Chap 4: properties of groups

1. there is exactly one identity element: if e_1 and e_2 are identity elements, then $e_1 = e_1 * e_2 = e_2$.

2. each element has exactly one inverse: if $a*a_1 = a_1 * a = e$, $a*a_2 = a_2*a = e$, then

$$a_1*a*a_2 = (a_1*a)*a_2 = e*a_2 = a_2$$
$$\| \quad a_1*(aa_2) = a_1*e = a_1 \quad /\!/$$

additive notation: $a+b$: $e=0$, $a^{-1}=-a$ (used for commutative operations)

multiplicative notation: $a \cdot b$ or ab.

Thm 1 (Cancellation law): $ab=ac \Rightarrow b=c$, $ba=ca \Rightarrow b=c$.

Pf: $ab=ac \Rightarrow a^{-1}(ab) = a^{-1}(ac)$

$$\begin{array}{ccc} a^{-1}(ab) & = & a^{-1}(ac) \\ \| & & \| \\ (a^{-1}a)\,b & & (a^{-1}a)\,c \\ \| & & \| \\ e \cdot b = b & = & c = e \cdot c \end{array}$$

Caution: $ab = ca \not\Rightarrow b=c$ in general if not commutative.

Thm 2: $ab=e \Rightarrow a=b^{-1}$ and $b=a^{-1}$.

Pf: $ab = e = a \cdot a^{-1} \xrightarrow{\text{Cancellation}} b=a^{-1}$

Thm 3: $(ab)^{-1} = b^{-1}a^{-1}$

$$(a^{-1})^{-1} = a$$

$abcd = ((ab)c)d = (ab)(cd) = a((bc)d) = a(b(cd)) = \cdots$

key point: by associative law, parentheses are redundant.

$\boxed{(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}}$ inverse of products.

notation: if G is a finite group, then $|G|$ denotes the order of group G = # elements in G.

Exercises:

A: Solving equations in groups.

1. $x^2 = b$ & $x^5 = e$: $\begin{cases} x^4 = b^2 \\ x^5 = e \end{cases} \Rightarrow x = x^5 (x^4)^{-1} = e(b^2)^{-1} = b^{-2}$

2. $x^2 b = x a^{-1} c \Rightarrow \underbrace{x^{-1} x^2}_{= x} = a^{-1} c \cdot b^{-1}$

3. $\begin{cases} x^2 a = b x c^{-1} \\ acx = xac \end{cases} \Rightarrow \underbrace{x^2 ac}_{= x\,x(ac) = x(ac)x = (ac)x^2} = bx$, $(ac)x = x(ac)$

$\Rightarrow b = x(ac) = (ac)x \Rightarrow \boxed{\begin{array}{c} x = b(ac)^{-1} \\ \| \\ (ac)^{-1} b \end{array}}$ (*)

$\Rightarrow x = x^2 (x^{-1}) = (ac)^{-1} b$
$= c^{-1} a^{-1} b$

check: $x^2 a = (ac)^{-1} b (ac)^{-1} b \cdot a$. $bxc^{-1} = b(ac)^{-1} b \cdot c^{-1}$

$(ac)x = ac(ac)^{-1} b = b$. $xac = (ac)^{-1} b (ac)$.

(*) $\Rightarrow$ b commutes with (ac) $\Rightarrow$ equations are satisfied.

B. Rules of algebra in groups. <u>true or False</u>

1. $x^2 = e \Rightarrow x = e$ False: $(\mathbb{Z}_2, +)$

3. $(ab)^2 = a^2 b^2$ <u>False</u>. true only if a commutes with b.

$\begin{array}{l} (ab)^2 = abab \\ \quad \| \\ a^2 b^2 = aabb \end{array} \Rightarrow ba = ab$

C. elements that commute:

1. $ab = ba \Rightarrow a^{-1}b^{-1} = (ba)^{-1} = (ab)^{-1} = b^{-1}a^{-1}$

2. $ab = ba \Rightarrow b^{-1}a = ab^{-1}$ i.e. b^{-1} commutes with a.

D. gp. elements and their inverses.

2. $abc = e \Rightarrow c = (ab)^{-1} = c \cdot ab = e$

$\Rightarrow a = (bc)^{-1} = bca = e$.

F: Constructing Small Groups.

4. There is exactly one group G of 4 elements, say $G = \{e, a, b, c\}$ satisfying additional property that $x \cdot x = e$ for every $x \in G$.
complete the table of operation:

	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e

$\longrightarrow$

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

isomorphic

G. Direct product $G \times H = \{(x, y) : x \in G, y \in H\}$ $(x,y)\cdot(x',y') = (xx', yy')$

Ex: $\mathbb{Z}_2 \times \mathbb{Z}_2$

	(0,0)	(1,0)	(0,1)	(1,1)
(0,0)	(0,0)	(1,0)	(0,1)	(1,1)
(1,0)	(1,0)	(0,0)	(1,1)	(0,1)
(0,1)	(0,1)	(1,1)	(0,0)	(1,0)
(1,1)	(1,1)	(0,1)	(1,0)	(0,0)