Introduction to Modern Algebra

Part VII. Advanced Group Theory

VII.37. Applications of the Sylow Theorems

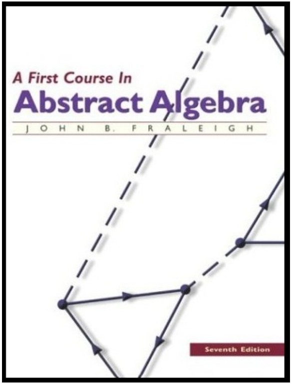

Table of contents

Theorem 37.1.

Theorem 37.1. Every group of prime - power (that is, every finite p-group) is solvable.

Proof. If G has order p^r, then by the First Sylow Theorem (Theorem 36.8) that G has a subgroup H_i of order p^i (part (1)) which is normal in a subgroup H_{i+1} of order p^{i+1} (by part (2)) for $i \leq i < r$. Then $\{e\} = H_0 < H_1 < \cdots < H_r = G$ is a composition series, since H_{i+1}/H_i is of order p and hence is simple (since it has no proper nontrivial subgroups, let alone any normal subgroups).

Theorem 37.1.

Theorem 37.1. Every group of prime - power (that is, every finite p-group) is solvable.

Proof. If G has order p^r, then by the First Sylow Theorem (Theorem 36.8) that G has a subgroup H_i of order p^i (part (1)) which is normal in a subgroup H_{i+1} of order p^{i+1} (by part (2)) for $i \leq i < r$. Then $\{e\} = H_0 < H_1 < \cdots < H_r = G$ is a composition series, since H_{i+1}/H_i is of order p and hence is simple (since it has no proper nontrivial subgroups, let alone any normal subgroups). In addition, since H_{i+1}/H_i is a group o f order p, then by the Fundamental Theorem of Finitely Generated Abelian Groups (Theorem 11.12), $H_{i+1}/H_i \cong \mathbb{Z}_p$ and hence is abelian. Therefore, G is solvable. □

Theorem 37.1.

Theorem 37.1. Every group of prime - power (that is, every finite p-group) is solvable.

Proof. If G has order p^r, then by the First Sylow Theorem (Theorem 36.8) that G has a subgroup H_i of order p^i (part (1)) which is normal in a subgroup H_{i+1} of order p^{i+1} (by part (2)) for $i \le i < r$. Then $\{e\} = H_0 < H_1 < \cdots < H_r = G$ is a composition series, since H_{i+1}/H_i is of order p and hence is simple (since it has no proper nontrivial subgroups, let alone any normal subgroups). In addition, since H_{i+1}/H_i is a group o f order p, then by the Fundamental Theorem of Finitely Generated Abelian Groups (Theorem 11.12), $H_{i+1}/H_i \cong \mathbb{Z}_p$ and hence is abelian. Therefore, G is solvable. □

Theorem 37.4.

Theorem 37.4. The center of a finite nontrivial p-group G is nontrivial.

Proof. In the class equation for G, each n_i divides $|G|$ for $c + 1 \leq i \leq r$. By Corollary 36.4, $|G| = p^n$ for some $n \in \mathbb{N}$.

Theorem 37.4.

Theorem 37.4. The center of a finite nontrivial p-group G is nontrivial.

Proof. In the class equation for G, each n_i divides $|G|$ for $c + 1 \leq i \leq r$. By Corollary 36.4, $|G| = p^n$ for some $n \in \mathbb{N}$. So p divides n_i (notice that each $n_i > 1$ since the fixed points are all contained in $X_G = Z(G)$) for each $c + 1 \leq i \leq r$. So p must also divide c. Since $e \in Z(G)$, then $c \geq 1$ and it follows that $c \geq p \geq 2$ and hence $Z(G)$ is nontrivial. □

Theorem 37.4.

Theorem 37.4. The center of a finite nontrivial p-group G is nontrivial.

Proof. In the class equation for G, each n_i divides $|G|$ for $c+1 \leq i \leq r$. By Corollary 36.4, $|G| = p^n$ for some $n \in \mathbb{N}$. So p divides n_i (notice that each $n_i > 1$ since the fixed points are all contained in $X_G = Z(G)$) for each $c+1 \leq i \leq r$. So p must also divide c. Since $e \in Z(G)$, then $c \geq 1$ and it follows that $c \geq p \geq 2$ and hence $Z(G)$ is nontrivial. $\square$

Lemma 37.5.

Lemma 37.5. Let G be a group containing normal subgroups H and K such that $H \cap K = \{e\}$ and $H \vee K = G$. Then G is isomorphic to $H \times K$.

Proof. Let $h \in H$ and $k \in K$. We have $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$ by associativity. Since H is a normal subgroup, then $kh^{-1}k^{-1} \in H$ (Theorem 14.13(2)) and so $h(kh^{-1}k^{-1}) \in H$. Since K is a normal subgroup, then $hkh^{-1} \in K$ (Theorem 14.13(2)) and so $(hkh^{-1}) \in K$ So we have $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1}) \in K \cap H$. Since $K \cap H = \{e\}$ by hypothesis, then $hkh^{-1}k^{-1} = e$ and $hk = kh$.

Lemma 37.5.

