§11. Normal Subgroups, Factor Groups, First Isomorphism Theorem

LEMMA Let G be a group, and let N be a subgroup of G. Then t.f.a.e.*)

(1) $gN = Ng, \quad \forall g \in G$ (i.e. left and right N-cosets are the same)

(2) $gNg^{-1} = N, \quad \forall g \in G$

(3) $gNg^{-1} \subset N, \quad \forall g \in G.$

Proof. (1) ⟹ (2): Assuming (1), if $g \in G$, then

$$gNg^{-1} = gN.g^{-1} = Ng.g^{-1} = N.gg^{-1} = N.1 = N.$$

(2) ⟹ (3): This is clear, since $N \subset N$.

(3) ⟹ (1): Assuming (3), if $g \in G$, then

$$gN = gN.1 = gN.g^{-1}g = gNg^{-1}.g \subset Ng$$

Replacing g by g^{-1} in $gN \subset Ng$ gives $g^{-1}N \subset Ng^{-1}$, so

$$Ng = 1.Ng = gg^{-1}.Ng = g.g^{-1}N.g \subset g.Ng^{-1}.g = gN.1 = gN.$$

Thus for all g we have both $gN \subset Ng$ and $Ng \subset gN$, so $gN = Ng$.

DEF. Let G be a group. A subgroup N of G is <u>normal</u>, written $N \triangleleft G$, if N satisfies any (and therefore all) of the conditions (1), (2), (3) in the Lemma.

THM A: Each subgroup of an abelian group is normal.

Proof. If H is a subgroup of an abelian group G, then for all $g \in G$,

$$gH = \{gh : h \in H\} = \{hg : h \in H\} = Hg,$$

showing that $H \triangleleft G$.

LEMMA. If $N \triangleleft G$, then the product of N-cosets is an N-coset. More precisely,

(4) $\quad (aN)(bN) = ab.N \quad \forall a \,\&\, b \in G.$

*) t.f.a.e. stands for "The following statements are equivalent", i.e. "Each of the following statements implies the others."

Proof. By (4) in the Lemma at the top of 11.1

$$(aN)(bN) = a.Nb.N = a.bN.N = ab.NN = abN.$$

COR. If $N \lhd G$, then

(5) $aN.N = N.aN = aN \quad \forall a \in G$

(6) $aN.a^{-1}N = a^{-1}N.aN = N \quad \forall a \in G$

Proof. (5): By (4) with $b = 1$, we get

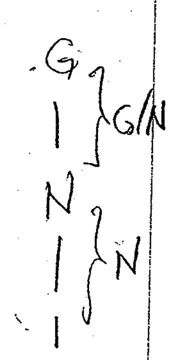
$$aN.N = aN.1N = a.1.N = aN \quad \forall a \in G.$$

Similarly, $N.aN = aN, \ \forall a \in G$

(6). By (4) with $b = a^{-1}$,

$$aN.a^{-1}N = aa^{-1}.N = 1.N = N \quad \forall a \in G.$$

Similarly, $a^{-1}N.aN = N, \ \forall a \in G.$



THM B If $N \lhd G$, then G/N (i.e. the set of all N-cosets in G), together with the multiplication of N-cosets, is a group, in which the identity element is the coset $N (= 1N)$, and $(aN)^{-1} = a^{-1}N$ for all $a \in G$. The group G/N is the <u>quotient group</u> or <u>factor group</u> of G by N.

Proof. By the Lemma at the bottom of 11.1, multiplication of N-cosets is a map from $G/N \times G/N$ to G/N. This multiplication is associative, since, by (4),

$$((aN)(bN))(cN) = (ab.N)(cN) = (ab.c)N = (a.bc)N = aN.bc.N = (aN)((bN.cN)).$$

By (5), the coset N is an (the!) identity element for this multiplication, so G/N is a monoid. By (6), $a^{-1}N$ is an (the!) inverse of the element aN in G/N, for each $a \in G$. Thus G/N is a group

DEF Let G_1 and G_2 be groups. A map $\varphi : G_1 \to G_2$ is a <u>homomorphism</u> if

$$(7) \qquad \varphi(ab) = \varphi(a)\varphi(b) \quad \forall\, a \,\&\, b \in G_1.$$

If $\varphi : G_1 \to G_2$ is a bijective homomorphism, then φ is an <u>isomorphism</u> and G_1 and G_2 are <u>isomorphic</u>, written $G_1 \simeq G_2$.

