Real Analysis

Carter Aitken

2025-05-05

Abstract

We're studying abstract algebra, specifically groups and rings.

Contents

1 Operations on Sets

1.1 K-Ary Operations

- $\mathbb{N} \quad +, \cdot$
- $\mathbb{Z} \quad +, \cdot, -$
- $\mathbb{Q} \quad +, \cdot, -$
- $\mathbb{R} \quad +, \cdot, -$
- $\mathbb{C} \quad +, \cdot, -, x \mapsto \overline{x}, x \mapsto \sqrt{x}$
- $(\text{Vectors}) \quad +, (\text{scalarmul})$
- $(\text{Matricies}) \quad +, (\text{scalarmul}), (\text{matrixmul})$
- $(\text{polynomials}) \quad +, \cdot$

In abstract algebra, we're iinterested in what notions of ”numbers” exists.

The different ”types” of numbers really are distinguished by the operations on them. In this class we'll stick with operating on sets.

Definition 1.1: Binary Operations. *A* ***binary operation*** *on a set X is a function $b : X \times X \to X$.*

Note: we often write binary operators inline (like in Haskell).

We could use $+, \cdot, \times, \div, \otimes, \boxtimes, \oplus, \boxplus, \diamond$

```
FIND \gop in the .tex file to change the operator used.
/\\newcommand{\\gop}
```

Definition 1.2. *a* ***k-ary operator*** *on X is a func $f : \underbrace{X \times \cdots \times X}_{k} \to X$.*

$x \mapsto \frac{1}{x}$ on $\mathbb{Q}$ isn't a unary operation b/c $\frac{1}{0}$ isn't defined.
$\mathbb{Q}^{\times} = \{x \in \mathbb{Q} : x \neq 0\}$ does have the reciprocal as a binary operator, but not minus.

1.2 Associative Operations

Definition 1.3. *a binary operator $\boxtimes$ on X is* ***associative*** *if*

$$x \boxtimes (y \boxtimes z) = (x \boxtimes y) \boxtimes z, \quad \forall x, y, z \in X$$

$+, \cdot$ on $\mathbb{N}, \mathbb{Z}$ are associative. $- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ isn't associative. Neither is $\div : \mathbb{Q}^\times \times \mathbb{Q}^\times \to \mathbb{Q}^\times$. Function composition is associative.

Definition 1.4: (Informal) Bracketing. *Let $\boxtimes$ be a bin operator on a set X. A* ***bracketing*** *of a seq $a_1, \dots, a_n \in X$ is a way of inserting brackets into*

$$a_1 \boxtimes \cdots \boxtimes a_n \text{ s/t the expression can be evaluated}$$

Definition 1.5: Bracketing. *A* ***bracket*** *of $a_1, \dots, a_n$ is*

$$\begin{aligned} n = 1 &: \text{(word) } a_1 \\ n > 1 &: (w_1 \boxtimes w_2) \textit{ where} \\ &\quad w_1 \text{is(bracket) } \textit{of } a_1, \dots a_k \\ &\quad w_2 \text{is(bracket) } \textit{of } a_{k+1}, \dots, a_n \end{aligned}$$

```
data Bracket t = Number t | Branch (Bracket t) (Bracket t)
evalBracket :: (t -> t -> t) -> Bracket t -> t
evalBracket fn aseq =
  case aseq of
    Number x              -> x
    Branch left' right' -> fn (evalBracket fn left')
                                (evalBracket fn right')
```

Proposition 1.1. *a binary operation $\boxtimes$ on X is associative* ***iff*** *for every seq $a_1, \dots, a_n$, $n \geq 1$, every bracketing of $a_1, \dots a_n$ evaluates to the same elem of X.*

Proof. ($\Longleftarrow$) Take $n = 3$. Then

$$(a \boxtimes b) \boxtimes c = a \boxtimes (b \boxtimes c),\ \forall a, b, c \in X$$

($\implies$) Proof by induction.
Base Case: $n = 1$. Every bracketing of a word evaluates to that same word.
Assume proposition is true for $n < k$, where $k > 1$. Let $a_1, \cdots, a_k \in X$. If w is a bracketing of $a_1, \ldots, a_k$ then $w = (w_1 \boxtimes w_2)$, where w_1 is a bracketing of $a_1, \ldots, a_l$ and w_2 is a bracketing of $a_{l+1}, \ldots, a_k$.

$$w_1 = (\cdots (a_1 \boxtimes a_2) \boxtimes \cdots) \boxtimes a_l$$

$$w_2 = (a_{l+1} \boxtimes (\cdots (a_{k-1} \boxtimes a_k) \cdots))$$

$$\begin{aligned} w &\overset{\text{in } X}{=} w_1 \boxtimes w_2 \\ &= (A \boxtimes a_l) \boxtimes w_2 \\ &= A \boxtimes (a_l \boxtimes w_2) \text{ by assoc.} \\ \cdots &= a_1 \boxtimes (\cdots (a_{k-1} \boxtimes a_k) \cdots) \end{aligned}$$

Hence any 2 bracketings of $a_1, \ldots, a_k$ evaluate to $a_1 \boxtimes (\cdots (a_{k-1} \boxtimes x_k) \cdots)$. By induction, the prop holds. □

Notation 1.1: Associativity makes Brackets Pointless. *Since $\boxtimes$ is associative, brackets become redundant.* $a \boxtimes b \boxtimes c := a \boxtimes (b \boxtimes c)$

Definition 1.6: Commutative. $(\boxtimes) : X \times X \to X$ *is **commutative** (or "abelian") if*

$$a \boxtimes b = b \boxtimes a, \forall a, b \in X$$

$+, \cdot$ on $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}$ are commutative.

$+$ on $M_{n \times m}$is(comm). (matrix mul) on M_n $\not$is(comm).

We're much more focused on associative operators as opposed to commutative.
We cover 2 Topics:

1. **Group Theory:** a single associative op w/ some additional properties

2. **Ring Theory:** 2 associative op that behave "like" $+$ & $\cdot$.

Definition 1.7: Identity. *An identity for a given bin op* $\boxtimes$ *is a element* $e \in X$ *s/t* $e \boxtimes x = x \boxtimes e = x$, $\forall x \in X$.

0 is an identity for $+$ on $\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \cdots$. 1 is an identity for $\cdot$ on $\mathbb{Q}$

Lemma 1.1: Uniqueness of Identity. *If* e *and* e' *are identities for* $\boxtimes$ *on* X*, then* $e = e'$.

Proof. $e = e \boxtimes e' = e'$ □

Definition 1.8: Inverse. *let* $\boxtimes$ *be a bin op on* X *with iden* e*. Let* $x \in X$*.* $y \in X$ *is a*

1. ***left inverse*** *for* X *if* $y \boxtimes x = e$*,*
2. ***right inverse*** *for* X *if* $x \boxtimes y = e$*,*
3. *and an* ***inverse*** *for* X *if* $x \boxtimes y = e = y \boxtimes x$*.*

Lemma 1.2: Associtivity implies Uniqueness of Inverses. *Suppose we have* $(\boxtimes)\text{is}(\text{assoc})$*. If* y_L *and* y_R *are left and right inverses of* x*, then* $y_L = y_R$.

Proof.

$$\begin{aligned}(y_L \boxtimes x) \boxtimes y_R &= e \boxtimes y_R \\ &= y_R \\ (y_L \boxtimes x) \boxtimes y_R &= y_L \boxtimes (x \boxtimes y_R) \quad \text{(by assoc)} \\ &= y_L \boxtimes e \\ &= y_L\end{aligned}$$

□

Consequences: x is invertable **iff** it has a left and right inverse.

Note: is is possible to be left invertable but not right invertable, and vice verse.

$\mathbb{N} = \{1, 2, \dots\}, +$ has no invertable elements.

$(\mathbb{Z}, +)$ has every element invertable.

$(\mathbb{Z}, \cdot)$ has only $\{\pm 1\}$ as invertable.

$(\mathbb{Q}, \cdot)$ has $\mathbb{Q}^{\times}$ as invertable.

Notation 1.2: Inverse. *if x is inivertable, and has a uni inv, then we denote it x^{-1}.*

Lemma 1.3: Properties of the Inverse. *Let* $(\boxtimes)$is(assoc) *w/ id* e.

1. *e is invertable,* $e^{-1} = e$.

   Proof. $e \boxtimes e = e$ □

2. *if a is invertable, then so is* a^{-1} *and* $(a^{-1})^{-1} = a$.

