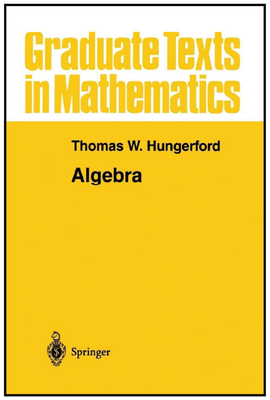
Modern Algebra

Chapter II. The Structure of Groups

II.4. The Action of a Group on a Set—Proofs of Theorems



Theorem II.4.3

Theorem II.4.3. If a group G acts on a set S, then the cardinal number of $x \in S$, $|\overline{x}|$, is the index $[G : G_x]$ (recall that $[G : G_x]$ is the cardinal number of the left cosets of subgroups G_x in group G).

Proof. Let $g, h \in G$. We denote the group action with a star, $\star$. We have

$$g \star x = h \star x \iff g^{-1} \star (h \star x) = g^{-1} \star (g \star x) = (g^{-1}g) \star x = x$$

$$\iff g^{-1}h \in G_x (\text{defn of } G_x) \iff hG_x = gG_x.$$

So the map given by $gG_x \mapsto g \star x$ is well defined. This mapping from the set of cosets of G_x in G into the orbit of x, $\overline{x} = \{g \star x \mid g \in G\}$ is one to one (by this string of equivalent statements) and onto (since $g \star x \in \overline{x}$ is the image of coset gG_x). So this mapping is a bijection. Hence the cardinality of the set of left cosets of G_x in G equals the cardinality of set $\overline{x}$, $[G : G_x] = |\overline{x}|$. □

Corollary II.4.4

Corollary II.4.4. Let G be a finite group and K a subgroup of G.

(i) The number of elements in the conjugacy class of $x \in G$ is $[G : C_G(x)]$, which divides $|G|$.

(ii) If $\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n$ are the distinct conjugacy classes of G, then $|G| = \sum_{i=1}^n [G : C_G(x_i)]$.

(iii) The number of subgroups of G conjugate to K is $[G : N_G(K)]$, which divides $|G|$.

Proof. (i) Now $C_G(x) = \{g \in G \mid gx = xg\} = \{g \in G \mid gxg^{-1} = x\}$ is a subgroup of G (by Theorem II.4.2(ii) where the action is conjugation). So by Theorem II.4.3, the number of elements in the conjugacy class of x is $|\overline{x}| = |\{gxg^{-1} \mid g \in G\}| = [G : C_G(x)]$ (since action is conjugation). By Lagrange's Theorem (Theorem I.4.6) $[G : C_G(x)] = |G|/|C_G(x)|$ and so $[G : C_G(x)]$ divides $|G|$.

Corollary II.4.4 (continued 1)

Corollary II.4.4. Let G be a finite group and K a subgroup of G.

(ii) If $\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n$ are the distinct conjugacy classes of G, then $|G| = \sum_{i=1}^n [G : C_G(x_i)]$.

Proof (continued). (ii) Since conjugation by an element of group G is an action on G (treated as a set) then by Theorem II.4.2(i), conjugation is an equivalence relation. The conjugacy classes $\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n$ are the orbits of G under the action of conjugation and so are equivalence classes of G. Since the equivalence classes must partition G (Theorem 0.4.1) then $|G| = \sum_{i=1}^n |\overline{x}_i| = \sum_{i=1}^n [G : C_G(x_i)]$ by Theorem II.4.3.

Corollary II.4.4 (continued 2)

Corollary II.4.4. Let G be a finite group and K a subgroup of G.

(iii) The number of subgroups of G conjugate to K is $[G : N_G(K)]$, which divides $|G|$.

