Chap 5: Subgroups

Let G be a group. A nonempty subset S of G is called a subgroup if S is closed with respect to multiplication: $a, b \in S \Rightarrow ab \in S$ and S is closed with respect to inverses: $a \in S \Rightarrow a^{-1} \in S$.

Example. $(\mathbb{Z}, +)$ is a subgp. of $(\mathbb{R}, +)$.

set of even integers $(2\mathbb{Z}, +)$ is a subgp. of $(\mathbb{Z}, +)$. (set of odd integers is not a subgroup)

Fact: If G is a group and S is a subgroup, then S itself is a group.

Pf: First notice that $e \in S$: if $a \in S$, then $a^{-1} \in S$ and hence $e = a \cdot a^{-1} \in S$

closed w.r.t. inverses.

closed under mult.

Then G satisfies the axioms of group

$\Rightarrow$ S satisfies the axioms defining a group.

Example: 1. $(\mathcal{F}(\mathbb{R}), +)$ group of functions from $\mathbb{R}$ to $\mathbb{R}$:

identity $e = 0 : \mathbb{R} \to \mathbb{R}$, $x \mapsto 0$. $\forall x \in \mathbb{R}$

$f = f(x) : \mathbb{R} \to \mathbb{R}$ $\Rightarrow (f+g)(x) = f(x) + g(x)$

$g = g(x) : \mathbb{R} \to \mathbb{R}$ $\quad (-f)(x) = -f(x)$.

2. $(\mathcal{C}(\mathbb{R}), +)$ subgroup of continuous functions

3. $(\mathcal{D}(\mathbb{R}), +)$ subgroup of differentiable functions

Ex: Let G be any group. G has 2 trivial subgroups:

$S_1 = \{e\}$,

$S_2 = G$

all other subgps of G are called proper subgroups.

Ex: Suppose G is a group and $A=\{a_1, a_2, \cdots a_n\} \subset G$ is a subset of G. The subgroup generated by A is the subset that consists of all the possible products of elements in A and their inverses. This subgp. will be denoted by $\langle a_1, a_2, \cdots, a_n\rangle$

For example, 1. $A=\{a\}$ then $\langle a\rangle=\{e, a, a^{-1}, a^2, a^{-2}, \cdots, a^k, a^{-k} \cdots\}$

This can be a finite group or infinite group.

$\langle a\rangle$ is also called the cyclic subgroup generated by a.

$|\langle a\rangle|$: order of $\langle a\rangle$ = number of elements in $\langle a\rangle$ is called the order of the element a in G.

examples: • For any $k \in \mathbb{Z}$, $k\mathbb{Z}=\{km : m\in\mathbb{Z}\}$
$$k\mathbb{Z} = \langle k\rangle$$

• If $G=\mathbb{Z}_6$, $\langle 2\rangle=\{0, 2, 4\} \cong \mathbb{Z}_3$

2. $A=\langle a, b\rangle=\{e; a, b, a^{-1}, b^{-1}; ab, ab^{-1}, ba, ba^{-1}$,
$aaa, aab, aab^{-1}, aba, abb, aba^{-1}$
$ab^{-1}a, ab^{-1}a^{-1}, ab^{-1}b^{-1}; baa, \cdots\cdots \}$

there may be repetitions.

how to multiply: $(baba^{-1})(ab^{-1}a^{-2}b) = bab(a^{-1}a)b^{-1}a^{-2}b$
$= ba(bb^{-1})a^{-2}b$
$= baa^{-2}b = ba^{-1}b$.

Ex: $I=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $A=\begin{pmatrix}0&1\\1&0\end{pmatrix}$, $B=\begin{pmatrix}\cos\frac{2\pi}{3} & -\sin\frac{2\pi}{3}\\ \sin\frac{2\pi}{3} & \cos\frac{2\pi}{3}\end{pmatrix}=\begin{pmatrix}-\frac{1}{2} & -\frac{\sqrt{3}}{2}\\ \frac{\sqrt{3}}{2} & -\frac{1}{2}\end{pmatrix}$,

A, B satisfies the relation: $\boxed{A^2=I,\ B^3=I,\ AB^2=BA.\ (*)}$

$\Rightarrow \langle A,B\rangle=\{I,\ A,\ B,\ B^2,\ AB,\ BA\}$ is a group of order 6.

$\langle A\rangle=\{I,A\}$, $\langle B\rangle=\{I,B,B^2\}$.