3. *if a and* bis(invertable) $\implies (a \boxtimes b)^{-1} = b^{-1} \boxtimes a^{-1}$

   Proof. $a \boxtimes b \boxtimes b^{-1} \boxtimes a^{-1} = a \boxtimes e \boxtimes a^{-1} = e$ Similiar in reverse. □

4. *a is invertable **iff***

$$a \boxtimes x = b$$
$$y \boxtimes a = b$$

both have uniq sols $\forall b \in X$.

Proof. $(\implies)$ Assume a is invertable. Then

$$x = a^{-1} \boxtimes b$$
$$y = b \boxtimes a^{-1}$$

$(\impliedby)$ Assume the system has a uni X and Y, $\forall B \in X$. Let $b = e$, where e is the identity of $(X, \boxtimes)$.

$$\begin{aligned} a \boxtimes x &= e \\ y \boxtimes a &= e \\ \implies x &= a_R^{-1} \\ \implies y &= a_L^{-1} \\ (\boxtimes)\text{is(assoc)} \implies a_R^{-1} &= a_L^{-1} = a^{-1} \\ \implies &a \text{ is invertable} \end{aligned}$$

□

Lemma 1.4: Cancellation Property. *Let $\boxtimes$ be an assoc bin op on X w/ id e. If it has a left inverse and* $a \boxtimes u = a \boxtimes v \implies u = v$. *Vice Versa.*

Proof. It should be taken as an axiom. □

2 Groups

2.1 Definitions

Definition 2.1: Group. *a group is a pair $(G, \boxtimes)$ where G is a set and $\boxtimes$ is an assoc bin op on G, w/ and id e, s/t every elem of G is invertable.*

Notation 2.1: Multiplicative Notation. *if the op is clear, we'll usually just write G instead of $(G, \boxtimes)$.*
*We often use $(\cdot)$ as the default symbol for the operation on a group, or even just writing $g \cdot h = gh$. The identity can be denoted by $e, e_G, 1, 1_G$. We use a^{-1} for the inverse of a. This is called **multiplicative notation**.*

Definition 2.2: Abelian Group. *A group $(G, \boxtimes)$ is **abelian** if $\boxtimes$ is abelian (commutative).*

For abelian groups, we often use additive notation.
$(+), \mathrm{idis}0$ or $0_G, \mathrm{inv}(a) = a$.

1. $\mathbb{Z}^+$ is an abelian group (under $+$).

   $$(+)\mathrm{is}(\mathrm{assoc}),\ \mathrm{inv}(a) = -a,\ \mathrm{id}(+) = 0,\ +\mathrm{is}(\mathrm{bin\ op})$$

   Note that this is true for $\mathbb{Q}^+ = (\mathbb{Q}, +)$, $\mathbb{R}^+$.

2. $\mathbb{Z}^{\cdot}$ isn't a group; every element in $\mathbb{Z}$ isn't invertable under $(\cdot)$

3. We know that $|\mathbb{Z}| = |\mathbb{Q}|$. Let $\phi\mathrm{is}(\mathrm{bij}) : \mathbb{Z} \to \mathbb{Q}$. Define an operator on $\mathbb{Z}$ by $a \boxtimes b = \phi^{-1}(\phi(a) + \phi(b))$. $(\mathbb{Z}, \boxtimes)$ is an (abelian) group. (**Ex:** $1 \boxtimes 2 = 8$)

Lemma 2.1. `Let`

```
\(\gop\is(\T{assoc}\),
\(\T{bin op on }M\)
\(\mathrm{id}\ \is\ e,\
G:=\{g\in M:g\ \is\ \TM{invertable\;wrt\;\boxtimes}\}\). Then
\(G\) is a group w/ \(g\cdot h:=g\gop h\).
```

Proof. Hmk. □

The smallest possible group is called the trivial group, and it has one element, $\{e\}$, $ee = e$.

1. invertability
2. identity
3. closure of $(\boxtimes)$
4. assoc of $(\boxtimes)$.

$$\mathbb{Q}^\times = \{a \in \mathbb{Q} : a \neq 0\}$$

$$\mathbb{R}^\times = \{a \in \mathbb{R} : a \neq 0\}$$

Both are groups under multiplication (bad notation considering $\mathbb{R}^+$ is a group but $\mathbb{Q}^\times$ is a set. I assume $\mathbb{Q}^\cdot$ is a group, equal to $(\mathbb{Q}^\times, (\cdot))$).

Corollary 2.1. *Let X be a set, and let S_X be the set of functions $\{f : X \to X : f\text{is}(\text{invertable})\} = \{f \in \text{Fun}(X, X) : f\text{is}(\text{inv})\}$.*
Then S_X is a group under function composition.

Definition 2.3: Permutation Group. *$X := \{1, \ldots, n\}$. S_X is called the permutation group of rank n, and is denoted S_n.*

$$\Sigma := \{\sigma \in \text{Fun}(X, X) : \sigma\text{is}(\text{bij})\}$$

$$S_X := (\Sigma, \circ)$$

Definition 2.4: Order. *The order of a group $G = (E, \boxtimes)$ is $|G| = |E|$, where E is finite. If E is infinite, we'll say $|G| = +\infty$.*

$$|S_n| = |(\Sigma, \circ)| = n!$$

$(M, \boxtimes)\text{is(monoid)} \implies (M|_{(\text{inv})}, \boxtimes)\text{is(group)}$

Example of above. $M_n\mathbb{F} := M_{n\times n}(\mathbb{F})$.
$(M_n\mathbb{F}, \cdot)\text{is(monoid)}$, so $\left(M_n\mathbb{F}|_{(\text{inv})}, \cdot\right)$ is(group)

Notation 2.2: General Linear Group. $\left(M_n\mathbb{F}|_{(\text{int})}, \cdot\right)$ *is called the **general linear group** (over $\mathbb{F}$), denoted*

$$\text{GL}_n\mathbb{F}$$

2.2 Dihedral Groups

Definition 2.5: N-Gon. *Let $\mathbb{P}_n : n \geq 3$ denote the regular n-gon, with verticies*

$$v_k = \left(\cos\frac{2\pi k}{n}, \sin\frac{2\pi k}{n}\right) : 0 \leq j \leq n \quad \textit{noting } v_n = v_0$$

Definition 2.6: An N-Gon Symmetry. *A **symmetry of the n-gon** is an elem $T \in \text{GL}_2\mathbb{R}$ s/t $T(\mathbb{P}_n) = \mathbb{P}_n$*

Definition 2.7: Dihedral Group. *The set of symmetries of $\mathbb{P}_n$ is called the dihedral group of rank n, denoted D_{2n}.*

Lemma 2.2: Dihedral GROUP. *D_{2n} is a group under matrix multiplication.*

Proof. Later, in section subgroups. □

What are the elems of D_{2n}? $\text{Id}(D_{2n}) = I_2$.
Rotation s by $\frac{2\pi}{n}$ radians are elems, and $s(v_i) = v_{i+1}$, $\forall i = 0, \ldots, n-1$.
Reflection along the x axis is an elem, so $r(v_i) = v_{n-i}$.

Definition 2.8: Group Power.

$g^n := \underbrace{g \cdot g \cdot \cdots \cdot g}_{n}, \; n \geq 0.$

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

$g^0 := e = \mathrm{Id}(G).$

Note. *$g^{-n} = (g^{-1})^n$ and $g^{-n}g^n = e$ Prove the following:*

$$g^n g^m = g^{n+m}$$

$$(g^n)^m = g^{nm}$$

All this also has additive notation. $ng = g + \cdots + g$ and $(-n)g = \underbrace{(-g) + \cdots + (-g)}_{n}$

Note.

$$(gh)^n \neq g^n h^n$$

Definition 2.9: Order of an Element. *The **order** $g \in G$ is denoted*

$$|g| := \min(\{k \geq 1 : gk = e\} \cup \{+\infty\})$$

Example: $|e| = 1$, $|g| = 1 \iff g = e$. $\mathbb{Z}^+$, $|1| = +\infty$. $(\mathbb{Z} \backslash n\mathbb{Z}, +)$ $|[1]| = n$ b/c $n \cdot [1] = 0$

Lemma 2.3: Properties of Order. *1.* $g^n = e \implies g^{n-1} \cdot g = e \implies g^{n-1} = g^{-1}$

2. $g^n = e \iff (g^n)^{-1} = e$

$\implies |g^{-1}| = |g|$

Example

$$-[1] = (n-1)[1] = [n-1]$$

Back to dihedral groups.

