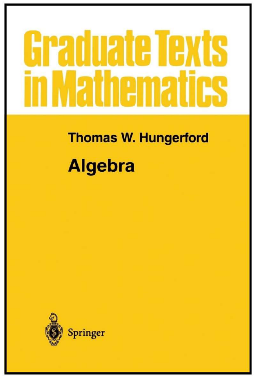
Modern Algebra

Chapter I. Groups

I.4. Cosets and Counting—Proofs of Theorems



Theorem I.4.2

Theorem I.4.2. Let H be a subgroup of a group G.

(*i*) Right and left congruence modulo H are each equivalence relations on G.

(*ii*) The equivalence class of $a \in G$ under right (and left) congruence modulo H is the set $Ha = \{ha \mid h \in H\}$ (and $aH = \{ah \mid h \in H\}$ for left congruence).

(*iii*) $|Ha| = |H| = |aH|$ for all $a \in G$.

The set Ha is a right coset of H in G and aH is a left coset of H in G.

Proof. We denote $a \equiv_r b \pmod{H}$ simply as $a \equiv b$ and prove the claims for right congruence with left congruence following similarly.
(i) Let $a, b, c \in G$. Then $a \equiv a$ since $aa^{-1} = e \in H$ (reflexive).
For $a \equiv b$ we have $ab^{-1} \in H$ and since H is a group, $(ab^{-1})^{-1} = ba^{-1} \in H$ and so $b \equiv a$ (symmetric).
Suppose $a \equiv b$ and $b \equiv c$. Then $ab^{-1}, bc^{-1} \in H$ and so $(ab^{-1})(bc^{-1}) = ac^{-1} \in H$ and so $a \equiv c$ (transitive). So $\equiv$ is an equivalence relation. □

Theorem I.4.2

Theorem I.4.2. Let H be a subgroup of a group G.

(*ii*) The equivalence class of $a \in G$ under right (and left) congruence modulo H is the set $Ha = \{ha \mid h \in H\}$ (and $aH = \{ah \mid h \in H\}$ for left congruence).

(*iii*) $|Ha| = |H| = |aH|$ for all $a \in G$.

The set Ha is a right coset of H in G and aH is a left coset of H in G.

Proof (continued). (ii) The equivalence class of $a \in G$ under right congruence is

$$\{x \in G \mid x \equiv a\} = \{x \in G \mid xa^{-1} \in H\} = \{x \in G \mid xa^{-1} = h, h \in H\}$$

$$= \{x \in G \mid x = ha, h \in H\} = \{ha \mid h \in H\} = Ha.$$

□

(iii) Define $\alpha : Ha \to H$ as $\alpha(ha) = h$. If $\alpha(h_1 a) = \alpha(h_2 a)$ then $h_1 = h_2$ and α is one to one. If $h \in H$ then $\alpha(ha) = h$ where $ha \in Ha$, so α is onto. Therefore $|Ha| = |H|$. □

Corollary I.4.3

Corollary I.4.3. Let H be a subgroup of group G.

(*i*) G is the union of the right (and left) cosets of H in G.

(*ii*) Two right (or two left) cosets of H in G are either disjoint or equal.

(*iii*) For $a, b \in G$, we have that $Ha = Hb$ if and only if $ab^{-1} \in H$, and $aH = bH$ if and only if $a^{-1}b \in H$.

(*iv*) If $\mathcal{R}$ is the set of distinct right cosets of H in G and $\mathcal{L}$ is the set of distinct left cosets of H in G, then $|\mathcal{R}| = |\mathcal{L}|$.

Proof. (iv) Define $\alpha : \mathcal{R} \to \mathcal{L}$ as $\alpha(Ha) = a^{-1}H$. If $\alpha(Ha) = \alpha(Hb)$ then $a^{-1}H = b^{-1}H$ and $(a^{-1})^{-1}b^{-1} \in H$ or $ab^{-1} \in H$ and so by (iii) $Ha = Hb$, so α is one to one. If $aH \in \mathcal{L}$ then $\alpha(Ha^{-1}) = (a^{-1})^{-1}H = aH$ and so α is onto. Since α is a bijection, then $|\mathcal{R}| = |\mathcal{L}|$. □

Theorem I.4.5

Theorem I.4.5. If K, H, G are groups with $K < H < G$, then $[G : K] = [G : H][H : K]$. If any two of these indices are finite, then so is the third.

