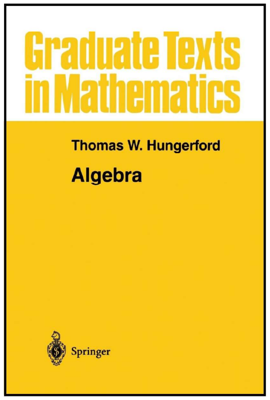
Modern Algebra

Chapter I. Groups

I.5. Normality, Quotient Groups,and Homomorphisms
—Proofs of Theorems



Theorem I.5.1

Theorem I.5.1. If N is a subgroup of group G, then the following conditions are equivalent.

(i) Left and right congruence modulo N coincide (that is, define the same equivalence relation on G);

(ii) Every left coset of N in G is a right coset of N in G;

(iii) $aN = Na$ for all $a \in G$;

(iv) For all $a \in G$, $aNa^{-1} \subset N$ where $aNa^{-1} = \{ana^{-1} \mid n \in N\}$;

(v) For all $a \in G$, $aNa^{-1} = N$.

Proof. $(i) \Rightarrow (ii)$. If left and right congruence mod N coincide then $ab^{-1} \in N$ if and only if $a^{-1}b \in N$ (by Definition I.4.1). Let $x \in aN$. Then $a^{-1}x \in N$ and by the congruence assumption $ax^{-1} \in N$. Therefore $(ax^{-1})^{-1} = xa^{-1} \in N$ and $x \in Na$; hence $aN \subseteq Na$. Similarly $Na \subseteq aN$ and $aN = Na$. □

Theorem I.5.1 (continued 1)

Theorem I.5.1. If N is a subgroup of group G, then the following conditions are equivalent.

(i) Left and right congruence modulo N coincide (that is, define the same equivalence relation on G);

(ii) Every left coset of N in G is a right coset of N in G;

(iii) $aN = Na$ for all $a \in G$.

Proof (continued). $(iii) \Rightarrow (i)$. Suppose $aN = Na$ and let $a \equiv_r b \pmod N$; that is, $ab^{-1} \in N$. Then $(ab^{-1})^{-1} = ba^{-1} \in N$ and $b \in Na = aN$. Hence $a^{-1}b \in N$ and $a \equiv_\ell b \pmod N$.
Similarly, $a \equiv_\ell b \pmod N$ implies that $a \equiv_r b \pmod N$ and if $aN = Na$ then left and right congruence coincide. □
$(ii) \Rightarrow (iii)$. Let aN be a left coset of N. Then by hypothesis $aN = Nb$ for some $b \in G$. But $e \in N$ so $ae = a \in aN = Nb$ and similarly $a \in Na$. So $a \in Na \cap Nb$ and since the cosets of N partition G, then it must be that $Na = Nb$ and so $aN = Nb = Na$. □

Theorem I.5.1 (continued 2)

Theorem I.5.1. If N is a subgroup of group G, then the following conditions are equivalent.

(ii) Every left coset of N in G is a right coset of N in G;

(iii) $aN = Na$ for all $a \in G$.

(iv) For all $a \in G$, $aNa^{-1} \subset N$ where $aNa^{-1} = \{ana^{-1} \mid n \in N\}$;

(v) For all $a \in G$, $aNa^{-1} = N$.

Proof (continued). $(iii) \Rightarrow (iv)$. If $aN = Na$ for all $a \in G$, then for each $n \in N$ we have $an \in Na$ and so $ana^{-1} \in N$. Therefore $aNa^{-1} \subseteq N$. □
$(iv) \Rightarrow (v)$. Suppose $aNa^{-1} \subseteq N$ for all $a \in G$. Then replace a with a^{-1} we get $a^{-1}Na \subseteq N$. So for any $n \in N$ we have $n = (aa^{-1})n(aa^{-1})$ $= a(a^{-1}na)a^{-1} \in aNa^{-1}$ and so $N \subseteq aNa^{-1}$. Combining this with the hypothesis of (iv) gives $aNa^{-1} = N$ for all $a \in G$. □
$(v) \Rightarrow (ii)$. If $aNa^{-1} = N$ for all $a \in G$, then $aN = Na$ for all $a \in G$ and left and right cosets coincide. □