D_{2n}, $|s| = n \equiv s^n(\mathbb{P}_n) = \mathbb{P}_n$. $|r| = 2 \equiv r^2(\mathbb{P}_n) = \mathbb{P}_n$.

So $e, s, s^2, \ldots, s^{n-1} \in D_{2n}$, and $r, sr, s^2r, \cdots, s^{n-1}r \in D_{2n}$.

Proposition 2.1: Dihedral Group Explicit Classification. $D_{2n} = \{s^i : 0 \leq i < n\} \cup \{s^i r : 0 \leq i < n\}$ *and* $|D_{2n}| = 2n$

Proof. $S, T \in D_{2n}$. So S, T are linear operations. So if

$$S(v_0) = T(v_0)$$

$$S(v_1) = T(v_1)$$

$$\implies S = T$$

following if we treat v_0, v_1 as basic vectors.
Claim 2: $T \in D_{2n} \implies$

$$(T(v_0), T(v_1)) \in \{(v_i, v_{i+1}) : 0 \leq i \leq n-1\} \cup \{(v_{i+1}, v_i) : 0 \leq i \leq n-1\} =: V$$

Proof. v_0, v_1 have to be sent to adj verticies (by picture lol, although we could use a "convexity" arguement).
$(s^i(v_0), s^i(v_1)) = (v_i, v_{i+1})$ $(r(v_0), r(v_1)) = (v_0, v_{n-1})$
$(s^i r(v_0), s^i r(v_1)) = (s^i(v_0), s^i(v_{n-1})$ (v_i, v_{i-1}) □

Claim 3: $\phi : D_{2n} \to V : \phi(T) = (T(v_0), T(v_1))$ is a bijection. By claim 1, it's a injection, and by the calculation above, it's a surjection. Finally, $2n = |V|$ and $D_{2n} = |V| \implies 2n = |D_{2n}|$.
So $\{s^i : 0 \leq i \leq n-1\} \cup \{s^i r : 0 \leq i \leq n-1\} = D_{2n}$.
Also $rs(v_0) = r(v_1) = v_{n-1}$, $rs(v_1) = v_{n-2}$ so $rs = s^{n-1}r = s^{-1}r$. □

2.3 Subgroups

Definition 2.10: Subgroup. *Let G be a group. $H :\subseteq G$ is a* ***subgroup*** *if*

1. $\forall g, h \in H,\ g \cdot h \in H$
2. $g \in H \implies g^{-1} \in H$
3. $e_G \in H$

Notation 2.3: Subgroup. $H \leq G \iff H$ *is a subgroup of* G.

Proposition 2.2: A Subgroup is a Group. $H \leq G \implies G\text{is(group)}$, *with* $\cdot_H : H \times H \to H$.

Proof. First, $\cdot_H$ is well defined b/c H is clsd under $\cdot_G$.
Next, e_G is an identity for $\cdot_H$.
$\cdot_H$ is assoc b/c $\cdot_G$ is assoc.
Finally, and elem is inv b/c it has an inverge in H wrt $\cdot_G$. □

Example 2.1.

$$\mathbb{Z}^+ \leq \mathbb{Q}^+ \leq \mathbb{R}^+ \leq \mathbb{C}^+$$

$$\mathbb{N}^+ \not\leq \mathbb{Z}^+$$

Example 2.2: The Dihedral Group is a Subgroup of the General Linear Group.

$$D_{2n} \leq \mathrm{GL}_2\mathbb{R}$$

Example 2.3. $\mathbb{Q}_{>0} \leq \mathbb{Q}^\times$

$$\textit{2:}\ \ \langle s \rangle = \{s^i : 0 \leq i < n\} \leq D_{2n}$$

Proof of 2.

1. $s^i \cdot s^j = s^{i+j} = s^{an+k} = (s^n)^a \cdot s^k = e^a \cdot s^k = s^k$
2. $g^{-1} = g^{n-i}$, $(g^0)^{-1} = g^0$
3. $e = s^0 = e$

□

Example 2.4. $m\mathbb{Z} := \{mk : k \in \mathbb{Z}\} \leq \mathbb{Z}^+$.

Proof. $mj_1 + mk_2 = m(k_1 + k_2) \in m\mathbb{Z}$. $-mk = m(-k) \in m\mathbb{Z}$. $0 = m0 \in m\mathbb{Z}$. □

Example 2.5. $G \leq G$ *and* $\{e_G\} \leq G$.

Definition 2.11: Proper Subgroup. *$H \leq G$ is **proper** if $H \neq F$, denoted $H < G$.*

"nontrivial proper subgroup..." $\{e\} \neq H \neq G$

Proposition 2.3. *Let $H \subseteq G$ be a subset of a group G. Then $H \leq G$ iff*

1. *$H \neq \emptyset$ and*
2. *$g, h \in H \implies g \cdot h^{-1} \in H$.*

Proof. ($\implies$) clear.
($\impliedby$) Suppose (a) and (b) hold. By (a), $H \ni g$. By (b), $e = g \cdot g^{-1} \in H$. If $g, h \in H$, then $h^{-1} \in H$, so $g \cdot (h^{-1})^{-1} \in H$, but $g \cdot (h^{-1})^{-1} = g \cdot h \in H$. □

Example 2.6: Subspaces are Subgroups of the Additive Vector Space Group. *If W is a subspace of vector space V, the $W \leq V^+$.*

Check. $0 \in W$ so nonempty.
$v, w \in W \implies v - w \in W$, so W is a subgroup. □

Proposition 2.4. *Suppose $G$is(group) and $H \subseteq G$ is finite. Then $H \subseteq G$ $\underline{\textit{iff}}$*

1. *$H \neq \emptyset$*
2. *$g \cdot h \in H$*

Proof. ($\implies$) Clear.
($\impliedby$) Assume (1.) and (2.) hold. So $g \in H$. By induction, $g^n \in H$ $\forall n \geq 1$.
B/c H is finite, $g^1, g^2, g^3, \ldots,$ repeats. So $g^i = g^j$ fore some $1 \leq i < j$.
But now we know $g^{j-i} = e \in H$ noting that $j - i \geq 1$.
We now know $g^n \in H$ for $n \geq 0$. Since $g^{j-i} = e \implies g^{j-i-1} \cdot g = e \implies g^{-1} = g^{j-i-1}$. Since $j - i - 1 \geq 0$, $g^{-1} \in H$.
So if $g, h \in H$, then $h^{-1} \in H$, then $gh^{-1} \in H$, so H is a subgroup. □

Aside. the Set of subgroups of G form a **lattice**.

Proposition 2.5. *Suppose $\mathcal{F}$ is a nonempty set of subgroups of G. Then*

$$K = \bigcap_{H \in \mathcal{F}} H$$

is a subgroup.

Notation 2.4: (Not in Class) anonymous intersection. $K := \cap''\mathcal{F}$

$$\mathcal{F} := \{f \leq G : f \neq \emptyset\}$$

Can we shorten the above?

Proof. $e \in H,\ \forall H \in \mathcal{F} \implies e \in K$.
If $g, h \in K \implies g, h \in H,\ \forall H \in \mathcal{F}$.

$$gh^{-1} \in H,\ \forall H \in \mathcal{F}$$

$$\implies gh^{-1} \in K, \text{ so } K \leq G$$

□

Definition 2.12: Generator. *Let $S \subseteq G$. Then $\langle S \rangle := \bigcap_{S \subseteq H \leq G} H$.*
The intersection of all subgroups that contain S. ***The Subgroup of G Generated by S****.*
If $S \subseteq K \leq G$ then $\langle S \rangle \leq K$.

Note 2.1. *$\langle S \rangle$ is the smallest possible subgroup of G containing S.*
By prop, $\langle S \rangle$ is a subgroup.

Example 2.7: Trivial Subgroup generated by the Emptyset. $\langle \emptyset \rangle = \bigcap_{H \leq G} H = \{e\}$. *All subgroups of G must have the identity e.*

Example 2.8: Group generated by itself. $\langle G \rangle = G$. *The smallest subgroup containing G is G itself.*

Notation 2.5: Redundant Curls. $\langle \{s_1, s_2, \ldots\} \rangle =: \langle s_1, s_2, \ldots \rangle$

Example 2.9: Rotations generated by s. $\langle s \rangle \supseteq \{s\} \implies s^i \in \langle s \rangle, \forall i$.
We previously saw that $\{s^i : 0 \leq i < n\} \leq D_{2n}$, *so* $\langle s \rangle = \{s^i : 0 \leq i < n\}$.

