Theorem (Natural Homomorphism)

Let

- R *be a congruence relation on a groupoid* $(G, *)$
- $(G/R, \circledast)$ *be the corresponding quotient groupoid*

Then the function $f_R : G \to G/R$ *defined by*

- $f_R(a) = [a]$

is an onto homomorphism, called the natural homomorphism.

Natural Homomorphism.

If $[a] \in G/R$, then

- $f_R(a) = [a]$
- So f_R is an onto function

If a and b are elements of G, then

- $f_R(a * b) = [a * b] = [a] \circledast [b] = f_R(a) \circledast f_R(b)$

So f_R is a homomorphism. ❀

Theorem (Fundamental Homomorphism Theorem)

Let

- $f : G \to G'$ *be a homomorphism of the groupoid* $(G, \ *)$ *onto the groupoid* $(G', \ *')$
- R *be the relation on* G *defined by,* $\forall a, b \in G$
  - $a \ R \ b$ *if and only if* $f(a) = f(b)$

Then

- R *is a congruence relation*
- $(G', \ *')$ *and the quotient groupoid* $(G/R, \ \circledast)$ *are isomorphic*

Proof: R is an equivalence relation.

- $a \ R \ a$ for every $a \in S$, since $f(a) = f(a)$
- if $a \ R \ b$, then $f(a) = f(b)$, so bRa
- if $a \ R \ b$ and $b \ R \ c$
  - $f(a) = f(b)$ and $f(b) = f(c)$
  - so $f(a) = f(c)$ and $a \ R \ c$

Hence R is an equivalence relation. ❀

Proof: R is a congruence relation.

- Suppose that $a \; R \; a_1$ and $b \; R \; b_1$
- $f(a) = f(a_1)$ and $f(b) = f(b_1)$
- $f(a * b) = f(a) *' f(b) = f(a_1) *' f(b_1) = f(a_1 * b_1)$
    - since f is a homomorphism

Hence $(a * b) \; R \; (a_1 * b_1)$

Proof: $\overline{f}$ is a function.

$\overline{f} \stackrel{\text{def}}{=} \{([a],\ f(a)) | [a] \in G/R\}$: a relation from G/R to G'

- Suppose that $[a] = [a']$
- $a\ R\ a'$, so $f(a) = f(a')$, which implies that $\overline{f}$ is a function.
- write $\overline{f} : G/R \to G'$, where $\overline{f}([a]) = f(a)$ for $[a] \in G/R$.

❀

Proof: $\overline{f}$ is a one to one function.

$\overline{f} \stackrel{\text{def}}{=} \{([a],\ f(a))|[a] \in G/R\}$: a relation from G/R to G'

- Suppose that $\overline{f}([a]) = \overline{f}([a'])$
- $f(a) = f(a')$, so $a\ R\ a'$, which implies that $[a] = [a']$.
- Hence $\overline{f}$ is one to one.

❀

Proof: $\overline{f}$ is an onto function.

$\overline{f} \overset{\text{def}}{=} \{([a],\ f(a)) | [a] \in G/R\}$: a relation from G/R to G'

- Suppose that $b \in G'$
- $f(a) = b$ for some element $a \in G$, since f is onto,
- $\overline{f}([a]) = f(a) = b$, so $\overline{f}$ is onto.

❀

Proof: $\overline{f}$ is an isomorphism.

$\overline{f} \stackrel{\text{def}}{=} \{([a],\ f(a)) | [a] \in G/R\}$: a relation from G/R to G'

$$
\begin{aligned}
\overline{f}([a] \circledast [b]) &= \overline{f}([a * b]) \\
&= f(a * b) \\
&= f(a) *' f(b) \\
&= \overline{f}([a]) *' \overline{f}([b])
\end{aligned}
$$

❀

Proof: $\overline{f}$ is an isomorphism.

$\overline{f} \stackrel{\text{def}}{=} \{([a],\ f(a)) | [a] \in G/R\}$: a relation from G/R to G'

$$\begin{aligned} \overline{f}([a] \circledast [b]) &= \overline{f}([a * b]) \\ &= f(a * b) \\ &= f(a) *' f(b) \\ &= \overline{f}([a]) *' \overline{f}([b]) \end{aligned}$$

Proof: $\overline{f}$ is an isomorphism.