THM C If $\varphi : G_1 \to G_2$ is a homomorphism, then

(1) $\varphi(1) = 1$ (i.e., φ takes the identity element of G_1 to the identity element of G_2);

(2) $\varphi(a^{-1}) = \varphi(a)^{-1}$ (i.e., "the image of an inverse is the inverse of the image").

Proof (1) In (7) put $a = b = 1$ and get $\varphi(1) = \varphi(1)^2$. Multiplying (on either side) by $\varphi(1)^{-1}$ gives $1 = \varphi(1)$.

(2) In (7) put $b = a^{-1}$ and get

$$1 = \varphi(1) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1}),$$

which implies $\varphi(a^{-1}) = \varphi(a)^{-1}$, e.g. by multiplying on the left by $\varphi(a)^{-1}$; or see Exercise 5 on 8.4.

THM D (1) For each group G, the identity map $1_G : G \to G$ is an isomorphism.

(2) If $\varphi : G_1 \to G_2$ is an isomorphism, so is $\varphi^{-1} : G_2 \to G_1$.

(3) If $\varphi : G_1 \to G_2$ and $\psi : G_2 \to G_3$ are isomorphisms, so is $\psi\varphi : G_1 \to G_3$.

COR. (1) For each group G, we have $G \simeq G$.

(2) If $G_1 \simeq G_2$, then $G_2 \simeq G_1$.

(3) If $G_1 \simeq G_2$ and $G_2 \simeq G_3$, then $G_1 \simeq G_3$.

EXERCISE 1. Prove Theorem D, and, using Theorem D, prove the Corollary.

DEF. Let $\varphi : G_1 \to G_2$ be a homomorphism. The <u>kernel</u> and <u>image</u> of φ are defined by

$$\ker\varphi = \{a \in G_1 : \varphi(a) = 1\}; \quad \text{i.e. } \ker\varphi = \varphi^{-1}(\{1\});$$

$$\operatorname{im}\varphi = \{\varphi(a) : a \in G_1\}, \quad \text{i.e. } \operatorname{im}\varphi = \varphi G_1;$$

Thus $\ker\varphi \subset G_1$ and $\operatorname{im}\varphi \subset G_2$.

THM E For each $N \lhd G$, the canonical surjection $\sigma : G \to G/N$, defined by $\varphi(a) = aN$ $\forall a \in G$ is a homomorphism with image G/N and kernel N.

Proof. Using $\bigcirc$ and (7), we have

$$\varphi(ab) = ab.N = aN.bN = \varphi(a)\varphi(b),$$

so φ is a homomorphism. Clearly $\varphi(G) = G/N$. Finally, $\ker\varphi = N$ since

$$a \in \ker\varphi \iff \varphi(a) = N \iff aN = N \iff a \in N.$$

THM F. For each subgroup H of G, the canonical injection $i : H \to G$, defined by $i(a) = a$ $\forall a \in H$ is a homomorphism with image H and kernel 1.

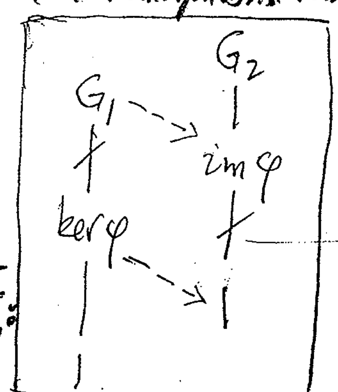
EXERCISE 2. Prove Theorem F.

THM G. (First Isomorphism Theorem) Let $\varphi : G_1 \to G_2$ be a homomorphism. Then

(1) $\ker\varphi$ is a normal subgroup of G_1;

(2) $\operatorname{im}\varphi$ is a subgroup of G_2;

(3) $\operatorname{im}\varphi \cong G_1/\ker\varphi$.



