Cancellation Rules

Theorem: Right Cancellation

Let G be a group:

$$\forall\, a, b, c \in G, a = b \iff ac = bc$$

Proof

Assume $a, b, c \in G$
Let $e \in G$ be the identity element.

$\implies$ Assume $a = b$

The binary operation is well-defined,
$\therefore ac = bc$

$\impliedby$ Assume $ac = bc$

$c^{-1} \in G$
$(ac)c^{-1} = (bc)c^{-1}$
$a(cc^{-1}) = b(cc^{-1})$
$ae = be$
$\therefore a = b$

Theorem: Left Cancellation

Let G be a group:

$$\forall\, a, b, c \in G, a = b \iff ca = cb$$

Proof

Assume $a, b, c \in G$
Let $e \in G$ be the identity element.

$\implies$ Assume $a = b$

The binary operation is well-defined,
$\therefore ca = cb$

$\impliedby$ Assume $ca = cb$

$c^{-1} \in G$
$c^{-1}(ca) = c^{-1}(cb)$
$(c^{-1}c)a = (c^{-1}c)b$
$ea = eb$
$\therefore a = b$

Theorem

Let G be a group:

$$\forall\, a, b \in G, ax = b \text{ has a unique solution in } G$$

Proof

First, show that there is at least one solution:
Let $x = a^{-1}b$
$ax = a(a^{-1}b) = (aa^{-1})b = eb = b$
$\therefore x = a^{-1}b$ is a solution.

Now, show uniqueness:
Assume that there are two solutions: x_1 and x_2
$ax_1 = ax_2$
$\therefore x_1 = x_2$

Theorem

Let G be a group:

$$\forall\, a, b \in G, xa = b \text{ has a unique solution in } G$$

Proof

First, show that there is at least one solution:
Let $x = ba^{-1}$
$xa = (ba^{-1})a = b(a^{-1}a) = be = b$
$\therefore x = ba^{-1}$ is a solution.

Now, show uniqueness:
Assume that there are two solutions: x_1 and x_2
$x_1a = x_2a$
$\therefore x_1 = x_2$