Notation 2.6: Inverse Map of a Set. $S^{-1} := \{s^{-1} : s \in S\}$

Proposition 2.6: Generators make Sets of Powers. *Suppose* $S \subseteq G$, $G \text{is(group)}$.

$$K = \{e\} \cup \{s_1 \cdot s_2 \cdots s_k : k \geq 1,\ s_1, s_2, \dots, s_k \in S \cup S^{-1}\}$$

Then $\langle S \rangle = K$.

Proof. Claim 1: $S \subseteq K \subseteq \langle S \rangle$
$S \subseteq K$ is clear.
Use induction to show $K \subseteq \langle S \rangle$.
Claim 2: $K \subseteq G$.
$e \in K$. Suppose $g = s_1 \cdots s_k,\ h = t_1 \cdots t_l, \in K$, for $s_1, \dots, s_k, t_1, \dots, t_l \in S \cup S^{-1}$.
($k = 0$ means $g = e$, $l = 0 \implies h = e$).
Then

$$gh^{-1} = s_1 \cdots s_k t_l^{-1} \cdots t_1^{-1} \in K$$

So $K \leq G$.
By claims 1 and 2, $K \subseteq \langle S \rangle \subseteq K \implies K = \langle S \rangle$. □

Lemma 2.4. $G \supseteq S$ *generates* G *if* $\langle S \rangle = G$.

Definition 2.13: Cyclic Groups. *A group is cyclic* ***iff*** *it's generated by a single element.*

$$G = \langle a \rangle \implies G \text{is(cyclic)}$$

Definition 2.14: Cyclic Subgroups. *A* ***cyclic subgroup*** *of a group* G *is a subgroup of the form* $\langle a \rangle$ *for some* $a \in G$.

Lemma 2.5: Cyclic Group Chacterization into Powers. *if G is a group, then*

1. *if $a \in G$, then $\langle a \rangle = \{a^i : i \in \mathbb{Z}\}$*
2. *$a \in G$ & $|a| = n < \infty \implies \langle a \rangle = \{a^i : 0 \leq i < n\}$*

Proof.

1. is a coro to characterization of $\langle a \rangle$ into powers prop
2. $i = kn + r \implies a^i = a^r$

□

Example 2.10: Integers generated by 1.

$$\mathbb{Z}^+ = \langle 1 \rangle = \{n \cdot 1 : n \in Z\}$$

$$n \in \mathbb{Z},\ \langle n \rangle = \{kn : k \in \mathbb{Z}\} = n\mathbb{Z}$$

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

Note 2.2. $\langle a \rangle = \langle a^{-1} \rangle$

Example 2.11: Rationals aren't Cyclic.

$$\mathbb{Q}^+ \ \not\text{is}(\text{cyclic})$$

Assume for contradiction it is. Then

$$\forall q \in \mathbb{Q},\ q = np \text{ for some } p \in \mathbb{Q},\ n \in \mathbb{Z}$$

Take $p \in \mathbb{Q}$. Then $\frac{1}{2}p \notin \langle p \rangle$. So $\mathbb{Q}^+$ isn't cyclic.

Example 2.12: Sets generated by s and r from D2n.

$$\langle s \rangle = \{e, s^1, s^2, \dots\}$$

$$\langle r \rangle = \{e, r\}$$

Proposition 2.7: Order of a = Order of gen(a).

$$|\langle a\rangle| = |a|$$

Proof. By the lemma, we know $|\langle a\rangle| \leq |a|$.
$|\left\langle a\right\rangle| = \infty = |a|$. If $|\left\langle a\right\rangle| = n < \infty$, then

$$\langle a\rangle = \{a^i : i \in \mathbb{Z}\}, \quad \text{so we must have repitians}$$

$$a_0, a_1, \ldots, a_n$$

$$\text{So for some } 0 \leq i < j \leq n$$

$$a^i = a^j \implies |a| \leq j - i \leq n$$

$$\implies |a| \leq n = |\left\langle a\right\rangle|$$

□

Example 2.13: Integers.

$$|a| = |\left\langle a\right\rangle| = |a\mathbb{Z}| = \begin{cases} \infty & a \neq 0 \\ 1 & a = 0 \end{cases}$$

Example 2.14: Modulo Integers.

$$|\pm 1| = |\left\langle \pm 1\right\rangle| = |\mathbb{Z}\backslash n\mathbb{Z}| = n$$

Lemma 2.6: Set Equality for Generators. *Suppose $T \subseteq \langle S\rangle$. Then*

$$\langle S\rangle = \langle T\rangle \iff S \subseteq \langle T\rangle$$

Proof. $(\implies)$ obvious.
$(\impliedby)$

$$S \subseteq \langle T\rangle \ \&\ T \subseteq \langle S\rangle \implies \langle S\rangle = \langle T\rangle$$

□

Example 2.15: What generates the modulo integers?. *When does $[a] \in \mathbb{Z} \backslash n\mathbb{Z}$ generate $\mathbb{Z} \backslash n\mathbb{Z}$?*

$$\begin{aligned}
\mathbb{Z} \backslash n\mathbb{Z} = \langle [a] \rangle &\iff [1] \in \langle [a] \rangle \\
&\iff [1] = x[a] \\
&\iff 1 \equiv xa \mod n \\
&\iff xa - 1 = yn, \ x, y \in \mathbb{Z} \\
&\iff xa + yn = 1 \\
&\iff \gcd(a, n) = 1
\end{aligned}$$

2.4 Modulo and Generators

Lemma 2.7. $g \in G \text{is(grp)}$

$$g^n = e \implies |g| \mid n$$

Proof. Hwk. □

Lemma 2.8.

$$a \mid n \implies |[a]| = \frac{n}{a} \in \mathbb{Z} \backslash n\mathbb{Z}$$

Proof.

$$a \mid n \iff \exists k \in \mathbb{Z} \text{ s/t } ak = n$$

$$l\,[a] \neq 0 \Longleftarrow 1 \leq l \leq k$$

$$k\,[a] = 0 = \text{Id} \implies |[a]| = k = \frac{n}{a}$$

□

Lemma 2.9.

$$a, n \in \mathbb{Z}, \ n \neq 0, \ b := \gcd(a, n)$$

$$\langle [a] \rangle = \langle [b] \rangle$$

Proof.

$$b \mid a \iff \exists k \in \mathbb{Z} \text{ s/t } bk = a$$

$$\implies [a] \in \langle [b] \rangle$$

Note 2.3: README: Sometimes english is better. *saying all congruent to a are all multiples of all congruent to b. b is smaller lmao, so yep pretty much.*

$$\implies \langle [a] \rangle \subseteq \langle [b] \rangle$$

$$b = \gcd(a, n) \implies \exists x, y \in \mathbb{Z} \text{ s/t}$$

$$xa + yn = b$$

$$\implies x\,[a] + \cancelto{0}{[yn]} = [b]$$

$$\implies [b] \in \langle [a] \rangle$$

$$\implies \langle [b] \rangle = \langle [a] \rangle$$

□

Proposition 2.8.

$$a, n \in \mathbb{Z},\ n \neq 0$$

$$\implies |[a]| = \frac{n}{\gcd(a, n)}$$

Proof.

$$|[a]| = |\langle [a] \rangle| = |\langle [b] \rangle| \text{ where } b := \gcd(a, n)$$

$$= |[b]| = \frac{n}{b}$$

□

Note 2.4: Old Definitions from Algebra.

$$\mathbb{Z}\backslash n\mathbb{Z} := \{[k] : k = 0, \dots, n-1\}$$

$$[k] := \{m \in \mathbb{Z} : m \equiv k \pmod{n}\}$$

$$|g| = |\langle g \rangle|$$

$$\langle g \rangle := \{g^n : n \in \mathbb{Z}\}$$

Corollary 2.2.

