb{Z}_n, \cdot)$ is not a group because not all elts have inverses.

Define $U(n) := \{ [a] \in \mathbb{Z}_n \mid [a] \text{ has an inverse under } \cdot \}$ to be the group of units of $\mathbb{Z}_n$

units mean invertible elements

**Prop** $U(n)$ is equal to $\{[a] \in \mathbb{Z}_n \mid a \text{ and } n \text{ are relatively prime}\}$

**Proof** Textbook Prop 3.4(6)

**Ex** Cayley table for $U(4) = \{1, 3\}$ under $\cdot$

| $\cdot$ | 1 | 3 |
|---|---|---|
| 1 | 1 | 3 |
| 3 | 3 | 1 |

(extra notes)

## From Week 2 Practice Problems

<u>Prop 3.21</u> Let $a, b$ be elts of a group $G$.

① The equation $ax = b$ has a unique solution in $G$

② The equation $xa = b$ has a unique solution in $G$

<u>Prop 3.22</u> Let $a, b, c$ be elts of a group $G$.

① (Right cancellation law) $ba = ca$ implies $b = c$

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

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

## New groups from old

See Textbook Example 3.28

**Direct product** of groups $(G, *)$ and $(H, \cdot)$ is

a new group w/

set: $G \times H = \{ (g,h) : g \in G, h \in H \}$

Cartesian product

binary operation: $(g,h) * (g', h') = (g * g', h \cdot h')$

Identity: $(e_G, e_H)$

Inverse of $(g,h)$ is $(g^{-1}, h^{-1})$

Ex Write the Cayley table for $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{ (0,0), (0,1), (0,2), (1,0), (1,1), (1,2) \}$

| | (0,0) | (0,1) | (0,2) | (1,0) | (1,1) | (1,2) |
|---|---|---|---|---|---|---|
| (0,0) | (0,0) | (0,1) | (0,2) | (1,0) | (1,1) | (1,2) |
| (0,1) | (0,1) | (0,2) | (0,0) | (1,1) | (1,2) | (1,0) |
| (0,2) | (0,2) | (0,0) | (0,1) | (1,2) | (1,0) | (1,1) |
| (1,0) | (1,0) | (1,1) | (1,2) | (0,0) | (0,1) | (0,2) |
| (1,1) | (1,1) | (1,2) | (1,0) | (0,1) | (0,2) | (0,0) |
| (1,2) | (1,2) | (1,0) | (1,1) | (0,2) | (0,0) | (0,1) |

## Sec 3.3 Subgroups

**Def** $G$ group.

A <u>subgroup</u> of $G$ is a subset $H \subseteq G$ which is also a group under the same binary operation.

Notation: $H \leq G$ means $H$ is a subgroup of $G$

\leq

Some propositions for checking subgroups.

**Prop** A subset $H$ of $G$ is a subgroup iff all three conditions hold:

use this

1. The identity $e$ of $G$ is in $H$
2. If $h_1, h_2 \in H$ then $h_1 h_2 \in H$
   (H is closed under the group operation)
3. If $h \in H$, then $h^{-1} \in H$.

**Prop** A subset $H$ of $G$ is a subgroup iff all two conditions hold:

1. $H$ is not empty
2. If $g, h \in H$ then $gh^{-1} \in H$.

<u>Ex</u> Find all subgroups of $G = \mathbb{Z}_2 \times \mathbb{Z}_3$

$$G = \{ (0,0),\ (0,1),\ (0,2),\ (1,0),\ (1,1),\ (1,2) \}$$

$$\begin{tikzcd}[column sep=small]
 & G \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Z}_2 \times \{0\} \arrow[dr, dash] & & \mathbb{Z}_3 \times \{0\} \arrow[dl, dash] \\
 & \{e\} = \{(0,0)\} &
\end{tikzcd}$$