$\overline{f} \overset{\text{def}}{=} \{([a],\ f(a)) | [a] \in G/R\}$: a relation from G/R to G'

$$\begin{aligned}\overline{f}([a] \circledast [b]) &= \overline{f}([a * b]) \\ &= f(a * b) \\ &= f(a) *' f(b) \\ &= \overline{f}([a]) *' \overline{f}([b])\end{aligned}$$

❀

Fundamental Homomorphism Theorem

Proof: $\overline{f}$ is an isomorphism.

$\overline{f} \stackrel{\text{def}}{=} \{([a],\ f(a)) | [a] \in G/R\}$: a relation from G/R to G'

$$\begin{aligned}
\overline{f}([a] \circledast [b]) &= \overline{f}([a * b]) \\
&= f(a * b) \\
&= f(a) *' f(b) \\
&= \overline{f}([a]) *' \overline{f}([b])
\end{aligned}$$

Fundamental Homomorphism Theorem

Notice

- The Theorem can be described by the diagram on the right.
  - f_R is the natural homomorphism.
- It follows from the definitions of f_R and $\overline{f}$ that
  - $\overline{f} \circ f_R = f$
- Since
  - $(\overline{f} \circ f_R)(a) = \overline{f}(f_R(a)) = \overline{f}([a]) = f(a)$

$$
\begin{tikzcd}
G \arrow[rr, "f"] \arrow[dr, "f_R"'] & & G' \\
& G/R \arrow[ur, "\overline{f}"'] &
\end{tikzcd}
$$

Definition (Normal Subgroup)

Let

- H be a subgroup of a group G
- $a \in G$

The left and right coset of H in G determined by a is the set

- $aH = \{ah | h \in H\}$
- $Ha = \{ha | h \in H\}$

A subgroup H of G is normal if $aH = Ha$, for all $a \in G$

Warning

- If $Ha = aH$, it does not follow that, for $h \in H$ and $a \in G$, $ha = ah$.
- But $ha = ah'$, where h' is some other element in H.

Example

Let

- G be the symmetric group S_3
- The subset $H = \{f_1, g_2\}$ is a subgroup of G

Compute all the distinct left cosets of H in G.

Solution: $H = \{f_1, g_2\}$

- $f_1H = g_2H = H$
- $f_2H = \{f_2, g_1\}$
- $f_3H = \{f_3, g_3\}$
- $g_1H = \{g_1, f_2\} = f_2H$
- $g_3H = \{g_3, f_3\} = f_3H$

The distinct left cosets

- H, f_2H, and f_3H.

$(S_3, *)$

$*$	f_1	f_2	f_3	g_1	g_2	g_3
f_1	f_1	f_2	f_3	g_1	g_2	g_3
f_2	f_2	f_3	f_1	g_3	g_1	g_2
f_3	f_3	f_1	f_2	g_2	g_3	g_1
g_1	g_1	g_2	g_3	f_1	f_2	f_3
g_2	g_2	g_3	g_1	f_3	f_1	f_2
g_3	g_3	g_1	g_2	f_2	f_3	f_1

Theorem

If K is a finite subgroup of a group G, then every left coset of K in G has exactly as many elements as K.

Theorem (Lagrange's Group Theorem)

The order of a subgroup divides the order of the Group.

Theorem

If K is a finite subgroup of a group G, then every left coset of K in G has exactly as many elements as K.

Theorem (Lagrange's Group Theorem)

The order of a subgroup divides the order of the Group.

Proof.

- Let
  - aK be a left coset of K in G, where $a \in G$
  - $f : K \to aK$ be defined by $f(k) = ak$, for $k \in K$
- f is one to one
- f is onto
- Therefore, f is bijection, K and aK have the same number of elements.

Proof.

- Let
  - aK be a left coset of K in G, where $a \in G$
  - $f : K \to aK$ be defined by $f(k) = ak$, for $k \in K$
- f is one to one
- f is onto
- Therefore, f is bijection, K and aK have the same number of elements.

