Document last updated Tue, Sep 16, 2025

Abstract Algebra Notes

Day 2 Tue, 9/16/25 "Pythagorean Triple" Day!

Outline * Break before 8 pm

- Present HW
- Quiz 1
- Lecture: groups from integers modulo n
  - Ch 3 subgroup, generators
  - Ch 30 Cayley diagrams
- Group activity: problems for next week's HW & quiz

TODO
Fri: TP 2 Overleaf
Next Tue: HW02 Due in class
Study for Quiz 2: Quiz @ start of class

Integers modulo n

(Ch 0 pg 6)

What month will it be 1 month from now?
12 months from now? 25 months from now?

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 divides $(b-a)$,

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

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

Denote $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$.
integers mod n

Ch 2 Example 7 pg 44

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

$(\mathbb{Z}_n, +)$ is also denoted by $\mathbb{Z}_n$ for short

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.

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.

See Ch 2 Example 11 (pg 46)

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 $\{ a \in \mathbb{Z}_n \mid a \text{ and } n \text{ are relatively prime} \}$

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

$\cdot$	1	3
1	1	3
3	3	1

Ch 3 Finite groups ; Subgroups

I. Terminology & notation

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

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

If $x^k \neq e$ for every positive integer k, then x has infinite order

Ex: $|$Rectangle mattress group$| = 4$, $|D_4| = 8$

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

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

$|$Reflection$| = 2$

Ex Order of $(\mathbb{Z}_4, +)$ is 4

order of 0 : 1 $\quad 0 = 0$

1 : 4 (because $\underbrace{1+1+1+1}_{4 \text{ is the smallest}} = 0$)

2 : 2 (because $2+2=0$)

3 : 2 (because $3+3+3+3=0$)

II Subgroup Test

__Def__ G group. A __subgroup__ of G is a subset $H \subseteq G$ which is also a group under the same binary operation.

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

Prop (Subgroup Test) Let H be a subset of a group G.

Suppose H satisfies all 3 conditions:

① H is nonempty
(for example, show e 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 $h^{-1} \in H$.
(H is closed under taking inverses)

Then H is a subgroup of G.

Ex: Suppose G is an abelian group.

Let $H = \{x \in G \mid x^2 = e\}$

Prove that $H \leq G$

__Proof__ ① $e^2 = e$ by def of identity so $e \in H$

② Assume $a, b \in H$. Then $a^2 = e$ and $b^2 = e$.

Then $(ab)(ab) = a(ba)b$

$= a(ab)b$ since G is abelian

$= (aa)(bb)$

$= e\ e$ since $a^2 = e$ and $b^2 = e$

$= e$

So $ab \in H$

③ Suppose $a \in H$. Then $a^2 = e$, so $a^{-1} = a \in H$. $\boxtimes$

III. Cyclic groups

Def G group, $x \in G$

$\langle x \rangle \stackrel{\text{def}}{=} \{ x^k : k \in \mathbb{Z} \}$

If the group operation is additive, write $\langle x \rangle = \{ kx : k \in \mathbb{Z} \}$

Ex $G = \mathbb{Z}$, $\langle 1 \rangle = \mathbb{Z} = \langle -1 \rangle$,

$\langle 5 \rangle = \{ 5k : k \in \mathbb{Z} \} = \langle -5 \rangle$

$G = \mathbb{Z}_8$, $\langle 1 \rangle = \mathbb{Z}_8 = \langle 3 \rangle$

$\langle 2 \rangle = \{0, 2, 4, 6\}$

$\langle 4 \rangle = \{0, 4\}$

$G = U(10)$ $\langle 1 \rangle = \{1\}$

$\langle 3 \rangle = \{1, 3, 7, 9\} = G$

$\langle 7 \rangle = \{1, 3, 7, 9\} = G$

$\langle 9 \rangle = \{1, 9\}$

Thm $\langle x \rangle$ is a subgroup of G (Thm 3.4)

Pf ① $e = x^0 \in \langle x \rangle$

② If $y, z \in \langle x \rangle$, then $y = x^m$ and $z = x^n$ for some $m, n \in \mathbb{Z}$

Thus $yz = x^m x^n = x^{m+n}$, by Exponent law

so $yz \in \langle x \rangle$

③ If $y \in \langle x \rangle$, then $y = x^m$ for some $m \in \mathbb{Z}$

Then $y^{-1} = (x^m)^{-1} = x^{-m}$ by Exponent law

so $y^{-1} \in \langle x \rangle$.

Thus $\langle x \rangle \leq G$. $\square$

Def $\langle x \rangle$ is called the cyclic subgroup of G generated by x.

Def A group G is called a cyclic group if $G = \langle x \rangle$ for some $x \in G$, and x is called a generator of G.

