Prop 2: $\forall a \in G$, a^{-1} is unique

Cancellation Law

left cancellation law:

$a \cdot b = a \cdot c$, $a, b, c \in G$

$\Rightarrow b = c$

right cancellation law

$a \cdot b = c \cdot b$

$\Rightarrow a = c$

Prop 3: Cancellation Law Holds In a Group

Proof: $(G, \cdot)$

$a \cdot b = a \cdot c$

$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c)$ Id.

$(a^{-1} \cdot a) \cdot b = (a^{-1} \cdot a) \cdot c$ Assoc

$e \cdot b = e \cdot c$

$b = c$

More examples

1) $\mathbb{Z}_n$, integers modulo n

operation in $\mathbb{Z}_5$?

1) addition modulo 5

2) multiplication modulo 5

$(\mathbb{Z}_5, +)$

Cayley Table

$(G, \cdot)$ finite group

$\cdot$	a_1	a_2	...	a_n
a_1	$a_1 \cdot a_1$	$a_1 \cdot a_2$	...	$a_1 \cdot a_n$
a_2	$a_2 \cdot a_1$			
⋮				
a_n	$a_n \cdot a_1$	...		$a_n \cdot a_n$

for $(\mathbb{Z}_5, +_5)$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

1) closure ✓

2) identity ✓ 0

3) inverse ✓ inv of $a = -a \bmod 5$

4) associativity ✓

→ group

also abelian group (commutes)

2) Group of units modulo n, $U(n)$

e.g. $n=4$

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

identity [1]