Proof.

- Let
  - aK be a left coset of K in G, where $a \in G$
  - $f : K \to aK$ be defined by $f(k) = ak$, for $k \in K$
- f is one to one
  - Assume that $f(k_1) = f(k_2)$, for $k_1, k_2 \in K$
  - $ak_1 = ak_2$
  - $k_1 = k_2$, by left multiplying a^{-1}
  - f is one to one
- f is onto
- Therefore, f is bijection, K and aK have the same number of elements.

Proof.

- Let
  - aK be a left coset of K in G, where $a \in G$
  - $f : K \to aK$ be defined by $f(k) = ak$, for $k \in K$
- f is one to one
  - Assume that $f(k_1) = f(k_2)$, for $k_1, k_2 \in K$
  - $ak_1 = ak_2$
  - $k_1 = k_2$, by left multiplying a^{-1}
  - f is one to one
- f is onto
- Therefore, f is bijection, K and aK have the same number of elements.

Proof.

- Let
  - aK be a left coset of K in G, where $a \in G$
  - $f : K \to aK$ be defined by $f(k) = ak$, for $k \in K$
- f is one to one
  - Assume that $f(k_1) = f(k_2)$, for $k_1, k_2 \in K$
  - $ak_1 = ak_2$
  - $k_1 = k_2$, by left multiplying a^{-1}
  - f is one to one
- f is onto
- Therefore, f is bijection, K and aK have the same number of elements.

Proof.

- Let
  - aK be a left coset of K in G, where $a \in G$
  - $f : K \to aK$ be defined by $f(k) = ak$, for $k \in K$
- f is one to one
  - Assume that $f(k_1) = f(k_2)$, for $k_1, k_2 \in K$
  - $ak_1 = ak_2$
  - $k_1 = k_2$, by left multiplying a^{-1}
  - f is one to one
- f is onto
- Therefore, f is bijection, K and aK have the same number of elements.

Proof.

- Let
  - aK be a left coset of K in G, where $a \in G$
  - $f : K \to aK$ be defined by $f(k) = ak$, for $k \in K$
- f is one to one
- f is onto
- Therefore, f is bijection, K and aK have the same number of elements.

Proof.

- Let
  - aK be a left coset of K in G, where $a \in G$
  - $f : K \to aK$ be defined by $f(k) = ak$, for $k \in K$
- f is one to one
- f is onto
  - Let b be an arbitrary element in aK
  - $b = ak$ for some $k \in K$
  - $f(k) = ak = b$
  - f is onto.
- Therefore, f is bijection, K and aK have the same number of elements.

Proof.

- Let
  - aK be a left coset of K in G, where $a \in G$
  - $f : K \to aK$ be defined by $f(k) = ak$, for $k \in K$
- f is one to one
- f is onto
  - Let b be an arbitrary element in aK
  - $b = ak$ for some $k \in K$
  - $f(k) = ak = b$
  - f is onto.
- Therefore, f is bijection, K and aK have the same number of elements.

Proof.

- Let
  - aK be a left coset of K in G, where $a \in G$
  - $f : K \to aK$ be defined by $f(k) = ak$, for $k \in K$
- f is one to one
- f is onto
  - Let b be an arbitrary element in aK
  - $b = ak$ for some $k \in K$
  - $f(k) = ak = b$
  - f is onto.
- Therefore, f is bijection, K and aK have the same number of elements.

Proof.

- Let
  - aK be a left coset of K in G, where $a \in G$
  - $f : K \to aK$ be defined by $f(k) = ak$, for $k \in K$
- f is one to one
- f is onto
  - Let b be an arbitrary element in aK
  - $b = ak$ for some $k \in K$
  - $f(k) = ak = b$
  - f is onto.
- Therefore, f is bijection, K and aK have the same number of elements.

Proof.

- Let
  - aK be a left coset of K in G, where $a \in G$
  - $f : K \to aK$ be defined by $f(k) = ak$, for $k \in K$
- f is one to one
- f is onto
- Therefore, f is bijection, K and aK have the same number of elements.