1. *$n \in \mathbb{N}$, $a \in \mathbb{Z}\backslash n\mathbb{Z}$, $|\langle a \rangle| \mid n$. order of any cyclic subgroup of $\mathbb{Z}\backslash n\mathbb{Z}$ divides n*

2. *(idk)*
$$\forall d \mid n,\ \exists!\, \langle [a] \rangle \ \textit{s/t}\ |\langle [a] \rangle| = d \textit{ where } [a] = \frac{n}{d}$$

Proof. **1.**
$$\exists a \in \mathbb{Z} \text{ s/t } |\langle a \rangle| = d$$
$$\text{By a lem above, } d = \frac{n}{\gcd(a, b)} \,\Bigg|\, n$$

2.
$$\langle [a] \rangle = \langle [\gcd(a, n)] \rangle = \left\langle \left[\frac{n}{d}\right] \right\rangle$$

So any subgroup of order d must be in

$$\left\langle \left[\frac{n}{d}\right] \right\rangle$$

Conversely,
$$d \mid n,\ \left| \left\langle \left[\frac{n}{d}\right] \right\rangle \right| = \left| \frac{n}{d} \right| = \frac{n}{n/d} = d$$

□

Example 2.16. $\mathbb{Z}\backslash 6\mathbb{Z}$

$$\langle [6] \rangle = \{0\} \implies |\langle [6] \rangle| = 1$$

$$\langle [3] \rangle = \{0, 3\} \implies |\langle [3] \rangle| = 2$$

$$\langle [2] \rangle = \{0, 2, 4\} \implies |\langle [2] \rangle| = 3$$

$$\langle [1] \rangle = \{0, \dots, 5\} \implies |\langle [1] \rangle| = 6$$

Later: All subgroups of cyclic groups are cyclic. Every cyclic group is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}\backslash n\mathbb{Z}$ for some n.

2.5 Homomorphisms

Definition 2.15: Homomorphism. *Let $G, H\text{is}(\text{grp})$. Then a fn $f : G \to H$ is a **homomorphism** if*

$$\forall g, h \in G,\ f(g \underset{G}{\cdot} h) = f(g) \underset{H}{\cdot} f(h)$$

Example 2.17.

$$G = \mathrm{GL}_n\mathbb{R} := M_n\mathbb{R}|_{\mathrm{inv}},\ H = \mathbb{R}^\times$$

$$\det : \mathrm{GL}_n\mathbb{R} \to \mathbb{R}^\times$$

$$\det(A \underset{\mathrm{GL}_n\mathbb{R}}{\cdot} B) = \det(A) \underset{\mathbb{R}}{\cdot} \det(B)$$

Example 2.18. $T : V \to W\text{is}(\text{linear transform}) \implies T : V^+ \to W^+\text{is}(\text{hom})$

Example 2.19. $\overset{\subseteq\mathbb{R}^\times}{\mathbb{R}_{>0}} \to \mathbb{R}_{>0} : x \mapsto \sqrt{x}$

$$\sqrt{ab} = \sqrt{a} \cdot \sqrt{b}$$

Example 2.20. $\phi : \mathbb{R}^+ \to \mathbb{R}^\times : x \mapsto e^x$

$$\phi(x + y) = e^{x+y} = e^x e^y = \phi(x)\phi(y)$$

Example 2.21.

$$\phi : \mathbb{R}^+ \to \mathbb{R}^+ : x \mapsto e^x$$

$$e^{x+y} \neq e^x + e^y \implies \phi \textit{ isn't a hom}$$

Example 2.22.

$$\mathbb{Z}^+ \to \mathbb{Z}^+ : x \mapsto mx$$

$$m(x + y) = mx + my$$

Example 2.23.

$$H \leq G$$

$$i : H \hookrightarrow G : h \mapsto h \textit{ is a hom}$$

Example 2.24.

$$\varphi : G \to H,\ \psi : H \to K$$

$$\textit{Claim: } \psi \circ \varphi \textit{ is a hom}$$

Proof.

$$\text{Let } g, h \in G, \text{ then } \phi \circ \varphi(gh)$$

$$= \psi(\varphi(g) \cdot \varphi(h))$$

$$= \psi \circ \varphi(g) \cdot \psi \circ \varphi(h)$$

□

Example 2.25.

$$K \leq G,\ \varphi : G \to H \textit{ is a hom}$$

$$\textit{Then } \left.\varphi\right|_K : K \to H \textit{ is a hom}$$

Proof.

$$K \overset{i}{\hookrightarrow} G \to H$$

$$\varphi|_K = \varphi \circ i$$

□

Lemma 2.10: Properties of Homomorphisms. *Let ϕ be a homomorphism.*

1. $\varphi(e_G) = e_H$

Proof.

$$\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G)$$

Consider

$$e_H = h^{-1} \cdot h \text{ for some } h \in H$$

$$e_H = \varphi(e_G)^{-1} \cdot \varphi(e_G) = \varphi(e_G)^{-1} \cdot \varphi(e_G) \cdot \varphi(e_G) = \varphi(e_G)$$

□

2. $\varphi(g^{-1}) = \varphi(g)^{-1}$

Proof.

$$e_H = \varphi(e_G) = \varphi(g^{-1} \cdot g) = \varphi(g^{-1})\varphi(g)$$

$$\implies \varphi(g)^{-1} = \phi(g^{-1})$$

□

3. $\varphi(g^n) = \varphi(g)^n$

Proof. Induction. Works for integers. □

4. $|\varphi(g)| \mid |g|$

Proof.

$$|g| = n < \infty$$

$$\text{Then } \varphi(g)^n = \varphi(g^n) = \phi(e) = e$$

$$\text{Note that } h^m = e \implies |h| \mid m$$

$$\implies |\varphi(g)| \mid n$$

$$|g| = \infty, \ |\varphi(g)| \cdot \infty = \infty$$

$$\text{So } |\varphi(g)| \mid \infty$$

□

Notation 2.7. $f : X \to Y, \ S \subseteq X. \ f(S) = \{f(x) : x \in S\}$

Proposition 2.9: Homomorphisms Preserve Sub-Group Order. $\varphi : G \to H \text{is(hom)},\ K \leq G.\text{then}\varphi(K) \leq H.$

Proof. $e_G \in K \implies \varphi(e_G) = e_H = e_K \in \varphi(K)$

$$g_{\varphi(K)}, h_{\varphi(K)} \in \varphi(K),\ g_{\varphi(K)} = \varphi(g_G) \text{ and } h_{\varphi(K)} = \varphi(h_G)$$

$$g_G h_G^{-1} \in K \text{ because } K \leq G$$

$$g_{\varphi(K)} h_{\varphi(K)}^{-1} = \varphi(g_G)\varphi(h_G)^{-1} = \varphi(g_G h_G^{-1}) \in \varphi(K)$$

$$\implies \varphi(K) \leq G$$

□

Definition 2.16: Image. $\varphi : G \to H$ *hom. The* ***image*** *denoted* $\text{Im}\varphi$ *is the subgroup of* $\varphi(G)$ *of* H.

Note 2.5. $G \leq G \implies \varphi(G) \leq H \implies \text{Im}\varphi \leq H$

Example 2.26. $\varphi : \mathbb{R}^+ \to \mathbb{R}^\times : x \mapsto e^x$

$$\text{Im}\varphi = \varphi(\mathbb{R}^+) = \mathbb{R}^\times_{>0}$$

Example 2.27. $\varphi : \mathbb{Z} \to \mathbb{Z} : x \mapsto mx$. $\text{Im}\varphi = \varphi(\mathbb{Z}) = m\mathbb{Z}$

Lemma 2.11: Minimal Image. $\varphi : G \to H \text{is(hom)}.\ \text{Im}\varphi \leq K \leq H \text{then} \widetilde{\varphi} : G \to K : g \mapsto \varphi(g) \text{is(hom)} w/\ \text{Im}\widetilde{\varphi} = \text{Im}\varphi$

Proof. "Obvious," from note above. □

We say $\widetilde{\varphi}$ is **induced by** φ. “Trivially build from.”