$\langle AB\rangle=\{I,\ AB,\ \underset{\underset{ABAB=AAB^2B}{\parallel}}{(AB)^2}=I\}=\{I,AB\}$

$\langle BA\rangle=\{I,\ BA,\ \underset{\underset{BABA}{\parallel}}{(BA)^2}=\underset{\underset{AB^2BA}{\parallel}}{I}\}=\{I,BA\}$

$BABA=AB^2BA$

The operation table is determined by $(*)$. so $(*)$ is called a set of defining equations.

Exercises. A: Recognizing subgroups

1. $G=\langle\mathbb{R},+\rangle$, $H=\{\log a : a\in\mathbb{Q},\ a>0\}$

(i) $\log a+\log b=\log(ab)$ $\quad a,b\in\mathbb{Q}_{>0}\Rightarrow ab\in\mathbb{Q}_{>0}$ So: H is closed w.r.t. multiplication

(ii) $-\log a=\log\frac{1}{a}$ $\quad a\in\mathbb{Q}_{>0}\Rightarrow a^{-1}\in\mathbb{Q}_{>0}$ So H is closed w.r.t. inverses

$\Rightarrow$ H is a subgroup of G.

B. 5. $G = \langle \mathcal{D}(\mathbb{R}), + \rangle$, $H = \{f \in \mathcal{D}(\mathbb{R}) : \frac{df}{dx} \text{ is constant}\}$

(i) $f, g \in H \Rightarrow \frac{d}{dx}(f+g) = \frac{df}{dx} + \frac{dg}{dx}$ is constant $\Rightarrow f+g \in H$

(ii) $f \in H \Rightarrow \frac{d}{dx}(-f) = -\frac{df}{dx}$ is a constant $\Rightarrow -f \in H$

$\Rightarrow H$ is a sub group of G

C. subgps of Abelian gps. Assume: G is commutative (i.e. abelian)

5. Let H be a sbgp. of G. $K = \{x \in G : \exists \text{ integer } n > 0 \text{ s.t. } x^n \in H\}$.

(i) $x, y \in G \Rightarrow \exists n_1, n_2 \; x^{n_1} \in H, y^{n_2} \in H \Rightarrow (xy)^{n_1 n_2} \underset{\substack{\uparrow \\ G \text{ is commutative}}}{=} (x^{n_1})^{n_2} (y^{n_2})^{n_1} \in H$

(ii) $x \in G \Rightarrow \exists n \; x^n \in H \Rightarrow (x^{-1})^n = (x^n)^{-1} \in H$

Not True in general if G is not abelian (i.e. not commutative)

Ex: $G = \mathbb{Z}_2 * \mathbb{Z}_2 = \langle a, b \mid a^2 = e, b^2 = e \rangle$

$H = \{e\}$ $\quad (ab)^n = \underbrace{(ab)(ab)\cdots(ab)}_{n} \neq e$.

D. subgroups ~~of~~ an arbitrary group.

7. $H < G$ $\quad K = \{x \in G : xax^{-1} \in H \text{ iff } a \in H\}$

(a) K is a subgp. of G:

(i) If $x, y \in K$, then: $(xy)a(xy)^{-1} = x(yay^{-1})x^{-1} \in H \overset{x \in K}{\iff} yay^{-1} \in H \iff a \in H$

$\Rightarrow x \cdot y \in K$

(ii) If $x \in K$, then: • $x^{-1}a(x^{-1})^{-1} = x^{-1}ax \in H \Rightarrow a = xbx^{-1} \in H$, where $b = x^{-1}ax$

• $a \in H$ & $x^{-1}ax = b \Rightarrow xbx^{-1} \in H \overset{x \in K}{\iff} b \in H$

(b) H is a subgp. of K. Just need to show $H \subset K$

$x \in H$. $xax^{-1} = b \in H \Rightarrow a = x^{-1}bx \in H$

$a \in H \Rightarrow xax^{-1} \in H$

so $xax^{-1} \in H$ iff $a \in H$.

5. Interesting reduction: Let G be a finite gp., S be a nonempty subset of G. Suppose S is closed w.r.t. multiplication. Then S is a subgp. of G (i.e. S is also closed w.r.t. inverses).