Theorem I.5.3

Theorem I.5.3. Let K and N be subgroups of a group G with N normal in G. Then

(*i*) $N \cap K \triangleleft K$;
(*ii*) $N \triangleleft N \vee K$;
(*iii*) $NK = N \vee K = KN$;
(*iv*) If $K \triangleleft G$ and $K \cap N = \{e\}$, then $nk = kn$ for all $k \in K$ and $n \in N$.

Proof. Recall that the join of subgroups H and K is the subgroup of G generated by $H \cup K$.
(i) Let $n \in N \cap K$ and $a \in K$. Then $ana^{-1} \in N$ since $N \triangleleft G$ and $a \in G$. Also, $ana^{-1} \in K$ since $K < G$ and we have assumed that $a, n \in K$. So such a and n satisfy $ana^{-1} \in N \cap K$ and $a(N \cap K)a^{-1} \subseteq N \cap K$, so $N \cap K \triangleleft K$ by Theorem I.5.1(iv). □
(ii) Since N and K are subgroups of G then $N \vee K < G$ ($N \vee K$ is the smallest group containing $N \cup K$ and G is a group containing $N \cup K$). Since $N \triangleleft G$ and $N < N \vee K$, then $N \triangleleft N \vee K$. □

Theorem I.5.3 (continued 1)

Theorem I.5.3. Let K and N be subgroups of a group G with N normal in G. Then

(*iii*) $NK = N \vee K = KN$.

Proof (continued). (iii) Now $NK = \{nk \mid n \in N, k \in K\}$ and $N \vee K$ is the smallest group containing $N \cup K$, so certainly $NK \subset N \vee K$. An element $x \in N \vee K$ is a product of the form $n_1k_1n_2k_2 \cdots n_rk_r$ where $n_i \in N$, $k_i \in K$ by Theorem I.2.8. Since $N \triangleleft G$ then $n_ik_i = k_in_i'$ for some $n_i' \in N$ (by Theorem I.5.1(iii) where we consider the coset $Nk_i = k_iN$) and therefore x can be written in the form $n(k_1k_2 \cdots k_r)$ where $n \in N$ (we move the k_is "to the right" one at a time and then use the normality of N to shift all the n_i's "to the left"). Thus any $n_1k_1n_2k_2 \cdots n_rk_r \in N \vee K$ is of the form $n(k_1k_2 \cdots k_r) \in NK$ and so $N \vee K \subseteq NK$. Therefore $NK = N \vee K$. Similarly (still using the normality of N) we can shift the n_is "to the right" and show that $KN = N \vee K$. □

Theorem I.5.3 (continued 2)

Theorem I.5.3. Let K and N be subgroups of a group G with N normal in G. Then

(*i*) $N \cap K \triangleleft K$;
(*ii*) $N \triangleleft N \vee K$;
(*iii*) $NK = N \vee K = KN$;
(*iv*) If $K \triangleleft G$ and $K \cap N = \{e\}$, then $nk = kn$ for all $k \in K$ and $n \in N$.

Proof (continued). (iv) Let $k \in K$ and $n \in N$. Then $nkn^{-1} \in K$ since we now hypothesize $K \triangleleft G$. Also $kn^{-1}k^{-1} \in N$ since $N \triangleleft G$. Hence $(nkn^{-1})k^{-1} \in K$ (since $nkn^{-1}, k^{-1} \in K$) and $(nkn^{-1})k^{-1} = n(kn^{-1}k^{-1}) \in N$ (since $n, kn^{-1}k^{-1} \in N$). So $nkn^{-1}k^{-1} \in N \cap K = \{e\}$ and $nk = kn$. □