Proof. By Corollary 4.3(i and ii), $G = \cup_{i \in I} Ha_i$ with $a_i \in G$ and $\{a_i \mid i \in I\}$ consists of exactly one element from each right coset of H in G (the set $\{a_i \mid i \in I\}$ is called a "complete set of right coset representatives" and $|\{a_i \mid i \in I\}| = |I| = [G : H]$). Similarly, $H = \cup_{j \in J} Kb_j$ with $b_j \in H$ and $|J| = [H : K]$. By Corollary 4.3(ii) the Ha_i are mutually disjoint and the Kb_j are mutually disjoint. Therefore

$$G = \cup_{i \in I} Ha_i = \cup_{i \in I} \left(\cup_{j \in J} Kb_j\right) a_i = \cup_{(i,j) \in I \times J} Kb_j a_i.$$

ASSUME that the $Kb_j a_i$ are not mutually disjoint.

Theorem I.4.5 (continued)

Theorem I.4.5. If K, H, G are groups with $K < H < G$, then $[G : K] = [G : H][H : K]$. If any two of these indices are finite, then so is the third.

Proof (continued). They are still cosets of K in G and so if they are not disjoint then they must be equal by Corollary 4.3(ii). Then our assumption implies $Kb_j a_i = Kb_r a_t$ for either $j \neq r$ or $i \neq t$. But then $b_j a_i = kb_r a_t$ for some $k \in K$ (choosing $e \in K$ on the left-hand side). Since $b_j, b_r, k \in H$ then $Ha_i = Hb_j a_i = H(b_j a_i) = H(kb_r a_t) = Hkb_r a_t = Ha_t$. So $i = t$ and $b_j a_i = kb_r a_t$ implies that $b_j = kb_r$. Thus $Kb_j = Kkb_r = Kb_r$ and $j = r$. Then $Kb_j a_i = Kb_r a_t$ only if $i = t$ and $j = r$, a CONTRADICTION to our assumption of not mutually disjoint. Therefore the cosets $Kb_j a_i$ are mutually disjoint and the cardinality of such cosets is $|I \times J| = |I||J|$ by the product of Cardinal numbers (see Definition 0.8.3 of Section 0.8. Cardinal Numbers). Whence(!) $[G : K] = |I \times J| = |I||J| = [G : H][H : K]$. "The last statement of the theorem is obvious." □

Corollary I.4.6, Lagrange's Theorem

Corollary I.4.6. Lagrange's Theorem.
If H is a subgroup of a group G, then $|G| = [G : H]|H|$. In particular, if G is finite then the order $|a|$ of $a \in G$ divides $|G|$ and $|H|$ divides $|G|$.

Proof. With $K = \langle e \rangle$ we have $[G : K] = [G : \langle e \rangle] = |G|$ and $[H : K] = [H : \langle e \rangle] = |H|$. We then have by Theorem I.4.5 that $[G : K] = [G : H][H : K]$ or $|G| = [G : H]|H|$. In the event that $H = \langle a \rangle$, $|a| = |H|$ and the second claim follows. □

Theorem I.4.7

Theorem I.4.7. Let H and K be finite subgroups of a group G. Then $|HK| = |H||K|/|H \cap K|$.

Proof. Let $C = H \cap K$. Then C is a finite subgroup of G by Corollary I.2.6. C is also a subgroup of H and of K. By Lagrange's Theorem (Corollary I.4.6), $[K : C] = |K|/|C| = |K|/|H \cap K| = n$. So K is the disjoint union of n cosets of C: $K = Ck_1 \cup Ck_2 \cup \cdots \cup Ck_n$ for some $k_i \in K$.

Next, we consider the sets HCk_i. ASSUME $HCk_i \cap HCk_j \neq \varnothing$ for some $i \neq j$. Then $h_1 c_1 k_i = h_2 c_2 k_j$ for some $h_1, h_2 \in H$ and $c_1, c_2 \in C$. Then $c_1 k_i k_j^{-1} = h_1^{-1} h_2 c_2 \in H$ since $h_1^{-1}, h_2 \in H$ and $c_1, c_2 \in C = H \cap K \subset H$. Also, $c_1^{-1} \in C \subset H$ and so $c_1^{-1}(c_1 k_i k_j^{-1}) = k_i k_j^{-1} \in H$. But $k_i k_j^{-1} \in K$ and so $k_i k_j^{-1} \in C$. By Corollary I.4.3(iii), this implies that $Ck_i = Ck_j$, CONTRADICTING the disjointness of the cosets Ck_i and Ck_j. So the assumption that $HCk_i \cap HCk_j \neq \varnothing$ is false and hence HCk_i and HCk_j are disjoint for all distinct i and j.