Proof (1) Let $N = \ker\varphi$. We verify first that N is a subgroup of G_1:
Since $\varphi(1) = 1$, we have $1 \in N$. Also, if a & $b \in N$, then
$\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} = 1.1^{-1} = 1$, so $ab^{-1} \in N$. Thus N is a subgroup.
We show next that $N \lhd G_1$: If $a \in N$ and $g \in G_1$, then
$\varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g^{-1}) = \varphi(g).1.\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = 1$,
so $gag^{-1} \in N$. Thus $gNg^{-1} \subset N$ for all $g \in G_1$, so $N \lhd G_1$ by Defn 11.1.
(2) Let $H = \operatorname{im}\varphi$. We verify next that H is a subgroup of G_2:
Since $\varphi(1) = 1$, we have $1 \in H$. Also, if a & $b \in H$, then $a = \varphi(\alpha)$ & $b = \varphi(\beta)$
for some α & $\beta \in G_1$, so $ab^{-1} = \varphi(\alpha)\varphi(\beta)^{-1} = \varphi(\alpha)\varphi(\beta^{-1}) = \varphi(\alpha\beta^{-1}) \in \varphi(G_1) = H$.
Thus H is a subgroup of G_2.

(3) Keeping the notation $N = \ker\varphi$ and $H = \operatorname{im}\varphi$, it remains to construct an isomorphism $\Phi : G/N \to H$. Put

$$\boxed{\Phi(aN) = \varphi(a).}$$

Is this map Φ really well defined? I.e., if $\tilde{a}N = aN$, is $\varphi(\tilde{a}) = \varphi(a)$?
If $\tilde{a}N = aN$, then $a^{-1}\tilde{a} = a^{-1}\tilde{a}\cdot 1 \in a^{-1}\tilde{a}.N = a^{-1}.\tilde{a}N = a^{-1}.aN = a^{-1}a.N = 1N = N$,
i.e. $a^{-1}\tilde{a} \in N$, so $\varphi(a)^{-1}\varphi(\tilde{a}) = \varphi(a^{-1})\varphi(\tilde{a}) = \varphi(a^{-1}\tilde{a}) = 1$, so $\varphi(\tilde{a}) = \varphi(a)$,
so, yes, $\Phi : G/N \to H$ is well defined.

Is Φ a homomorphism? For aN & $bN \in G/N$, we have
$\Phi(aN.bN) = \Phi(abN) = \varphi(ab) = \varphi(a)\varphi(b) = \Phi(aN)\Phi(bN)$,
so, yes, Φ is a homomorphism.

Is Φ surjective? Each element of $H = \operatorname{im}\varphi$ is of the form $\varphi(a) = \Phi(aN)$ for some $a \in G$, i.e. some $aN \in G/N$; so $\Phi(G/N) = H$,
so, yes, Φ is surjective.

Is Φ injective? For aN & $bN \in G/N$, if $\Phi(aN) = \Phi(bN)$, then $\varphi(a) = \varphi(b)$, so
$\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} = 1$, so $ab^{-1} \in N$, so $(aN)(bN)^{-1} = aNb^{-1}N = ab^{-1}N = N$,
so $aN = bN$, so, yes Φ is injective.

Thus $\Phi : G/N \to H$ is a bijective homomorphism, i.e. isomorphism,
so G/N and H are isomorphic, i.e. $G/\ker\varphi \cong \operatorname{im}\varphi$.

EXERCISE 3. (1) Prove that if G is infinite cyclic and $G = \langle g \rangle$, and $N = \langle g^n \rangle$ for some $n \in \mathbb{N}$, then $N \triangleleft G$ and G/N is cyclic of order n, and $G/N = \langle gN \rangle$.
(2) Prove that if G is cyclic of order n and $G = \langle g \rangle$, and $N = \langle g^e \rangle$ for some divisor e of n, then G/N is cyclic of order e, and $G/N = \langle gN \rangle$.

EXERCISE 4. Let $G = S_3$. See 8.4 and Exercise 6 on 8.4.
Prove that $\langle r \rangle$ is a normal subgroup of G, but the subgroups $\langle t_1 \rangle, \langle t_2 \rangle, \langle t_3 \rangle$ are not normal, and prove that $G/\langle r \rangle = \langle t_1 \langle r \rangle \rangle$. Hint: Show first $t_1\langle r \rangle t_1^{-1} = \langle r \rangle$ & $r\langle t_1 \rangle r^{-1} = \langle t_2 \rangle$.