Theorem I.5.4

Theorem I.5.4. If N is a normal subgroup of a group G and G/N is the set of all (left) cosets of N in G, then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = (ab)N$.
Proof. Much of the work is already done in Theorem I.1.5. For $g \in G$, the coset gN is the equivalence class of $g \in G$ under the equivalence relation of congruence modulo N by Theorem I.4.2(ii). To use Theorem I.1.5, we need to confirm that $a_1 \sim a_2$ and $b_1 \sim b_2$ imply that $a_1b_1 \sim a_2b_2$. So suppose that $a_1 \equiv a_2 \pmod N$ and $b_1 \equiv b_2 \pmod N$; that is, $a_1a_2^{-1} = n_a \in N$ and $b_1b_2^{-1} = n_b \in N$. Then $(a_1b_1)(a_2b_2)^{-1} = a_1b_1b_2^{-1}a_2^{-1} = a_1n_ba_2^{-1}$. Since N is normal, $a_1N = Na_1$ by Theorem I.5.1(iii) which implies that $a_1n_b = na_1$ for some $n \in N$. So $(a_1b_1)(a_2b_2)^{-1} = a_1n_ba_2^{-1} = na_1a_2^{-1} = n(a_1a_2^{-1}) = nn_a \in N$. Therefore, $a_1b_1 \equiv a_2b_2 \pmod N$. Theorem I.1.5 now implies that the equivalence classes (i.e., the cosets of N) form a monoid. Since G contains an identity and inverses then, based on how coset multiplication is defined, the cosets of N form a group as claimed. □

Theorem I.5.5

Theorem I.5.5. If $f : G \to H$ is a homomorphism of groups, then the kernel of f is a normal subgroup of G. Conversely, if N is a normal subgroup of G, then the map $\pi : G \to G/N$ given by $\pi(a) = aN$ is an epimorphism (that is, an onto homomorphism) with kernel N.

Proof. If $x \in \text{Ker}(f)$ and $a \in G$ then $f(axa^{-1}) = f(a)f(x)f(a^{-1}) = f(a)e_H f(a^{-1}) = f(a)f(a^{-1}) = f(aa^{-1}) = f(e_G) = e_H$ and so $axa^{-1} \in \text{Ker}(f)$. Hence, since we have taken $x \in \text{Ker}(f)$ then $a(\text{Ker}(f))a^{-1} \subset \text{Ker}(f)$ for all $a \in G$, and so by Theorem I.5.1(iv), $\text{Ker}(f) \lhd G$.
Next, suppose N is a normal subgroup. Then $\pi : G \to G/N$ given by $\pi(a) = aN$ is "clearly" onto (such a ranges over all elements of G and hence π produces all cosets of N). Now $\pi(ab) = (ab)N = (aN)(bN)$ $= \pi(a)\pi(b)$ (by the definition of coset multiplication). So π is a homomorphism and hence an epimorphism. Finally, $\text{Ker}(\pi) = \{a \in G \mid \pi(a) = e_G N = N\} = \{a \in G \mid aN = N\} = \{a \in G \mid a \in N\} = N$. □

Theorem I.5.6

Theorem I.5.6. If $f : G \to H$ is a homomorphism and N is a normal subgroup of G contained in the kernel of f, then there is a unique homomorphism $\overline{f} : G/N \to H$ such that $\overline{f}(aN) = f(a)$ for all $a \in G$. Also, $\text{Im}(f) = \text{Im}(\overline{f})$ and $\text{Ker}(\overline{f}) = \text{Ker}(f)/N$. $\overline{f}$ is an isomorphism if and only if f is an epimorphism and $N = \text{Ker}(f)$.

Proof. First, we introduce $\overline{f}$. If $b \in aN$ then $b = an$ for some $n \in N$. So, since f is a homomorphism then $f(b) = f(an) = f(a)f(n) = f(a)e_H = f(a)$ (since $n \in N \subseteq \text{Ker}(f)$). Since b is any representative of coset aN, then defining $\overline{f} : G/N \to H$ as $\overline{f}(aN) = f(a)$ produces a well defined function. Since $\overline{f}((aN)(bN)) = \overline{f}((ab)N) = f(ab) = f(a)f(b) = \overline{f}(aN)\overline{f}(bN)$ then $\overline{f}$ is a homomorphism.