Theorem I.4.7 (continued)

Theorem I.4.7. Let H and K be finite subgroups of a group G. Then $|HK| = |H||K|/|H \cap K|$.

Proof (continued). Since $HC = H$ (because $C < H$), we have

$$\begin{aligned} HK &= H(Ck_1 \uplus Ck_2 \uplus \cdots \uplus Ck_n) \\ &= HCk_1 \uplus HCk_2 \uplus \cdots \uplus HCk_n \\ &= Hk_1 \uplus Hk_2 \uplus \cdots \uplus Hk_n. \end{aligned}$$

So HK consists of $n = |K|/|H \cap K|$ disjoint cosets of H in G and $|HK| = |H|n = |H|(|K|/|H \cap K|)$. □

Theorem I.4.8

Proposition I.4.8. If H and K are subgroups of a group G, then $[H : H \cap K] \le [G : K]$. If $[G : K]$ is finite, then $[H : H \cap K] = [G : K]$ if and only if $G = KH$.

Proof. Let A be the set of all right cosets of $H \cap K$ in H (of which there are $[H : H \cap K]$) and let B be the set of all right cosets of K in G (of which there are $[G : K]$). Define $\varphi : A \to B$ as $\varphi((H \cap K)h) = Kh$. Since φ is defined in terms of representatives (the h's in H) then we must confirm that φ is well-defined. Suppose $(H \cap K)h' = (H \cap K)h$. Then $h'h^{-1} \in H \cap K$ (by Corollary I.4.3(iii)). So $h'h^{-1} \in K$ and $Kh' = Kh$ (by Corollary I.4.3(iii)), or $\varphi((H \cap K)h') = \varphi((H \cap K)h)$ and φ is well-defined. Next, if $\varphi((H \cap K)h') = Kh' = Kh = \varphi((H \cap K)h)$, then $h'h^{-1} \in K$ (by Corollary I.4.3(iii)), $h'h^{-1} \in H \cap K$, and $(H \cap K)h' = (H \cap K)h$ (again, by Corollary I.4.3(iii)). So φ is one to one. Then the domain of φ is at most as large as the range of φ, or $[H : H \cap K] = |A| \le |B| = [G : K]$.

Theorem I.4.8 (continued)

Proof (continued). Suppose $[G : K]$ is finite. Then $[H : H \cap K] = |A| = |B| = [G : K]$ if and only if φ is onto (since we already know that φ is one to one by the above argument). So the second claim holds if and only if φ is onto (the finiteness of $[G : K]$ is used here). (1) Let $g \in G$. If φ is onto then for Kg a right coset of K in G we have $\varphi((H \cap K)h) = Kg$ for some $(H \cap K)h$ a right coset of $H \cap K$ in H. Then $\varphi((H \cap K)h) = Kh = Kg$ and so $gh^{-1} \in K$ (by Corollary I.4.3(iii)). Hence $(gh^{-1})h \in KH$, or $g \in KH$. So $G \subseteq KH$. Of course, since H and K are subgroups of G then $G \supseteq HK$. So if φ is onto then $G = KH$. (2) Suppose $G = KH$. Let Kg be a right coset of K in G. Since $G = KH$, then $g = kh$ for some $k \in K$ and $h \in H$. Hence $Kg = K(kh) = Kh$ since $k \in K$ and so $\varphi((H \cap K)h) = Kh = Kg$ and φ is onto. That is, φ is onto if and only if $G = KH$. So for finite $[G : K]$ we have $[H : H \cap K] = [G : K]$ if and only if $G = KH$. □

Proposition I.4.9

Proposition I.4.9. Let H and K be subgroups of finite index of group G. Then $[G : H \cap K]$ is finite and $[G : H \cap K] \le [G : H][G : K]$. Furthermore, $[G : H \cap K] = [G : H][G : K]$ if and only if $G = HK$.

Proof. We have $K \cap H < H < G$ and so by Theorem I.4.5 $[G : H \cap K] = [G : H][H : H \cap K]$. By Proposition I.4.8 $[H : H \cap K] \le [G : K]$ and so we have $[G : H \cap K] \le [G : H][G : K]$ as claimed and the hypotheses imply $[G : H \cap K]$ is finite. Also, by Proposition I.4.8, $[H : H \cap K] = [G : K]$ if and only if $G = KH$, so $[G : H \cap K] = [G : H][G : K]$ if and only if $G = KH$. □