Proof (continued). (iii) Now $N_G(K) = \{g \in G \mid gKg^{-1} = K\}$ is a subgroup of G (by Theorem II.4.2(ii) where set S is the set of all subgroups of G, so $x = K$ is an element of S, and the action is conjugation). Here, the orbit of $x = K$ under conjugation is $\overline{x} = \overline{K} = \{gKg^{-1} \mid g \in G\}$ and so $|\overline{x}| = |\overline{K}|$ is the number of distinct conjugates of K in G, each of which is a subgroup of G by Exercise I.5.6. So the number of subgroups of G conjugate to K is $|\overline{x}| = |\overline{K}|$ and by Theorem II.4.3 this equals $[G : N_G(K)]$. By Lagrange's Theorem (Theorem I.4.6) $[G : N_G(K)] = |G|/|N_G(K)|$ and so $[G : N_G(K)]$ divides $|G|$. □

Theorem II.4.5

Theorem II.4.5. If a group G acts on set S, then this action induces a homomorphism mapping $G \to A(S)$ where $A(S)$ is the group of all permutations of S.

Proof. We represent the group action with a star, $\star$. If $g \in G$, define $\tau_g : S \to S$ by $x \mapsto g \star x$. Since $x = e \star x = (g^{-1}g) \star x = g^{-1} \star (g \star x)$ for all $x \in S$, then τ_g is onto (since $\tau_g(g^{-1} \star x) = x$). Similarly, $g \star x = g \star y$ (where $x, y \in S$) implies

$$\begin{aligned} x &= g^{-1} \star (g \star x) \text{ by above} \\ &= g^{-1} \star (g \star y) \text{ by hypothesis} \\ &= y \text{ by above,} \end{aligned}$$

whence τ_g is one to one. So τ_g is a bijection from set S to set S, so τ_g is a permutation of set S (see the definition on page 26). By the definition of action, $\tau_{gg'} = \tau_g \tau_{g'}$ for all $g, g' \in G$, so the map $G \to A(S)$ given by $g \mapsto \tau_g$ is a homomorphism and this map is the desired ("induced") map. □

Corollary II.4.6

Corollary II.4.6. Cayley's Theorem.
If G is a group, then there is a monomorphism (a one to one homomorphism) mapping $G \to A(G)$. Hence, every group is isomorphic to a group of permutations. In particular, every finite group is isomorphic to a subgroup of S_n with $n = |G|$.

Proof. We represent the group action with a star, $\star$. Let G act on itself by left translation (so g acts on x to produce $g \star x = gx \in G$). Then by Theorem II.4.5, there is a homomorphism $\tau : G \to A(G)$; as seen in the proof, the homomorphism maps $g \in G$ to τ_g where $\tau_g(x) = g \star x = gx$. If $\tau(g) = \tau_g = 1_G$ (that is, g is mapped under τ to the identity of $A(G)$; so $g \in \mathrm{Ker}(\tau)$), then $g \star x = gx = \tau_g(x) = x$ for all $x \in G$. The only element such that $gx = x$ for all $x \in G$ is $g = e$. That is, $\mathrm{Ker}(\tau) = \{e\}$. By Theorem I.2.3(i) τ is a monomorphism (one to one homomorphism). So τ is an isomorphism between G and $\tau(G)$ and so G is isomorphic to a subgroup of $A(G)$ (that is, $\tau(G) < A(G)$ is a group of permutations). When $|G| = n$, $A(G) \cong S_n$ and this gives the second claim. □

Corollary II.4.7

Corollary II.4.7. Let G be a group.

(i) For each $g \in G$, conjugation by g induces an automorphism of G.

(ii) There is a homomorphism mapping $G \to \mathrm{Aut}(G)$ whose kernel is $C(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$.

Proof. (i) If G acts on itself by conjugation, then for each $g \in G$, the map $\tau_g : G \to G$ given by $\tau_g(x) = gxg^{-1}$ is a bijection, as shown in the proof of Theorem II.4.5. For $x, y \in G$, $\tau_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \tau_g(x)\tau_g(y)$ and so τ_g is a homomorphism. So τ_g is an isomorphism of G with itself. That is, τ_g is an automorphism of G—the automorphism induced by element $g \in G$.

Corollary II.4.7 (continued)

Corollary II.4.7. Let G be a group.

(i) For each $g \in G$, conjugation by g induces an automorphism of G.

(ii) There is a homomorphism mapping $G \to \text{Aut}(G)$ whose kernel is $C(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$.