Theorem I.5.6 (continued 1)

Theorem I.5.6. If $f : G \to H$ is a homomorphism and N is a normal subgroup of G contained in the kernel of f, then there is a unique homomorphism $\overline{f} : G/N \to H$ such that $\overline{f}(aN) = f(a)$ for all $a \in G$. Also, $\text{Im}(f) = \text{Im}(\overline{f})$ and $\text{Ker}(\overline{f}) = \text{Ker}(f)/N$. $\overline{f}$ is an isomorphism if and only if f is an epimorphism and $N = \text{Ker}(f)$.

Proof (continued). Next, $\text{Im}(\overline{f}) = \text{Im}(f)$ from the definition of $\overline{f}$ as $\overline{f}(aN) = f(a)$ (recall that "$\text{Im}(f)$" is the range of function f; see page 4). Also, $aN \in \text{Ker}(\overline{f})$ if and only if $\overline{f}(aN) = e$ if and only if $f(a) = e$ if and only if $a \in \text{Ker}(f)$. So $\text{Ker}(\overline{f}) = \{aN \mid a \in \text{Ker}(f)\} = \text{Ker}(f)/N$ (notice that the elements of $\text{Ker}(f)/N$ are the cosets of N by elements of $\text{Ker}(f)$). This establishes the "also" part of the claim.

Since $\overline{f}$ is defined entirely in terms of f, the uniqueness claim follows.

Theorem I.5.6 (continued 2)

Theorem I.5.6. If $f : G \to H$ is a homomorphism and N is a normal subgroup of G contained in the kernel of f, then there is a unique homomorphism $\overline{f} : G/N \to H$ such that $\overline{f}(aN) = f(a)$ for all $a \in G$. Also, $\text{Im}(f) = \text{Im}(\overline{f})$ and $\text{Ker}(\overline{f}) = \text{Ker}(f)/N$. $\overline{f}$ is an isomorphism if and only if f is an epimorphism and $N = \text{Ker}(f)$.

Proof (continued). Finally, for the isomorphism claim, notice that $\overline{f}$ is an epimorphism (an onto homomorphism) if and only if f is an epimorphism. By Theorem I.2.3, $\overline{f}$ is a monomorphism (a one to one homomorphism) if and only if $\text{Ker}(\overline{f}) = \text{Ker}(f)/N$ is the trivial subgroup of G/N. This is the case if and only if $\text{Ker}(f)/N = N$ which in turn is the case if and only if $\text{Ker}(f) = N$. □

Corollary I.5.8

Corollary I.5.8. If $f : G \to H$ is a homomorphism of groups, $N \triangleleft G$, $M \triangleleft H$, and $f(N) < M$, then f induces a homomorphism $\overline{f} : G/N \to H/M$, given by $aN \mapsto f(a)M$. $\overline{f}$ is an isomorphism if and only if $\mathrm{Im}(f) \vee M = H$ and $f^{-1}(M) \subset N$. In particular if f is an epimorphism such that $f(N) = M$ and $\mathrm{Ker}(f) \subset N$, then $\overline{f}$ is an isomorphism.

Proof. We break this into three stages (one of which we leave as a homework problem).
(A) Let $\pi : H \to H/M$ be the canonical epimorphism, $\pi(h) = hM$. Consider the composition $\pi \circ f : G \to H/M$. Since $f(N) < M$ then $N \subseteq f^{-1}(M)$. Now $\mathrm{Ker}(\pi f)$ consists of the elements of G mapped to M under $\pi \circ f$; this is the elements of G mapped to M by f (since $\pi(h) = hM = M$ if and only if $h \in M$) and hence is $f^{-1}(M)$. So $N \subseteq f^{-1}(M) = \mathrm{Ker}(\pi f)$. Hence N is a normal subgroup of G contained in the kernel of πf.