Equivalence Class vs. Coset

Theorem

Let

- R *be a congruence relation on a group* G
- $H = [e]$, *the equivalence class containing the identity*

Then

- H *is a normal subgroup of* G
- $[a] = aH = Ha$, *for each* $a \in G$

Proof: for $a, b \in G$.

- $b \in [a]$
- iff $[b] = [a]$, for R is an equivalence relation
- iff $[e] = [a]^{-1}[b] = [a^{-1}b]$, for G/R is a group
- iff $H = [e] = [a^{-1}b]$
- iff $a^{-1}b \in H$ or $b \in aH$
- So $[a] = aH$ for every $a \in G$

❀

Question

Something Missing?

Proof: for $a, b \in G$.

- $b \in [a]$
- iff $[b] = [a]$, for R is an equivalence relation
- iff $[e] = [a]^{-1}[b] = [a^{-1}b]$, for G/R is a group
- iff $H = [e] = [a^{-1}b]$
- iff $a^{-1}b \in H$ or $b \in aH$
- So $[a] = aH$ for every $a \in G$

❀

Question

Something Missing?

Proof: for $a, b \in G$.

- $b \in [a]$
- iff $[b] = [a]$, for R is an equivalence relation
- iff $[e] = [a]^{-1}[b] = [a^{-1}b]$, for G/R is a group
- iff $H = [e] = [a^{-1}b]$
- iff $a^{-1}b \in H$ or $b \in aH$
- So $[a] = aH$ for every $a \in G$

Question

Something Missing?

Proof: for $a, b \in G$.

- $b \in [a]$
- iff $[b] = [a]$, for R is an equivalence relation
- iff $[e] = [a]^{-1}[b] = [a^{-1}b]$, for G/R is a group
- iff $H = [e] = [a^{-1}b]$
- iff $a^{-1}b \in H$ or $b \in aH$
- So $[a] = aH$ for every $a \in G$

❀

Question

Something Missing?

Proof: for $a, b \in G$.

- $b \in [a]$
- iff $[b] = [a]$, for R is an equivalence relation
- iff $[e] = [a]^{-1}[b] = [a^{-1}b]$, for G/R is a group
- iff $H = [e] = [a^{-1}b]$
- iff $a^{-1}b \in H$ or $b \in aH$
- So $[a] = aH$ for every $a \in G$

Question

Something Missing?

Proof: for $a, b \in G$.

- $b \in [a]$
- iff $[b] = [a]$, for R is an equivalence relation
- iff $[e] = [a]^{-1}[b] = [a^{-1}b]$, for G/R is a group
- iff $H = [e] = [a^{-1}b]$
- iff $a^{-1}b \in H$ or $b \in aH$
- So $[a] = aH$ for every $a \in G$

❀

Question

Something Missing?

Proof: for $a, b \in G$.

Similarly

- $b \in [a]$
- iff $H = [e] = [b][a]^{-1} = [ba^{-1}]$
- $[a] = Ha$

Thus $[a] = aH = Ha$, and H is normal. ❀

Question

Something Missing?

Proof: for $a, b \in G$.

Similarly

- $b \in [a]$
- iff $H = [e] = [b][a]^{-1} = [ba^{-1}]$
- $[a] = Ha$

Thus $[a] = aH = Ha$, and H is normal. ❀

Question

Something Missing?

Proof: for $a, b \in G$.

Similarly

- ♪ $b \in [a]$
- ♪ iff $H = [e] = [b][a]^{-1} = [ba^{-1}]$
- ♪ $[a] = Ha$

Thus $[a] = aH = Ha$, and H is normal. ❀

Question

Something Missing?

Proof: for $a, b \in G$.

Similarly

- $b \in [a]$
- iff $H = [e] = [b][a]^{-1} = [ba^{-1}]$
- $[a] = Ha$

Thus $[a] = aH = Ha$, and H is normal. ❀

Question

Something Missing?