E. Generators of gps.

1. List all the cyclic gps. of $\langle \mathbb{Z}_{10}, + \rangle$

- $\{0\}$. $\mathbb{Z}_{10}$ are trivial subgps.
- $\{0, 2, 4, 6, 8\}$, $\langle 3 \rangle = \{0, 3, 6, 9, 2, 5, 8, 1\} = \mathbb{Z}_{10}$

$\langle 4 \rangle = \{0, 4, 8, 2, 6\} = \langle 2 \rangle$, $\langle 5 \rangle = \{0, 5\}$

$\langle 6 \rangle = \{0, 6, 2, \cdots\} = \langle 2 \rangle$, $\langle 7 \rangle \ni \overline{21} = \overline{1} \Rightarrow \langle 7 \rangle = \mathbb{Z}_{10}$

$\langle 8 \rangle \ni \overline{32} = \overline{2} \Rightarrow \langle 8 \rangle = \langle 2 \rangle$, $\langle 9 \rangle \ni \overline{81} = \overline{1} \Rightarrow \langle 9 \rangle = \mathbb{Z}_{10}$

$\Rightarrow$ all different cyclic gps: $\{0\}$, $\mathbb{Z}_{10}$, $\langle 2 \rangle$, $\langle 5 \rangle$

2. $\mathbb{Z}_{10} = \langle 2, 5 \rangle$ because $2 \times (-2) + 5 = 1 \in \langle 2, 5 \rangle$

$\Rightarrow \langle 2, 5 \rangle \subset \langle 1 \rangle = \mathbb{Z}_{10}$.

F. Groups determined by generators and defining equations.

$G = \langle a, b \mid a^4 = e,\ a^2 = b^2,\ ba = ab^3 \rangle \simeq \{1, -1, i, -i, j, -j, k, -k\}$

$1 = e,\ -1 = b^2,\ i = a,\ -i = ab^2,\ j = b,\ -j = b^3,\ k = ab,\ -k = ab^3$

	$1 = e$	$i = a$	$j = b$	$-1 = b^2$	$-j = b^3$	$k = ab$	$-i = ab^2$	$-k = ab^3$
$1 = e$	e	a	b	b^2	b^3	ab	ab^2	ab^3
$i = a$	a	b^2	ab	ab^2	ab^3	b^3	e	b
$j = b$	b	ab^3	b^2	b^3	e	a	ab	ab^2
$-1 = b^2$	b^2	ab^2	b^3	e	b	ab^3	a	ab
$-j = b^3$	b^3	ab	e	b	b^2	ab^2	ab^3	a
$k = ab$	ab	b	ab^2	ab^3	a	b^2	b^3	e
$-i = ab^2$	ab^2	e	ab^3	a	ab	b	b^2	b^3
$-k = ab^3$	ab^3	b^3	a	ab	ab^2	e	b	b^2

$i^4 = (-1)^2 = 1 \Leftrightarrow a^4 = e$

$i^2 = -1 = j^2 \Leftrightarrow a^2 = b^2$

$ji = -k = ij^3 \Leftrightarrow ba = ab^3$

Sudoku

G. Cayley Diagrams.

Every finite gp. may be represented by a diagram known as Cayley diagram. A Cayley diagram consists of points joined by arrows.

- There is one point for every element of the group.
- The arrows represent the result of multiplying by a generator.

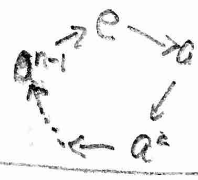
Ex: $G = \langle a \rangle$:

$\longrightarrow$: multiply by a

$e \to a \to a^2 \to \cdots$

infinite cyclic

or



finite cyclic gp.

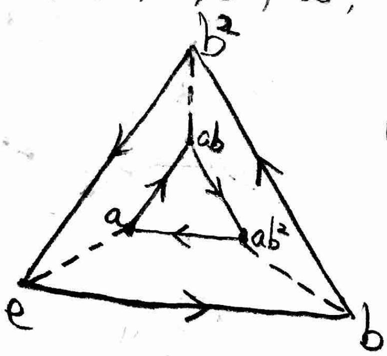
Ex: $G = \{e, a, b, b^2, ab, ab^2\} = \langle a, b \mid a^2 = e = b^3,\ ba = ab^2 \rangle$

$G = \langle a, b \rangle$

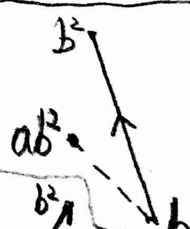
$\longrightarrow$: multiply by b on the right

$\dashrightarrow$: multiply by a

- - - - without arrow if $a^2 = e$ (i.e. $a = a^{-1}$)

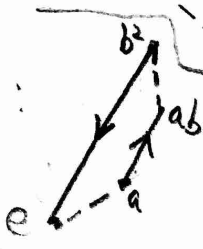


$(ab^2)(ab) = b^2$:



$(ab)^{-1}$:

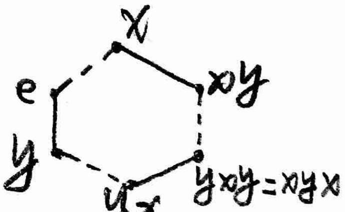
$ab = b^{-1}a$



A point-and-arrow diagram is the Cayley diagram of a group iff it has the following 2 properties:

(a) For each point x and generator a, there is exactly one a-arrow starting at x, and exactly one a-arrow ending at x; furthermore at most one arrow goes from x to another point y.