Corollary I.5.8 (continued 1)

Corollary I.5.8. If $f : G \to H$ is a homomorphism of groups, $N \triangleleft G$, $M \triangleleft H$, and $f(N) < M$, then f induces a homomorphism $\overline{f} : G/N \to H/M$, given by $aN \mapsto f(a)M$. $\overline{f}$ is an isomorphism if and only if $\mathrm{Im}(f) \vee M = H$ and $f^{-1}(M) \subset N$. In particular if f is an epimorphism such that $f(N) = M$ and $\mathrm{Ker}(f) \subset N$, then $\overline{f}$ is an isomorphism.

Proof (continued). So by Theorem I.5.6 (applied to πf) the map (in the notation of Theorem I.5.6 this map would be denoted $\overline{\pi f}$) $\overline{f} : G/N \to H/M$ given by $aN \mapsto (\pi f)(a) = f(a)M$ (that is, $\overline{\pi f}(aN) = (\pi f)(a) = \pi(f(a)) = f(a)M$) is a (unique) homomorphism that is an isomorphism if and only if πf is an epimorphism and $N = \mathrm{Ker}(\pi f)$.

(B) This last condition is equivalent to $\mathrm{Im}(f) \vee M = H$ and $f^{-1}(M) \subseteq N$. We leave this as a homework problem.

Corollary I.5.8 (continued 2)

Corollary I.5.8. If $f : G \to H$ is a homomorphism of groups, $N \triangleleft G$, $M \triangleleft H$, and $f(N) < M$, then f induces a homomorphism $\overline{f} : G/N \to H/M$, given by $aN \mapsto f(a)M$. $\overline{f}$ is an isomorphism if and only if $\mathrm{Im}(f) \vee M = H$ and $f^{-1}(M) \subset N$. In particular if f is an epimorphism such that $f(N) = M$ and $\mathrm{Ker}(f) \subset N$, then $\overline{f}$ is an isomorphism.

Proof (continued).
(C) (The "in particular" part.) If f is an epimorphism (and hence onto) then $H = \mathrm{Im}(f) = \mathrm{Im}(f) \vee M$. Hypothesizing $f(N) = M$ and $\mathrm{Ker}(f) \subseteq N$ gives $f^{-1}(M) \subseteq N$ as follows. Suppose not; ASSUME $f(g) \in M$ for some $g \in G \setminus N$. Since $f(N) = M$ then for some $n \in N$ we have $f(n) = f(g)$. Then $f(gn^{-1}) = f(g)f(n^{-1}) = f(g)(f(n))^{-1} = f(g)(f(g))^{-1} = e$ and $gn^{-1} \in \mathrm{Ker}(f) \subseteq N$. But $n \in N$ also, so $(gn^{-1})n = g \in N$, a CONTRADICTION. So the assumption that such g exists is false and $f^{-1}(M) \subseteq N$. So the conditions of (B) are satisfied and $\overline{f}$ is an isomorphism. □

Corollary I.5.9

Corollary I.5.9. Second Isomorphism Theorem.
If K and N are subgroups of a group G, with N normal in G, then $K/(N \cap K) \cong NK/N$.

Proof. We have $N \triangleleft NK$ by Theorem I.5.3(ii) and $NK = N \vee K$ by Theorem I.5.3(iii). With 1_G as the identity, we have the composition $K \xrightarrow{1_G} NK \xrightarrow{\pi} NK/N$ (where π is the canonical epimorphism) is a homomorphism, say $f = \pi \circ 1_G$. The kernel of f is the elements of K mapped to N (the identity element of NK/N), so $\mathrm{Ker}(f) = N \cap K$. So, by the First Isomorphism Theorem (Corollary I.5.7) f induces an isomorphism $\overline{f} : K/(K \cap N) \to \mathrm{Im}(f)$ and so: $\quad K/(K \cap N) \cong \mathrm{Im}(f). \quad (*)$
Every element in NK/N is of the form $(nk)N$ (for $n \in N, k \in K$). Since $N \triangleleft G$ then $nk = kn_1$ for some $n_1 \in N$, "whence" $(nk)N = (kn_1)N = kN = f(k)$. So every element of NK/N is in $\mathrm{Im}(f)$ and f is onto NK/N. So f is an epimorphism and $\mathrm{Im}(f) = NK/N$. So by $(*)$, we see that $K/K \cap N \cong NK/N$, under isomorphism $\overline{f}$. □