Example 2.28.

$$\varphi : \mathbb{R}^+ \to \mathbb{R}^\times : x \mapsto e^x$$

$$\widetilde{\varphi} : \mathbb{R}^+ \to \mathbb{R}^\times_{>0} : x \mapsto \varphi(x)$$

Lemma 2.12: Surjective Homomorphism.

$$\text{(hom) } \varphi : G \to H \text{is(surj)} \iff \text{Im}\varphi = H$$

Corollary 2.3: Phi Restricted to its Image is Surjective.

$$\text{(hom) } \varphi : G \to H, \textit{ induces a surj hom } \widetilde{\varphi} : G \to \varphi(H)$$

Proposition 2.10: Generaters and Homomorphisms are Abelian under Composition. if(hom) $\varphi : G \to H,\ S \subseteq G$then$\varphi(\langle S \rangle) = \langle \varphi(S) \rangle$

Proof.

$$\varphi(S^{-1}) = \{\varphi(x^{-1}) : x \in S\} = \{\varphi(x)^{-1} : x \in S\} = \varphi(S)^{-1}$$

$$\begin{aligned}
\varphi(\langle S \rangle_G) &= \varphi(\{s_1 \cdots s_n : n \geq 0,\ s_1, \cdots, s_n \in S \cup S^{-1}\}) \\
&= \{\varphi(s_1 \cdots s_n) : n \geq 0,\ s_1, \ldots, s_n \in S \cup S^{-1}\} \\
&= \{t_1 \cdots t_n : n \geq 0,\ t_1, \ldots, t_n \in \varphi(S \cup S^{-1})\},\ t_i = \varphi(s_i) \\
&= \{t_1 \cdots t_n : n \geq 0,\ t_1, \ldots, t_n \in \varphi(S) \cup \varphi(S)^{-1} \\
&= \langle \varphi(S) \rangle_H
\end{aligned}$$

□

Notation 2.8: Preimage of a function.

$$f : X \to Y,\ S \subseteq Y,\ f^{-1}(S) = \{x \in X : f(x) \in S\}$$

Proposition 2.11: Preimages of Homomorphisms of Subgroups are Subgroups. (hom) $\varphi : G \to H,\ K \leq H.$

$$\varphi^{-1}(K) \leq G$$

Proof.

$$\varphi(e_G) = e_H \in K \implies \varphi(e_G) \in K \implies e_G \in \varphi^{-1}(K) \blacksquare$$

$$g, h \in \varphi^{-1}(K) \implies \varphi(g), \varphi(h) \in K$$

$$\begin{aligned} &\implies \varphi(gh^{-1}) \in K \\ &= \varphi(g)\varphi(h)^{-1} \in K \\ &\implies gh^{-1} \in \varphi^{-1}(K) \end{aligned}$$

□

Proposition 2.12: Cyclic Groups have Cyclic Subgroups. *If G is cyclic, then all subgroups of G are cyclic.*

Proof. Suppose G is cyclic, $H \leq G$. Because G is cyclic, there is a surjective homomorphism $\varphi : \mathbb{Z} \to G$ (by HWK).

$$\implies \mathrm{Im}(\varphi) = G$$

let$K = \varphi^{-1}(H)$. By HWK, $K = m\mathbb{Z} = \langle m \rangle_{\mathbb{Z}}$.

Note 2.6.

$$\text{if(surj) } f \text{then} f(f^{-1}(S)) = S$$

$$\text{(surj) } \varphi \implies H = \varphi(\varphi^{-1}(H)) = \varphi(\langle m \rangle_{\mathbb{Z}}) = \langle \varphi(m) \rangle_G$$

□

Definition 2.17: Kernel. (hom) $\varphi : G \to H$. *The **kernel** of φ is the subgroup*

$$\ker\varphi = \varphi^{-1}(\{e_H\}) \textit{ of } G$$

Example 2.29.

$$\varphi : \mathbb{R}^+ \to \mathbb{R}^\times : x \mapsto e^x$$

$$\ker \varphi = \{x \in \mathbb{R} : e^x = 1\} = \{0\}$$

Example 2.30.

$$\varphi : \mathbb{Z} \to m\mathbb{Z} : x \mapsto mx$$

$$\ker\varphi = \begin{cases} \mathbb{Z} & m = 0 \\ \{0\} & m \neq 0 \end{cases}$$

Example 2.31: Special Linear Group.

$$\ker\left(\det : \mathrm{GL}_n\mathbb{R} \to \mathbb{R}^\times\right) =: \mathrm{SL}_n\mathbb{R}$$

Proposition 2.13: Homomorphic Injective Function. (hom) $\varphi : G \to H$is(inj) ***iff*** $\ker\varphi = \{e_G\}$

($\implies$) *Proof.* $\varphi$is(inj), so $\forall a_G, b_G \in G$,

$$\varphi(a_G) = \varphi(b_G)$$

$$\implies a_G = b_G$$

So,

$$\varphi(a_G) = e_H = \varphi(e_G)$$

$$\implies a_G = e_G \text{ by inj}$$

$$\implies \ker\varphi = \{e_G\}$$

□

($\implies$) *Proof.* Suppose $\ker\varphi = \{e_G\}$.

$$\text{if}\varphi(g_G) = \varphi(h_G)$$

$$\text{then}e_H = \varphi(g_G)^{-1}\varphi(h_G) = \varphi(g_G^{-1}h_G)$$

$$\implies g_G^{-1}h_G \in \ker\varphi$$

$$\implies g_G^{-1}h_G = e_G$$

$$\implies h_G = g_G$$

□

A hom $\varphi : G \to H$ is an iso if φ if φ is bijective (inj & surj).

Corollary 2.4: Isomorphic. *$\varphi : G \to H$is(iso) **iff** $\ker\varphi = \langle e_G\rangle$ and $\mathrm{Im}\varphi = H$.*

Note 2.7: Left Right Function Inverses. *$f : X \to Y$ is bij **iff** f has an inverse*

$$f^{-1} : Y \to X \text{ w/ properties}$$

$$f \circ f^{-1} = \mathrm{Id}_Y$$

$$f^{-1} \circ f = \mathrm{Id}_X$$

Proposition 2.14: Inverses are also Isomorphic. *$\varphi : G \to H$ iso then $\varphi^{-1} : H \to G$ is also iso (hom and bij).*

Proof.

1. $h_0, h_1 \in H.\text{let}g_i \in G$ be the unique elem w/ $\varphi(g_i) = h_i\ i = 0, 1, \ldots$

$$\begin{aligned}\varphi^{-1}(h_0h_1) &= \varphi^{-1}(\varphi(g_0)\varphi(g_1)) \\ &= \varphi^{-1}(\varphi(g_0g_1)) \\ &= g_0g_1 \\ &= \varphi^{-1}(h_0)\varphi^{-1}(h_1)\end{aligned}$$

So φ^{-1} is a hom. Sonce φ^{-1} is invertable, it's also a iso.

□

Corollary 2.5: Isomorphism iff Identity Compositions Exist.

$$\text{hom } \varphi : G \to H is iso \iff \exists\psi : H \to G \text{ s/t}$$

$$\varphi \circ \psi = \mathrm{Id}_H$$

$$\psi \circ \varphi = \mathrm{Id}_G$$

Definition 2.18: Isomorphic Sets. *Two groups G, H are isomorphic if there is an isomorphism $\varphi : G \to H$.*

Notation 2.9: Isomorphic Sets. $G \cong H$

Note 2.8: Key Facts about Isomorphic Sets.

1. $\text{if} G \cong H \text{then} H \cong G$
2. $\text{if} G \cong H$ and $H \cong K \text{then} G \cong K$
3. $G \cong G$

*This **IS NOT** an equivalence relation, as they have to act on sets, and the set of all groups is "hard" to talk about. Look into what a "**proper class**" is. If G $\cong$ H then they're called "**identical.**"*
In particular, if $G \cong H$, then

1. $|G| = |H|$
2. $G \text{isabelian} \iff H \text{isabelian}$
3. $|g| = |\varphi(g)|, \ \forall g \in G, \ \varphi : G \to H \text{isiso}$
4. $K \subseteq G \text{then} K \leq G \iff \varphi(K) \leq H$

Proposition 2.15: Isomorphic Cyclic Groups. *G, H are cyclic.*

$$G \cong H \iff |G| = |H|$$

Proof. ($\implies$) Clear from before. □

Proof. ($\Longleftarrow$). Assume $|H| = |G|$, and that they're cyclic.

$$G = \langle a \rangle \quad H = \langle b \rangle \,, \mathrm{let} n = |G| = |H|$$

Case 1: $n = \infty$.

$$G = \{a^i : i \in \mathbb{Z}\} \quad H = \{b^i : i \in \mathbb{Z}\}$$

$$a^i \neq a^j \mathrm{if} i \neq j \quad b^i \neq b^j \mathrm{if} i \neq j$$

$$\mathrm{let} \varphi : G \to H : a^i \mapsto b^i$$

Clearly a bijection.

$$\varphi(a^i a^j) = \varphi(a^{i+j}) = b^{i+j} = b^i b^j = \varphi(a^i)\varphi(a^j) \implies \text{(hom)}$$

□

Case 2: $n < \infty$.

$$G = \{a^i : 0 \le i < n\} \quad H = \{b^i : 0 \le i < n\}$$

$$\varphi : G \to H : a^i \mapsto b^i, \; 0 \le i < n$$

$$\varphi(a^i a^j) = \varphi(a^{i+j}) = \varphi(a^r)$$

$$\text{where } i + j = qn + r, \; q \in \mathbb{Z}, \; 0 \le r < n$$

$$\varphi(a^r) = b^r = b^{qn+r} = b^{i+j} = b^i b^j = \varphi(a^i)\varphi(b^j)$$

□

□

Corollary 2.6. *If G is cyclic, then*

1. $|G| = \infty, \; G \cong \mathbb{Z}^+$

2. $|G| < \infty, \; G \cong (\mathbb{Z}/n\mathbb{Z})^+ =: \mathbb{Z}_n^+$

Corollary 2.7: Cyclic Groups are Abelian. ...

