

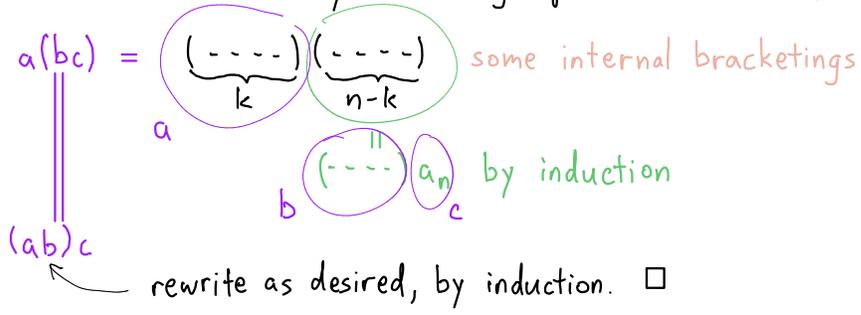
3. Uniqueness

" $\forall a$ " works in any monoid

- identity: For $a \in G$ fixed, $ga = a \Rightarrow g = e$ because $(ga)a^{-1} = g(aa^{-1}) = ge = g$ and $aa^{-1} = e$.
- more generally: operation in G is cancellative: $ab = ac \Rightarrow b = c$
- inverses: $ab = e \Rightarrow b = a^{-1}$ already discussed
- bracketing: $a_1 \dots a_n$ well defined, independent of bracketing

Pf: Induction on n . $n = 3$: $a(bc) = (ab)c$ by def.

$n \geq 4$: Show every bracketing equals $((\dots((a_1 a_2) a_3) \dots) a_{n-1}) a_n$.



Q. $(a_1 \dots a_n)^{-1} = ?$

Def: $a^n = \underbrace{a \dots a}_n$ for $n \in \mathbb{N}$ (so $a^0 = e$) and $a^{-n} = \underbrace{a^{-1} \dots a^{-1}}_n$

Lemma: $a^{r+s} = a^r a^s$ for $r, s \in \mathbb{Z}$. \square

Warning: • Don't write $\frac{a}{b}$. Why? ab^{-1} vs. $b^{-1}a$

• $(ab)^m \neq a^m b^m$ in general

Subgroups of \mathbb{Z}

Q. $H \leq \mathbb{Z} \Rightarrow H = ?$

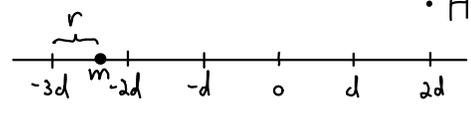
Prop: $H = d\mathbb{Z}$ for some $d \in \mathbb{Z}$.

Pf: $H = \{0\} \Rightarrow d = 0$. \checkmark order of H

Assume $|H| > 1$. Pick $d \in H$ with $d \neq 0$ and $|d|$ minimal. WLOG $d > 0$ since $-d \in H$. absolute value

Claim: $H = d\mathbb{Z}$. Pf: • $d\mathbb{Z} \subseteq H$: $d \in H \Rightarrow \underbrace{d + d + \dots + d}_{n \in \mathbb{Z}} \in H$ quotient remainder

• $H \subseteq d\mathbb{Z}$: Given $m \in H$, write $m = qd + r$ with $0 \leq r < d$.



Then $qd \in H \Rightarrow r = m - qd \in H \Rightarrow r = 0$. \square

E.g. $4\mathbb{Z} + 6\mathbb{Z} = \langle 4, 6 \rangle \subseteq \mathbb{Z}$
= subgroup generated by 4 and 6

abelian = smallest subgroup containing 4 and 6

$$= \{ \alpha \cdot 4 + \beta \cdot 6 \mid \alpha, \beta \in \mathbb{Z} \}.$$

But $\langle 4, 6 \rangle \neq \langle 4 \rangle$ and $\langle 4, 6 \rangle \neq \langle 6 \rangle$; $\langle 4, 6 \rangle = ? \langle 2 \rangle$

Cor: For $a, b \in \mathbb{Z}$, $\langle a, b \rangle = \langle \gcd(a, b) \rangle$. *check!*

Pf: $\langle a, b \rangle = \{ \alpha a + \beta b \mid \alpha, \beta \in \mathbb{Z} \} = d\mathbb{Z}$ by Prop.

$\Rightarrow d \mid a$ and $d \mid b$. But $d = \alpha a + \beta b$ for some $\alpha, \beta \in \mathbb{Z}$,

so $d \mid a$ and $d \mid b \Rightarrow d \mid (\alpha a + \beta b) = d$. \square

• find α, β
• compute d } Euclid's algorithm

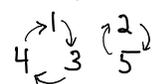
Def: In a group G , the cyclic subgroup generated by $a \in G$ is $\langle a \rangle = \{ \text{powers of } a \}$

$$\text{The order of } a \text{ is } |a| = |\langle a \rangle| = \{ a^n \mid n \in \mathbb{Z} \}.$$

E.g. In $G = \mathbb{Q}^*$, $a = 3 \Rightarrow \langle a \rangle = \{ \dots, 1/9, 1/3, 1, 3, 9, \dots \}$

$$|a| = \infty.$$

E.g. In $G = S_5$, $a = (134)(25)$ is cycle notation for $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$



$$|a| = \cancel{?} \begin{matrix} a^{-2} & a^{-1} & a^0 & a^1 & a^2 & a^3 & a^4 & a^5 & a^6 \\ 6 & a^4 & e & a & (143) & (25) & (134) & (143)(25) & e \end{matrix}$$

E.g. $a = e \Rightarrow |a| = \cancel{?} 1$

Prop: $\{ n \in \mathbb{Z} \mid a^n = e \} \leq \mathbb{Z}$, so it is $d\mathbb{Z}$ for some $d \in \mathbb{N}$.

• $d = 0 \Leftrightarrow |a| = \infty$.

• $d > 0 \Leftrightarrow |a| = d \Leftrightarrow d$ is the smallest positive integer with $a^d = e$.

Pf: S is a subgroup:

$$m, n \in S \Rightarrow a^{m+n} = a^m a^n = e e = e \Rightarrow m+n \in S.$$

$$m \in S \Rightarrow a^{-m} = (a^m)^{-1} = e^{-1} = e \Rightarrow m^{-1} \in S. \checkmark$$

$$\text{Now } a^m = a^n \Leftrightarrow a^{m-n} = e$$

$$\Leftrightarrow m-n \in d\mathbb{Z}$$

$$\bullet d = 0: \Leftrightarrow m = n \checkmark$$

$$\bullet d > 0: \Rightarrow \langle a \rangle = \{ e, a, a^2, \dots, a^{d-1} \}$$

all distinct

$$\text{and } a^d = e. \square$$