(b) If two different paths starting at x lead to the same destination then these two paths, starting at any point y, lead to the same destination.



	e	x	y	xy	yx	yxy
e	e	x	y	xy	yx	yxy
x	x	e	xy	y	yxy	yx
y	y	yx	e	yxy	x	xy
xy	xy	yxy	x	yx	e	y
yx	yx	y	yxy	e	xy	x
yxy	yxy	xy	yx	x	y	e

$\langle x, y \mid x^2=e, y^2=e, yxy=xyx \rangle$

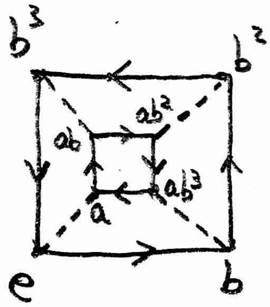
$\cong$

$\langle a, b \mid a^2=e, b^3=e, ba=ab^2 \rangle$

$a=x, \quad b=yx$

$ba = yx^2 = y =$

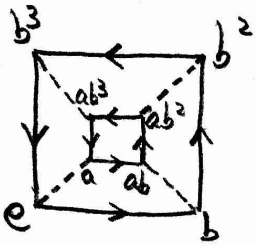
$ab^2 = x\, yxyx = yxy\, yx = y$



	e	a	b	b^2	b^3	ab	ab^2	ab^3
e	e	a	b	b^2	b^3	ab	ab^2	ab^3
a	a	e	ab	ab^2	ab^3	b	b^2	b^3
b	b	ab^3	b^2	b^3	e	a	ab	ab^2
b^2	b^2	ab^2	b^3	e	b	ab^3	a	ab
b^3	b^3	ab	e	b	b^2	ab^2	ab^3	a
ab	ab	b^3	ab^2	ab^3	a	e	b	b^2
ab^2	ab^2	b^2	ab^3	a	ab	b^3	e	b
ab^3	ab^3	b	a	ab	ab^2	b^2	b^3	e

$\langle a, b \mid a^2=e, b^4=e, ab=b^{-1}a \rangle \simeq D_4$

5.

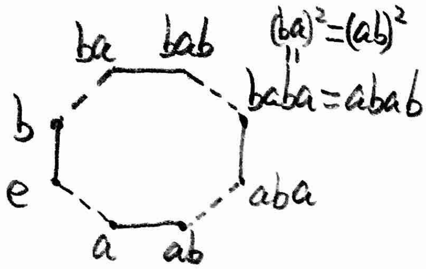


	e	a	b	b^2	b^3	ab	ab^2	ab^3
e	e	a	b	b^2	b^3	ab	ab^2	ab^3
a	a	e	ab	ab^2	ab^3	b	b^2	b^3
b	b	ab	b^2	b^3	e	ab^2	ab^3	ab^4
b^2	b^2	ab^2	b^3	e				
b^3	b^3							
ab	ab							
ab^2	ab^2							
ab^3	ab^3							

$G = \langle a, b \mid a^2 = e, b^4 = e, ab = ba \rangle$

$= \mathbb{Z}_2 \times \mathbb{Z}_4$

3.



$baba = abab = (ab)^2$

	e	a	b	ab	ba	aba	bab	$(ab)^2$
e	e	a	b	ab	ba	aba	bab	$(ab)^2$
a	a	e	ab	b	aba	ba	$(ab)^2$	bab
b	b	ba	e	bab	a	$(ab)^2$	ab	aba
ab	ab	aba	a	$(ab)^2$	e	bab	b	ba
ba	ba	b	bab	e	$(ab)^2$	a	aba	ab
aba	aba	ab	$(ab)^2$	a	bab	e	ba	b
bab	bab	$(ab)^2$	ba	aba	b	ab	e	a
$(ab)^2$	$(ab)^2$	bab	aba	ba	ab	b	a	e

$G = \langle a, b \mid a^2 = b^2 = e, abab = baba \rangle$

Claim: $G \cong D_4$.

Let $x = ab$, $y = b$. Then $x^4 = e$, $y^2 = e$. $y^{-1}xy = babb = ba$

$\phantom{y^{-1}xy} \parallel \qquad\qquad \parallel$

$x^3 = ababab = bababb$

So $G = \langle x, y \mid x^4 = e, y^2 = e, xy = yx^3 \rangle \cong D_4$

Quaternion group: $G = \langle a, b \mid a^4 = e, a^2 = b^2, ba = ab^3 \rangle$