Notation 2.10: Standard Cyclic Groups.

$$C_n = \langle a \rangle = \{a^i : 0 \leq i < n\}$$

$$C_\infty = \langle a \rangle = \{a^i : i \in \mathbb{Z}\}$$

2.6 Cosets and Lagrange's Theorem

Definition 2.19: Coset. *Let G be a group. If $g \in G$ and $S \subseteq G$, then*

$$gS = \{gh : h \in S\}$$

$$Sg = \{hg : h \in S\}$$

If $H \leq G$, then gH if called a left ***coset*** *of H in G, and respectfully right with Hg.*

Example 2.32.

1.

$$m\mathbb{Z} \leq \mathbb{Z} : \ k \in \mathbb{Z}, \ k + m\mathbb{Z} = \{k + mn : n \in \mathbb{Z}\}$$

2.

$$U^+ \leq V^+$$

$$v + U \text{isa coset}, \ v \in V$$

$$\text{Solution space of } Ax = 0 \text{is} \ker(A)$$

$$\text{Solution space of } Ax = b \text{is} w + \ker(A)$$

Proposition 2.16: Solution Cosets. *Suppose $\varphi : G \to K$ is a hom and $x_0 \in G$.*

$$b := \varphi(x_0)$$

The solution set to $\varphi(x) + b$ is a coset

$$\varphi^{-1}(\{b\}) = x_0 \ker(\varphi) = \ker(\varphi) x_0$$

Proof. Let $k \in \ker(\varphi)$. Then

$$\varphi(x_0 k) = \varphi(x_0)\varphi(k) = \varphi(x_0)e = b$$

$$\implies x_0 k \in \varphi^{-1}(\{b\})$$

$$\implies x_0 \ker(\varphi) \subseteq \varphi^{-1}(\{b\})$$

$$\text{let} y \in \varphi^{-1}(\{b\}), \text{ let} h = x_0^{-1} y$$

$$\implies y = x_0 h$$

$$\text{So } \varphi(h) = \varphi(x_0)^{-1}\varphi(y) = b^{-1}b = e$$

$$\implies h \in \ker(\varphi) \implies \varphi^{-1}(\{b\}) \subseteq \ker(\varphi)$$

□

Proposition 2.17. G is cyclic and $H \leq G$, then

$$|H| \mid |G|$$

Proof. let $h \in H$, $m = |H|$, $n = |G|$. $h^m = h^n = e \implies m \mid n$ □

Definition 2.20: Set Mod Set. let $H \leq G$.

$$G/H := \{gH : g \in G\}$$

$$H \backslash G := \{Hg : g \in G\}$$

The left/right sets of all cosets.

Example 2.33.

$$n\mathbb{Z} \leq \mathbb{Z}$$

$$\mathbb{Z}/n\mathbb{Z} = \{m + n\mathbb{Z} : m \in \mathbb{Z}\} = \{m + n\mathbb{Z} : 0 \leq m < n\}$$

Question: when is G/H a group?

Example 2.34.

$$H = \langle s \rangle \subseteq D_{2n}$$

$$s^i H = s^i \{s^0, s^1, \dots, s^{n-1}\}$$

$$= \{s^i, \dots, s^{i+n-1}\} = H$$

$$s^i r H = r s^{-i} H = r H = \{r, rs, \cdots, rs^{n-1}\} = \{s^i r : 0 \leq i < n\} = Hr$$

$$G/H = \{e, r\}/\{s^i : 0 \leq i < n\} = \{H, rH\} = H \backslash G$$

Example 2.35.

$$K = \langle r \rangle \leq D_{2n}$$

$$s^i r K = s^i K$$

$$D_{2n}/K = \{s^i K : 0 \leq i < n\}$$

$$K s^i = \{s^i, rs^i\} = \{s^i, s^{-i} r\} = \{s^i, s^{n-i} r\}$$

$$K s^i r = K r s^{-i} = K s^i$$

Just for an example of how these sets are different, take $n = 3,\ i = 1$.

$$s \langle r \rangle = \{s, sr\}$$

$$\langle r \rangle s = \{s, s^2 r\}$$

$$\implies s \langle r \rangle \neq \langle r \rangle s$$

$$D_{2n}/\langle r \rangle = \{s^i \langle r \rangle : 0 \leq i < n\}$$

$$\langle r \rangle \backslash D_{2n} = \{\langle r \rangle s^i : 0 \leq i < n\}$$

$$s^i \langle r \rangle \neq \langle r \rangle s^j \ \forall i, j \text{ w/ not both zero}$$

Note 2.9: Abelian Group's Left/Right Mod are Equivalent.

$$gH = Hg \implies G/H = H \backslash G$$

Definition 2.21: Partition. *Let X be a set. A* ***partitian*** *of X is a subset $Q \subseteq 2^X = \mathcal{P}(X)$ s/t*

1.

$$\bigcup_{S \in Q} S = X$$

2.

$$\text{if } S, T \in Q,\ S \neq T,\ \text{then } S \cap T = \emptyset$$

All elements are disjoint, and sum to the whole.

Proposition 2.18. *Let $H \leq G$, $g, k \in G$. Then TFAE:*

1. $g^{-1}k \in H$
2. $k \in gH$
3. $gH = kH$
4. $gH \cap kH \neq \emptyset$

$1 \implies 2$. $g^{-1}K \in H \implies g^{-1}K = h$ for some $h \implies h = gh \implies k \in gH$. □

$2 \implies 3$. $k \in gH \implies k = gh$ for some $h \in H$. Show $gH = kH$.

$\subseteq$.

$$\text{if} h' \in H \text{ then } kh' = ghh' \in gH$$

$$hh' \in H \text{ because } H \text{ is a subgroup}$$

$$\implies kH \in gH$$

□

$\supseteq$.

$$h' \in H,\ gh' = kh^{-1}h' \in kH$$

□

$\implies kH = gH$ □

$3 \implies 4$. by 2, $g \in kH \implies gH \cap kH \neq \emptyset$ □

$4 \implies 1.\ gh = kh' \implies k^{-1}g = h'h^{-1} \implies k^{-1}g \in H$ □

Corollary 2.8: G Mod H forms a Partitian of G. ...

Proof.

$$\text{if } gH \cap kH \neq \emptyset \text{ then } gH = kH$$

$$\implies \text{if } S \neq S' \text{ then } S \cap S' = \emptyset$$

$$\forall g \in G\ g \in gH \implies \bigcup_{S \in G/H} S = G$$

Note 2.10. *Although* $\bigcup_{g \in G} gH = G$*, its different from the above because it has to go through duplicates.*
Note that $k \in gH \implies gH = kH$*, which means there are loads of duplicate cosets in the second union.*

□

Definition 2.22: Relation. *A **relation** on a set* X *is a subset of* $X \times X$*.*

Notation 2.11.

$$R \subseteq X \times X.\ aRb \text{ means } (a,b) \in R$$

$$(\sim) \subseteq X \times X,\ \ a \sim b \text{ means} (a,b) \in (\sim)$$

Example 2.36. $(<) \subseteq \mathbb{N} \times \mathbb{N}$. $(<) = \{(a,b) : a \text{ is strictly less than } b\}$

Definition 2.23: Equivalence Relation. *A relation* $(\sim)$ *on* X *is called a **equivalence relation** if*

1. ***Reflexivity****:* $a \sim a,\ \forall a \in X$
2. ***Symmetry****:* $a \sim b \implies b \sim a,\ \forall a, b \in X$
3. ***Transitivity****:* $a \sim b \text{ and } b \sim c \implies a \sim c,\ \forall a, b, c \in X$

Definition 2.24: Equivalence Class. *If $x \in X$ and $(\sim)$ is an equivalence relation on X, then the* ***equivalence class*** *of x is*

$$[x] = [x]_\sim = \{y \in X : x \sim y\}$$

Example 2.37: Congruence Classes. $\equiv \pmod{n}$ *is an equiv relation on*$\mathbb{Z}$*, and*

$$[x] = \{y : y \equiv x \pmod{n}\}$$

Proposition 2.19: Equivalence Relations are like Set Mod Sets. *Suppose $(\sim)$ is a eq. relation on X. Then TFAE:*

1. $x \sim y$
2. $y \in [x]$
3. $[y] = [x]$
4. $[x] \cap [y] \neq \emptyset$

Proof. If you need these, let me know b/c I didn't want to write them out. □

Corollary 2.9: The Equivalence Class Partitian. *The set of equivalence classes $\{[x]_\sim : x \in X\}$ is a partitian of X.*

Proof. The union is the whole thing.
If two classes have nonempty intersection, they're equal by above. □

Lemma 2.13: Equivalence Relation iff Partitian. *If Q s/t $\emptyset \notin Q$ is a partitian of X, then the relation $(\sim)$ defined by $x \sim y$ iff there is some $S \in Q$ s/t $x, y \in Q$ is an equiv relation and $\{[x] : x \in X\} = Q$.*
Look at each set in Q. Then a relation is induced by if both elements are in that set.