Proof (continued). (ii) Let G act on itself by conjugation. By Theorem II.4.5, there is a homomorphism $\tau : G \to A(G)$ (where $A(G)$ is the group of all permutations of G). This τ is induced by the conjugation action, so for $g \in G$ we have $\tau(g) \in A(G)$ is the permutation of G that maps $x \in G$ to gxg^{-1}. Now if $g \in \text{Ker}(\tau)$ then $\tau(g) = 1_G$ and this is the case if and only if $gxg^{-1} = x$ for all $x \in G$. So if $g \in \text{Ker}(\tau)$ then $g \in C(G)$ (and if $g \in C(G)$ then $g \in \text{Ker}(\tau)$). That is, $\text{Ker}(\tau) = C(G)$. □

Proposition II.4.8

Proposition II.4.8. Let H be a subgroup of a group G and let G act on set S of all left cosets of H in G by left translation. Then the kernel of the induced homomorphism mapping $G \to A(S)$ is contained in H.

Proof. Since G acts on S by left translation, the induced homomorphism mapping $G \to A(S)$ maps g to the permutation of the set of left cosets of H, say τ_g, which maps xH to gxH (so $\tau_g(xH) = gxH$ and the homomorphism maps g to τ_g). If g is in the kernel of the homomorphism then $\tau_g = 1_S$ and so $gxH = xH$ for all $x \in G$. In particular, for $x = e$ we have $geH = eH = H$. Now $gH = H$ implies $g \in H$ (for example, $e \in H$ and so $ge = g \in H$). So the kernel is contained in H. □

Corollary II.4.9

Corollary II.4.9. If H is a subgroup of index n in a group G (that is, H has n left cosets in G) and no nontrivial normal subgroup of G is contained in H, then G is isomorphic to a subgroup of S_n.

Proof. Let S be the set of all left cosets of H in G. Let G act on the set S by left translation. By Proposition II.4.8, the kernel of the induced homomorphism mapping $G \mapsto A(S)$ is contained in H. The kernel is a normal subgroup of G by Theorem I.5.5. By hypothesis, the only normal subgroup of G contained in H is $\langle e \rangle$, so the kernel of the induced homomorphism is $\langle e \rangle$. By Theorem I.2.3(i) the induced homomorphism is a monomorphism (that is, it is one to one). Therefore G is isomorphic to a subgroup of the group of all permutations of the n left cosets of H. This group of permutations is isomorphic to S_n and so G is isomorphic to a subgroup of S_n. □

Corollary II.4.10

Corollary II.4.10. If H is a subgroup of a finite group G of index p (that is, H has p left cosets in G), where p is the smallest prime dividing the order of G, then H is normal in G.

Proof. Let S be the set of all left cosets of H in G. Then the set of all permutations of S, $A(S)$, forms a group isomorphic to S_p since the number of left cosets in $[G : H] = p$. If K is the kernel of the induced homomorphism mapping $G \to A(S)$ of Proposition II.4.8, then K is normal in G (as shown in the proof of Corollary II.4.9) and is contained in H (as shown in the proof of Proposition II.4.8). Furthermore, G/K is isomorphic to a subgroup of S_p by the First Isomorphism Theorem (Corollary I.5.7; the image of the induced homomorphism is some subgroup of $A(S)$). Hence, by Lagrange's Theorem (Corollary I.4.6), $|G/K|$ divides $|S_p| = p!$. But every divisor of $|G/K| = [G : K]$ must divide $|G| = |K|[G : K]$.

Corollary II.4.10 (continued)

Corollary II.4.10. If H is a subgroup of a finite group G of index p (that is, H has p left cosets in G), where p is the smallest prime dividing the order of G, then H is normal in G.

Proof (continued). Since no number smaller than p (except 1) can divide $|G|$, we must have $|G/K| = p$ or $|G/K| = 1$. However

$$\begin{aligned} |G/K| &= [G:K] = [G:H][H:K] \\ &= p[H:K] \text{ since } p = [G:H] \text{ by hypothesis} \\ &\geq p. \end{aligned}$$

Therefore $|G/K| = p$ and it must be that $[H:K] = 1$. So $H = K$. But K is normal in G and so H is normal in G. □