Notice - Equivalence Class vs. Coset

The quotient group G/R consists of all the left cosets of $N = [e]$. The operation in G/R is given by

- $(aN)(bN) = [a] \circledast [b] = [ab] = abN$

and the function $f_R : G \to G/R$, defined by

- $f_R(a) = aN$

is a homomorphism from G onto G/R. For this reason, we will often write G/R as G/N.

Theorem

Let

- N *be a normal subgroup of a group* G
- R *be the following relation on* G
  - $a\ R\ b$ *if and only if* $a^{-1}b \in N$

Then

- R *is a congruence relation on* G
- N *is the equivalence class* $[e]$ *relative to* R, *where* e *is the identity of* G

Proof. R is an equivalence relation.

Let $a \in G$

- $a \; R \; a$, since $a^{-1}a = e \in N$
- R is reflexive

❀

Proof. R is an equivalence relation.

Suppose that $a \ R \ b$

- $a^{-1}b \in N$
- $N \ni (a^{-1}b)^{-1} = b^{-1}a$
- $b \ R \ a$
- R is symmetric.

Proof. R is an equivalence relation.

Suppose that $a\ R\ b$ and $b\ R\ c$

- $a^{-1}b \in N$ and $b^{-1}c \in N$
- $N \ni (a^{-1}b)(b^{-1}c) = a^{-1}c$
- $a\ R\ c$
- R is transitive.

Proof. R is a congruence relation on G.

Suppose that $a\ R\ b$ and $c\ R\ d$

- $a^{-1}b \in N$ and $c^{-1}d \in N$
- Since N is normal, $Nd = dN$
- Since $a^{-1}b \in N$, then $a^{-1}bd = dn$ for some $n \in N$.
- $(ac)^{-1}bd = (c^{-1}a^{-1})(bd) = c^{-1}(a^{-1}b)d = (c^{-1}d)n \in N$
- So $ac\ R\ bd$.
- Hence R is a congruence relation on G.

Proof.

Proof. $N = [e]$

- $N \subseteq [e]$
- $[e] \subseteq N$
- Hence $N = [e]$

Proof.

Proof. $N = [e]$

- $N \subseteq [e]$
  - Suppose that $x \in N$
  - $x^{-1}e = x^{-1} \in N$
  - $x \; R \; e$
  - $x \in [e]$
  - $N \subseteq [e]$
- $[e] \subseteq N$
- Hence $N = [e]$

Proof.

Proof. $N = [e]$

- $N \subseteq [e]$
- $[e] \subseteq N$
  - Conversely, if $x \in [e]$
  - $x \; R \; e$
  - $x^{-1}e = x^{-1} \in N$
  - $x \in N$
  - $[e] \subseteq N$
- Hence $N = [e]$

Proof.

Proof. $N = [e]$

- $N \subseteq [e]$
- $[e] \subseteq N$
- Hence $N = [e]$

❀

Corollary

Let

- f *be a homomorphism from a group* $(G, \ *)$ *onto a group* $(G', \ *')$
- *The kernel of* f, $ker(f)$, *be defined by*
  - $ker(f) = \{a \in G | f(a) = e'\}$

Then

- $ker(f)$ *is a normal subgroup of* G
- *The quotient group* $G/ker(f)$ *is isomorphic to* G'

Example

Consider the homomorphism $f : \mathbb{Z} \to \mathbb{Z}_n$ defined by $f(m) = [r]$, where r is the remainder when m is divided by n.

- Find $ker(f)$

Solution.

- An integer m in $\mathbb{Z}$ belongs to $ker(f)$
  - if and only if
- $f(m) = [0]$
  - if and only if
- m is a multiple of n
- Hence $ker(f) = n\mathbb{Z}$.

The conclusion is . . .

Following four are equivalent

- a congruence relation R on G
- a normal subgroup H of G
- a homomorphism from G to G/R or G'
- the kernel of a homomorphism from G to G'

Homework

- 22,28 @page 331
- 28,32 @page 349
- 24@338
- 4,18,39@353-354
- Let G be a group, and let N and H be subgroups of G such that N is normal in G. Prove that
  1. HN is a subgroup of G.
  2. N is a normal subgroup of HN.