Ex $\mathbb{Z}$ is cyclic, 1 is a generator.
-1 is also a generator

$\langle 1 \rangle = \mathbb{Z} = \langle -1 \rangle$

Ex $\mathbb{Z}_{12}$ is cyclic, 1 is a generator.
Other possible generators are $5, 7, 11$

In fact, every $\mathbb{Z}_n$ is cyclic.

Ex $U(8)$ is not cyclic. We see that $\langle x \rangle \neq U(8)$ for all $x \in U(8)$.

$\langle 1 \rangle = \{1\}$ $\quad$ $\langle 5 \rangle = \{1, 5\}$

$\langle 3 \rangle = \{1, 3\}$ $\quad$ $\langle 7 \rangle = \{1, 7\}$

(extra)

Thm $\langle x \rangle$ is the smallest subgroup of G containing x, meaning: if $H \leq G$ and $x \in H$ then $\langle x \rangle \leq H$.

Proof Suppose $x \in H$ for some subgroup $H \leq G$.

We need to show $x^k \in H$ for all $k \in \mathbb{Z}$.

$k=0$: $x^0 = e \in H$ (by requirement that H contains the identity)

$k \in \mathbb{N}$: $x^k = \underbrace{x\, x \cdots x}_{k \text{ times}} \in H$ (since H is closed under the group operation)

$k=-1$: $x^{-1} \in H$ (since H contains the inverse of each $h \in H$)

$k \in \mathbb{Z}_{\leq -1}$: $x^{-k} = (a^{-1})^k = \underbrace{a^{-1} \cdots a^{-1}}_{k} \in H$ (again by closure)

Therefore $\langle x \rangle = \{x^k : k \in \mathbb{Z}\} \leq H$. $\square$

Generators and Cayley diagrams

Ch 30 pg 482

Def Let G be a group, and let S be a subset of G.
We say that S is a generating set of G
(or S is a set of generators for G)
if every elt in G is a finite product of
elts in S and their inverses. Notation: $G = \langle S \rangle$

Ex $D_n = \langle \mathrm{Rot}\left(\frac{2\pi}{n}\right), f \rangle$ where f is any specific flip.

Ex $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle = \langle 2,3 \rangle = \langle 7, 12 \rangle = \langle 2,3,5 \rangle$

Def S is called minimal if no proper subset of S

different than minimum

is a generating set of G.

Ex $\{2,3\}, \{2,3,5\}, \{1\}$ are all generating sets of $\mathbb{Z}$.
$\{2,3\}$ and $\{1\}$ are both minimal, and $\{2,3,5\}$ is not minimal.

Def Given a group G and a set of generators S, a <u>Cayley diagram</u> (or Cayley graph) consists of

1. vertices : all elts of G

2. colored (or labeled) arrows : all elts in generating set S

* Write $x \xrightarrow{h} y$ iff $xh = y$ for some $h \in S$

(applying arrow h means multiplying on the right)

<u>Note</u> Following an h-arrow backwards means multiplying on the right by h^{-1}:

$$x \xrightarrow{h} y \quad \text{means} \quad y h^{-1} = x$$

* If, in addition, h is its own inverse, then we have $xh = y$ iff $x = xhh = yh$

$$\begin{tikzcd} x \arrow[r, shift left, "h"] & y \arrow[l, shift left, "h"] \end{tikzcd} \quad \text{or} \quad \begin{tikzcd} x \arrow[r, leftrightarrow, "h"] & y \end{tikzcd}$$

Our convention is to drop the tips on all these two-way arrows: $\begin{tikzcd} x \arrow[r, dash, "h"] & y \end{tikzcd}$

<u>Ex</u> $U(9) = \{1, 2, 4, 5, 7, 8\}$ is cyclic.

2 is a generator:

$$\begin{tikzcd} 1 \arrow[r, "\times 2"] & 2 \arrow[r, "\times 2"] & 4 \arrow[r, "\times 2"] & 8 \arrow[r, "\times 2"] & 7 \arrow[r, "\times 2"] & 5 \arrow[lllll, bend left, "\times 2"] \end{tikzcd}$$

This is the Cayley graph for $G = U(9)$ with generating set $S = \{2\}$

<u>Fact / Def</u> Any cyclic group $\langle x \rangle$ has Cayley graph

$$\begin{tikzcd} e \arrow[r, "x"] & x \arrow[r, "x"] & x^2 \arrow[r, "x"] & x^3 \arrow[r] & \cdots \; x^{n-1} \arrow[llll, bend left, "x"] \end{tikzcd}$$ if $\underbrace{|x|}_{\text{"order of } x\text{"}} = n$

and

$$\cdots \longrightarrow x^{-1} \xrightarrow{x} e \xrightarrow{x} x \xrightarrow{x} x^2 \xrightarrow{x} x^3 \longrightarrow \cdots$$ if x has infinite order

<u>Ex</u> $\mathbb{Z}_4 = \langle 1 \rangle$

$$\begin{tikzcd} 0 \arrow[r, "+1"] & 1 \arrow[r, "+1"] & 2 \arrow[r, "+1"] & 3 \arrow[lll, bend left, "+1"] \end{tikzcd}$$