Corollary I.5.10

Corollary I.5.10. Third Isomorphism Theorem.
If H and K are normal subgroups of a group G such that $K < H$, then H/K is a normal subgroup of G/K and $(G/K)/(H/K) \cong G/H$.

Proof. The identity map $1_G : G \to G$ satisfies $1_G(K) = K < H$. Define $I : G/K \to G/H$ as $I(aK) = aH$. Then I is a homomorphism (since the coset multiplication is done using representatives) and is onto since each coset of H is in $\text{Im}(I)$ (notice $K < H$ so K has "more" cosets in G than H). That is, I is an epimorphism. Now $H = I(aK)$ if and only if $a \in H$, so $\text{Ker}(I) = \{aK \mid a \in H\} = H/K$ (by definition of H/K as cosets of K in H). Since H/K is the kernel of a homomorphism then by Theorem I.5.5, $H/K \lhd G/H$. By Corollary I.5.7 (First Isomorphism Theorem), $G/H = \text{Im}(I) \cong (G/K)/\text{Ker}(I) = (G/K)/(H/K)$. □

Theorem I.5.11

Theorem I.5.11. If $f : G \to H$ is an epimorphism of groups, then the assignment $K \mapsto f(K)$ defines a one-to-one correspondence between the sets $S_f(G)$ of all subgroups K of G which contain $\text{Ker}(f)$ and the set $S(H)$ of all subgroups of H. Under this correspondence normal subgroups correspond to normal subgroups.

Proof. Since f is a homomorphism, then for $K < G$ we have $f(K)$ is a subgroup of H by Exercise I.2.9(b). So φ defined as $\varphi(K) = f(K)$ is a function $\varphi : S_f(G) \to S(H)$. By Exercise I.2.9(a), $f^{-1}(J)$ is a subgroup of G for every subgroup J of H. Since $J < H$ implies $\text{Ker}(f) < f^{-1}(J)$ (since $e \in J$) and $f(f^{-1}(J)) = J$, then φ is onto (since $\varphi(f^{-1}(J)) = J$). By Exercise I.5.18, $f^{-1}(f(K)) = K$ if and only if $\text{Ker}(f) < K$. Now by definition, $S_f(G)$ consists exactly of all subgroups K of G satisfying $\text{Ker}(f) < K$, and so $K < G$ with $f^{-1}(f(K)) = K$. So the only thing mapped to $f(K)$ under φ is K itself and φ is one to one. Hence, φ is one to one and onto; that is, φ is a one-to-one correspondence.
We leave the claim about corresponding subgroups as homework. □

Corollary I.5.12

Corollary I.5.12. If N is a normal subgroup of a group G, then every subgroup of G/N is of the form K/N, where K is a subgroup of G that contains N. Furthermore, K/N is normal in G/N if and only if K is normal in G.

Proof. Let $\pi : G \to G/N$ be the canonical epimorphism $\pi(g) = gN$. Then $\text{Ker}(\pi) = N$ (since N is the identity in G/N). By Theorem I.5.11 for every subgroup M of G/N (i.e., every element M of $S(H) = S(G/N)$ in the notation of Theorem I.5.11) there corresponds a subgroup K of G where K contains $\text{Ker}(\pi) = N$ (so K is in $S_\pi(G)$ in the notation of Theorem I.5.11). The correspondence is given by $\varphi(K) = \pi(K) = M$ and so $\pi(K) = \{kN \mid k \in K\} = K/N$, and $M \cong K/N$.
Furthermore, K/N is normal in G/N if and only if K is normal in G by the part of Theorem I.5.11 which states that normal subgroups correspond to normal subgroups. □