Groups and Rings

Carter Aitken

2025-05-05

Abstract

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

Contents

1 Operations on Sets **3**
1.1 K-Ary Operations . . . 3
Definition: Binary Operations . . . 3
1.2 Associative Operations . . . 4
Definition: (Informal) Bracketing . . . 4
Definition: Bracketing . . . 4
Notation: Associativity makes Brackets Pointless . . . 5
Definition: Commutative . . . 5
Definition: Identity . . . 6
Lemma: Uniqueness of Identity . . . 6
Definition: Inverse . . . 6
Lemma: Associtivity implies Uniqueness of Inverses . . . 6
Notation: Inverse . . . 7
Lemma: Properties of the Inverse . . . 8
Lemma: Cancellation Property . . . 8

2 Groups **9**
2.1 Definitions . . . 9
Definition: Group . . . 9
Notation: Multiplicative Notation . . . 9
Definition: Abelian Group . . . 9
Definition: Permutation Group . . . 10
Definition: Order . . . 10
Notation: General Linear Group . . . 10

2.2 Dihedral Groups . . . 11
Definition: N-Gon . . . 11
Definition: An N-Gon Symmetry . . . 11
Definition: Dihedral Group . . . 11
Lemma: Dihedral GROUP . . . 11
Definition: Group Power . . . 11
Definition: Order of an Element . . . 12
Lemma: Properties of Order . . . 12
Proposition: Dihedral Group Explicit Classification . . . 12
2.3 Subgroups . . . 13
Definition: Subgroup . . . 13
Notation: Subgroup . . . 13
Proposition: A Subgroup is a Group . . . 13
Example: The Dihedral Group is a Subgroup of the General Linear Group 14
Definition: Proper Subgroup . . . 14
Example: Subspaces are Subgroups of the Additive Vector Space Group . 15
Notation: (Not in Class) anonymous intersection . . . 16
Definition: Generator . . . 16
Example: Trivial Subgroup generated by the Emptyset . . . 16
Example: Group generated by itself . . . 16
Notation: Redundant Curls . . . 16
Example: Rotations generated by s . . . 16
Notation: Inverse Map of a Set . . . 16
Proposition: Generators make Sets of Powers . . . 17
Definition: Cyclic Groups . . . 17
Definition: Cyclic Subgroups . . . 17
Lemma: Cyclic Group Chacterization into Powers . . . 17
Example: Integers generated by 1 . . . 18
Example: Rationals aren't Cyclic . . . 18
Example: Sets generated by s and r from D2n . . . 18
Proposition: Order of a = Order of gen(a) . . . 18
Example: Integers . . . 19
Example: Modulo Integers . . . 19
Lemma: Set Equality for Generators . . . 19
Example: What generates the modulo integers? . . . 20

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 $a_1, \ldots, a_n \in X$ 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 $a_1, \ldots, a_n$ is*

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

```
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 $a_1, \ldots, a_n$, $n \geq 1$, every bracketing of $a_1, \ldots a_n$ evaluates to the same elem of X.*

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

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

($\Longrightarrow$) 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. $\square$

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 $M_{n\times m} \leftarrow$ (comm). (matrix mul) on $M_n \not\leftarrow$ (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. $e = e \boxtimes e' = e'$ $\square$

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 $(\boxtimes) \leftarrow (\text{assoc})$. If y_L and y_R are left and right inverses of x, then $y_L = y_R$.*

Proof.

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

$\square$

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* $(\boxtimes) \leftarrow (\text{assoc})$ *w/ id* e*.*

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

Proof. $e \boxtimes e = e$ $\square$

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

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

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

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 $(X, \boxtimes)$.

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

$\square$

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.
$(+), \mathrm{id} \leftarrow 0$ or $0_G, \mathrm{inv}(a) = a$.

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

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

   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 $\phi \leftarrow (\text{bij}) : \mathbb{Z} \to \mathbb{Q}$. 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 $\boxtimes \leftarrow$ (assoc, bin op on M, $\mathrm{id} \leftarrow e$), $G := \{g \in M : g \leftarrow (\text{invertable wrt } \boxtimes)\}$. Then G is a group w/ $g \cdot h := g \boxtimes h$.*

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 $\{f : X \to X : f \leftarrow (\text{invertable})\} = \{f \in \text{Fun}(X, X) : f \leftarrow (\text{inv})\}$.*
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.*

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

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

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 $|G| = +\infty$.*

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

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

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

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 $T \in \mathrm{GL}_2\mathbb{R}$ 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}? $\mathrm{Id}(D_{2n}) = I_2$.
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. $D_{2n} = \{s^i : 0 \leq i < n\} \cup \{s^ir : 0 \leq i < n\}$ *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. $H \leq G \implies G \leftarrow$ (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. $\mathbb{Q}_{>0} \leq \mathbb{Q}^\times$

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 $G \leftarrow$ (group) and $H \subseteq G$ is finite. Then $H \subseteq G$ 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. $\langle \{s_1, s_2, \dots\} \rangle =: \langle s_1, s_2, \dots \rangle$

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 $S \subseteq G$, $G \leftarrow$ (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.*

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

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. $i = kn + r \implies a^i = a^r$

$\square$

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.

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

Assume for contradiction it is. Then

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

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 $|\langle a\rangle| \leq |a|$.
$|\langle a\rangle| = \infty = |a|$. If $|\langle a\rangle| = n < \infty$, then

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

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

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

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

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

$\square$

Example 2.13: Integers.

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

Example 2.14: Modulo Integers.

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

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.
$(\impliedby)$

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

$\square$

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

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