

Basic Theory of Groups

(Section 2.1)

Recall: a group is a set G endowed
with a binary operation " \cdot "
that is associative and such
that an identity and inverse
elements exist.

Proposition: (Uniqueness of identity)

The identity element in any group is unique.

proof: Suppose G is a group under " \cdot " and suppose $\exists e, f \in G$ such that

$$e \cdot x = x \cdot e = f \cdot x = x \cdot f = x$$

$\forall x \in G$.

Then in $e \cdot x = x \cdot e = x$,

set $x = f$:

$$e \cdot f = f \cdot e = f$$

In $f \cdot x = x \cdot f = x$,

Set $x = e$,

$$f \cdot e = e \cdot f = e$$

Therefore, $f = e$.



Proposition : (uniqueness of inverse)

The inverse of any element in a group is unique.

Proof: Let G be a group under " \cdot ".

Let $x \in G$ and suppose \exists

$y, z \in G$ with

$$x \cdot y = y \cdot x = e$$

$$x \cdot z = z \cdot x = e$$

where e is the (unique!) identity of G .

Then we have

$$y = y \cdot e = y \cdot (x \cdot z)$$

$$= (y \cdot x) \cdot z \quad (\text{associativity})$$

$$= e \cdot z$$

$$= z$$

So $y = z$.

□

Notation: If G is a group under " \cdot " and $x \in G$, denote by x^{-1} the (unique!) inverse of x . The identity of G will be denoted by e or e_G if there is a chance of confusion.

Corollary: (inverse of the inverse) If

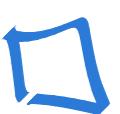
G is a group under " \cdot "

and $x \in G$, $(x^{-1})^{-1} = x$.

Proof: Since $x \cdot (x^{-1}) = (x^{-1}) \cdot x = e$,

by uniqueness of the inverse,

$$(x^{-1})^{-1} = x.$$



* Corollary: (cancellation) Let G be
a group under " \cdot ".

Then if $x, y, z \in G$,

$$x \cdot y = x \cdot z \Rightarrow y = z$$

and

$$y \cdot x = z \cdot x \Rightarrow y = z.$$

Proof: Suppose

$$x \cdot y = x \cdot z.$$

Then

$$x^{-1} \cdot (x \cdot y) = x^{-1} \cdot (x \cdot z)$$

and using associativity,

$$(x^{-1} \cdot x) \cdot y = x^{-1} \cdot (x \cdot y) = x^{-1} \cdot (x \cdot z) = (x^{-1} \cdot x) \cdot z$$

and so

$$e \cdot y = e \cdot z \quad \text{and}$$

$$y = z.$$

Similarly, if

$$yx = zx, \quad y = z$$

by multiplying on the
right by x^{-1} .



Recall: if G and H are groups with operations both abusively denoted by " \cdot ", an isomorphism of groups is a bijection

$\varphi: G \rightarrow H$ such that

$\forall x, y \in G,$

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$$

Proposition : (isomorphism properties)

Let $\varphi: G \rightarrow H$ be an isomorphism. Then

$$\underline{\varphi(e_G) = e_H} \quad \text{and}$$

$$\forall x \in G,$$

$$\underline{\varphi(x^{-1}) = \varphi(x)^{-1}}$$

Proof: Let $y \in H$. Then since φ is a bijection, $\exists x \in G$,

$$\varphi(x) = y.$$

Then

$$\begin{aligned}\varphi(e_6) \cdot y &= \varphi(e_6) \cdot \varphi(x) \\ &= \varphi(e_6 \cdot x) \\ &= \varphi(x) \\ &= y\end{aligned}$$

Similarly,

$$y \cdot \varphi(e_6) = y, \text{ so}$$

by uniqueness of identity in H ,

$$\varphi(e_6) = e_H -$$

Since we know $\varphi(e_6) = e_H$,
taking $x \in G$,

$$e_H = \varphi(e_6) = \varphi(x \cdot x^{-1}) = \varphi(x) \cdot \varphi(x^{-1})$$

similarly,

$$e_H = \varphi(x^{-1}) \cdot \varphi(x), \text{ so}$$

by uniqueness of inverses in H ,

$$\varphi(x)^{-1} = \varphi(x^{-1}).$$