<u>Ex</u> $\mathbb{Z}_n = \langle 1 \rangle$

$$\begin{tikzcd} 0 \arrow[r, "+1"] & 1 \arrow[r, "+1"] & \cdots \arrow[r, "+1"] & n-1 \arrow[lll, bend left] \end{tikzcd}$$

<u>Ex</u> $\mathbb{Z} = \langle 1 \rangle$ $\quad \cdots \rightarrow -2 \xrightarrow{+1} -1 \xrightarrow{+1} 0 \xrightarrow{+1} 1 \xrightarrow{+1} 2 \xrightarrow{+1} 3 \rightarrow \cdots$

<u>Remark</u>

- If $|x| = n$, $\langle x \rangle$ has a Cayley graph that is the same as a Cayley graph of $\mathbb{Z}_n$, so $\langle x \rangle$ is "the same" as $\mathbb{Z}_n$.

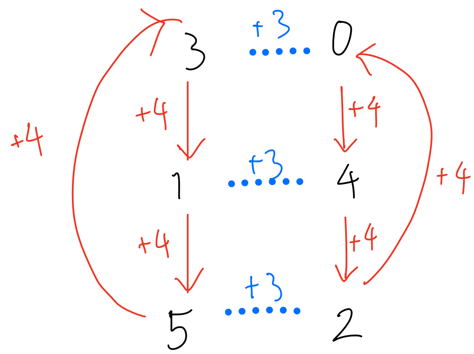
- If $|x| = \infty$, $\langle x \rangle$ has a Cayley graph that is the same as a Cayley graph of $\mathbb{Z}$, so $\langle x \rangle$ is "the same" as $\mathbb{Z}$.

- Properties about $\mathbb{Z}_n$ and $\mathbb{Z}$ hold for any cyclic group

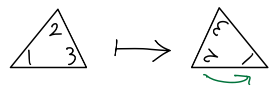
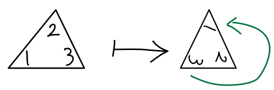
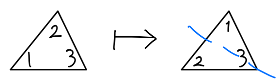
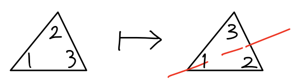
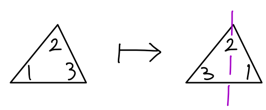
Ex Even though $\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle$, it has minimal generating set $S = \langle 3, 4 \rangle$

The Cayley diagram for generating set $\{3, 4\}$ of

$$\mathbb{Z}_6 = \langle \underset{\cdots\cdots}{\overset{f}{3}}, \underset{\longrightarrow}{\overset{R}{4}} \rangle \text{ is}$$

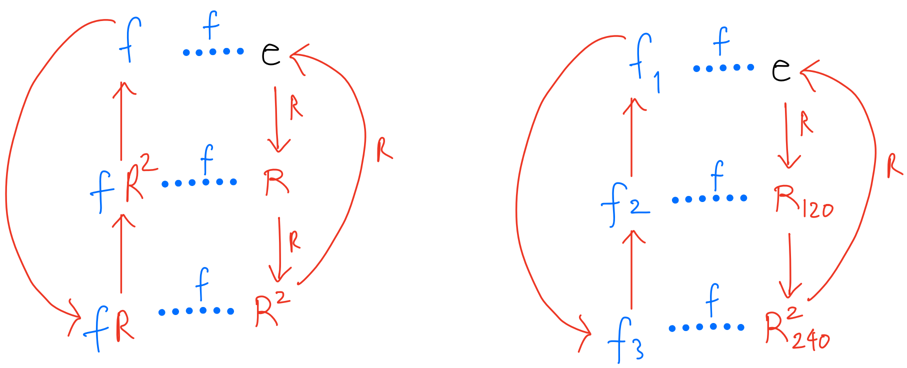


Ex Six rigid motions / symmetries:

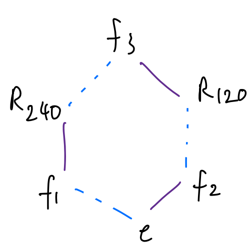
1) Identity $\qquad R_0$
2) Counterclockwise rotation by $\frac{2\pi}{3}$ R:  $\qquad R_{120}$
3) Counterclockwise rotation by $\frac{4\pi}{3}$ RR:  $\qquad R_{240}$
4) Negative slope mirror flip f_1: 
5) Positive slope mirror flip f_2: 
6) Vertical mirror flip f_3: 

$\circ$	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

The Cayley diagram for generating set $S = \{f = f_1, R = R_{120}\}$ of $D_3 = \langle f, R \rangle$ is below:



Exercise: The Cayley diagram for generating set $\{f_1, f_2\}$ of D_3 is below:



— end of PDF —