Proposition 2.20: Coset Relation. *$H \leq G$. We can define a relation $(\sim_H)$ on G by*

$$g \sim_H h = \top \iff g^{-1}h \in H$$

This is a equiv relation, and $[g]_\sim = gH$.

Proof. $(\sim_H)$ is he equiv relation defined by the partitian $\{gH : g \in G\} = G/H$.
Directly.
$g \sim h \iff g^{-1}h \in H \implies h^{-1}g \in H \iff h \sim g$.
$g \sim h$, $h \sim j$. $g^{-1}h \in H$, $h^{-1}j \in H$. Show $g^{-1}j \in H$. Since H is a subgroup, it's closed under its binary operation. So $g^{-1}hh^{-1}j = g^{-1}j \in H$.
Now we'll show $[g] = gH$.
Let $h \in [g] \iff g \sim h \iff g^{-1}h \in H \iff h \in gH$. □

Definition 2.25: Index. *$H \leq G$, the **index** of H in G is*

$$[G : H] := \begin{cases} |G/H| & : G/H \text{ is finite} \\ \infty & : \text{o/w} \end{cases}$$

"how many elements do we *really* have?"

Lemma 2.14. *fn $S \mapsto S^{-1}$ defns a bijection $G/H \mapsto H\backslash G$*

Proof. $gH \in G/H \implies gH \mapsto H^{-1}g^{-1} = Hg^{-1} = Hg \ni H\backslash G$
$S = (S^{-1})^{-1}$ □

Corollary 2.10.

$$[G : H] = \begin{cases} |H\backslash G| & : |H\backslash G| < \infty \\ \infty & : \text{o/w} \end{cases}$$

Lemma 2.15. *$S \subseteq G$, $g \in G$, $S \to gH : g \mapsto gh$ is bijection. In particular, $|S| = |gS|$.*

Proof.

$$gS \to S : S \mapsto g^{-1}S \text{ is an inverse}$$

□

Theorem 2.1: Lagrange. *The order of a subgroup divides the group, by the index of the subgroup in the group.*
If a group H is a subgroup of G, so $H \leq G$, then the order of G is equal to the index of H in G times the order of H.

$$|G| = [G : H]|H|$$

In particular, $|H| \mid |G|$.

The order of a group is equal to the order of the subgroup times the number of cosets, group mod subgroup.

If the order a group G is finite, then $[G : H] = \frac{|G|}{|H|}$.

Proof. Case 1.

$$\text{if } |H| = \infty \text{ then } |G| = \infty, \text{ then } |G| = [G : H]|H|$$

Case 2. Since G/H is a partition of G, if $[G : H] = \infty$, then $|G| = \infty \implies |G| = [G : H]|H|$.
Case 3. Suppose $[G : H]$ and $|H|$ are finite. Since G/H is a partitian,

$$|G| = \sum_{gH \in G/H} |gH| = \sum_{gH \in G/H} |H| = |H||G/H| = |H|[G : H]$$

□

Example 2.38.

$$[D_{2n} : \langle s \rangle] = \frac{|D_{2n}|}{|\,\langle s \rangle\,|} = \frac{2n}{|s|} = \frac{2n}{n} = 2$$

$$|\langle r \rangle| = |r| = 2 \implies [D_{2n} : \langle r \rangle] = n$$

There are n equivalence classes induced by the cosets rD_{2n} and $D_{2n}r$.

Example 2.39.

$$[\mathbb{Z} : m\mathbb{Z}] = |\mathbb{Z}/m\mathbb{Z}|$$

$$= |\{z + m\mathbb{Z} : z \in \mathbb{Z}\}| = \cdots = m$$

Corollary 2.11.

$$x \in G, \ |x| \mid |G|$$

Proof.

$$|x| = |\langle x \rangle|$$

$$\langle x \rangle \leq G \implies |\langle x \rangle| \mid |G| \implies |x| \mid |G|$$

□

Corollary 2.12: Prime Ordered Groups are Cyclic. *Let $|G|$ be prime. Then G is cyclic.*

Proof. Let $x \in G \setminus \{e\}$.
Then $|x| \mid |G|$.
Since $|G|$ is prime and $|x| \neq 1$, $|x| = |G|$.
So $|\langle x \rangle| = |G|$.
$\implies \langle x \rangle = G$. □

Note 2.11: Groups of a Certain Order.

1. $\{e\}$
2. C_2
3. C_3
4. $C_4, C_2 \times C_2$
5. C_5
6. $C_6, C_2 \times C_3$
7. C_7
8. $C_8, C_2 \times C_4, C_2 \times C_2 \times C_2, D_8$
9. $\vdots$

Proposition 2.21. if $\varphi : G \to H$ hom, then $\exists$bij $\varphi : G/\ker\varphi \to \text{Im}\varphi$.
This bijection is $\varphi = g\ker\varphi \mapsto \varphi(g)$

Proof. $g\ker\varphi$ is the solution set $\varphi(x) = \varphi(g)$.
$\implies \varphi(g\ker(\varphi)) = \{\varphi(g)\}$
$\implies \varphi^{-1}(\{\varphi(g)\}) = g\ker\varphi$
Let $\phi : G/\ker(\varphi) \to H := S \mapsto \varphi(S) = \{x\} \mapsto x$
We know it maps onto $\text{Im}(\varphi)$, and this function as an inverse
$\phi^{-1} : \text{Im}(\varphi) \to G/\ker(\varphi) := x \mapsto \varphi^{-1}(\{x\})$. □

Corollary 2.13.

$$[G : \ker(\varphi)] = \begin{cases} |\text{Im}\varphi| & |\text{Im}\varphi| < \infty \\ \infty & \text{o/w} \end{cases}$$

In particular, $|\text{Im}\varphi| \mid |G|$.

Proposition 2.22. if $|G|$ and $|H|$ *are coprime, then there is no non-trivial hom.*

Proof. $\varphi : G \to H$.
$\implies |\text{Im}\varphi| \mid |G| \implies |\text{Im}\varphi| \mid |H|$
$\implies |\text{Im}\varphi| = 1$
$\implies \text{Im}\varphi = \{e\}$
$\implies \varphi = g \mapsto e$ □

2.7 Normal Subgroups

When is $gH = Hh$?

$H \leq G$. $gH = Hg$ then $g \in Hh$ and $h \in hH$ so $gH = hH = Hh = Hg$. So $gH = Hh \iff gH = Hg$

Definition 2.26: Normal Subgroup. $H \leq G$ *is a* ***normal subgroup*** *if* $gH = Hg\ \forall g \in G$

Notation 2.12: Normal Subgroup. $H \trianglelefteq G$

Definition 2.27: Conjugate. $g, h \in G$. *The* ***conjugate*** *of* h *by* g *is* ghg^{-1}.

Note 2.12. *Since* $gS = \{gs : s \in S\}$ *and* $Sg = \{sg : s \in S\}$ *then* $gSg^{-1} = \{gsg^{-1} : s \in S\}$.

$$gH = Hg \iff gHg^{-1} = H$$

Proposition 2.23. $N \leq G$, *TFAE:*

1. $N \trianglelefteq G$
2. $gNg^{-1} = N \ \forall g \in G$
3. $gNg^{-1} \subseteq N \ \forall g \in G$
4. $G/N = N\backslash G$
5. $G/N \subseteq N\backslash G$
6. $N\backslash G \subseteq G/N$

Example 2.40. $\varphi : G \to H$ *is a hom,* $\ker(\varphi) \trianglelefteq G$.

Proof. $g \ker\varphi = \varphi^{-1}(\varphi(g)) = \ker\varphi g$
$\implies \ker\varphi \trianglelefteq G$ □