Lemma 37.5. Let G be a group containing normal subgroups H and K such that $H \cap K = \{e\}$ and $H \vee K = G$. Then G is isomorphic to $H \times K$.

Proof. Let $h \in H$ and $k \in K$. We have $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$ by associativity. Since H is a normal subgroup, then $kh^{-1}k^{-1} \in H$ (Theorem 14.13(2)) and so $h(kh^{-1}k^{-1}) \in H$. Since K is a normal subgroup, then $hkh^{-1} \in K$ (Theorem 14.13(2)) and so $(hkh^{-1}) \in K$ So we have $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1}) \in K \cap H$. Since $K \cap H = \{e\}$ by hypothesis, then $hkh^{-1}k^{-1} = e$ and $hk = kh$.

Let $\varphi : H \times K \to G$ be defined as $\varphi(hk) = hk$. Notice that for $(h, k), (h', k') = (hh', kk')$.

Lemma 37.5.

Lemma 37.5. Let G be a group containing normal subgroups H and K such that $H \cap K = \{e\}$ and $H \vee K = G$. Then G is isomorphic to $H \times K$.

Proof. Let $h \in H$ and $k \in K$. We have $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$ by associativity. Since H is a normal subgroup, then $kh^{-1}k^{-1} \in H$ (Theorem 14.13(2)) and so $h(kh^{-1}k^{-1}) \in H$. Since K is a normal subgroup, then $hkh^{-1} \in K$ (Theorem 14.13(2)) and so $(hkh^{-1}) \in K$ So we have $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1}) \in K \cap H$. Since $K \cap H = \{e\}$ by hypothesis, then $hkh^{-1}k^{-1} = e$ and $hk = kh$.

Let $\varphi : H \times K \to G$ be defined as $\varphi(hk) = hk$. Notice that for $(h, k), (h', k') = (hh', kk')$.

Lemma 37.5 (Continued 1).

Lemma 37.5 (Continued). Let G be a group containing normal subgroups H and K such that $H \cap K = \{e\}$ and $H \vee K = G$. Then G is isomorphic to $H \times K$.

Proof (Continued). Then

$$\begin{aligned} \varphi((h,k)\cdot(h',k')) &= \varphi(hh',kk') \\ &= hh'kk' \text{ by the definition of } \varphi \\ &= hkh'k' \text{ by the result of the first paragraph} \\ &= \varphi(h,k)\varphi(h',k') \text{ by the definition of } \varphi. \end{aligned}$$

So φ is a homomorphism.

Lemma 37.5 (Continued 2).

Lemma 37.5 (Continued). Let G be a group containing normal subgroups H and K such that $H \cap K = \{e\}$ and $H \vee K = G$. Then G is isomorphic to $H \times K$.

Proof (Continued). If $\varphi(h, k) = hk = e$, then $h = k^{-1}$ and so, since H and K are groups, both h and k are in $H \cap K$. But then $h = k = e$ and so $\text{Ker}(\varphi) = \{(e, e)\}$ (the identity in $H \times K$) and so φ is one to one by Corollary 13.18.

By Lemma 34.4, since K is a normal subgroup of G and H is subgroup of G, then $HK = H \vee K$. Also, $H \vee K = G$ by hypothesis. By the definition of φ, φ is onto $HK = H \vee K = G$. So φ is a one to one and onto homomorphism from $H \times K$ to G. That is, $G \cong H \times K$. □

Lemma 37.5 (Continued 2).

Lemma 37.5 (Continued). Let G be a group containing normal subgroups H and K such that $H \cap K = \{e\}$ and $H \vee K = G$. Then G is isomorphic to $H \times K$.

Proof (Continued). If $\varphi(h,k) = hk = e$, then $h = k^{-1}$ and so, since H and K are groups, both h and k are in $H \cap K$. But then $h = k = e$ and so $\mathrm{Ker}(\varphi) = \{(e,e)\}$ (the identity in $H \times K$) and so φ is one to one by Corollary 13.18.

By Lemma 34.4, since K is a normal subgroup of G and H is subgroup of G, then $HK = H \vee K$. Also, $H \vee K = G$ by hypothesis. By the definition of φ, φ is onto $HK = H \vee K = G$. So φ is a one to one and onto homomorphism from $H \times K$ to G. That is, $G \cong H \times K$. $\square$

Theorem 37.6.

Theorem. 37.6. For a prime number p, every group of order p^2 is abelian.

Proof. If G is not cyclic (and so no element is of order $|G| = p^2$), then every element of G except e must be of order p. Let a be such a element. Then the cyclic subgroup $\langle a \rangle$ of order p does not equal G. Also let $b \in G$ with $b \notin \langle a \rangle$. Then $\langle a \rangle \cap \langle b \rangle = \{e\}$ (otherwise, if $e \neq c \in \langle a \rangle \cap \langle b \rangle$ then c generates both the First Sylow Theorem (Theorem 36.8), $\langle a \rangle$ is a normal subgroup of order p^1 of group G (of order p^2).

Theorem 37.6.

Theorem. 37.6. For a prime number p, every group of order p^2 is abelian.

Proof. If G is not cyclic (and so no element is of order $|G| = p^2$), then every element of G except e must be of order p. Let a be such a element. Then the cyclic subgroup $\langle a \rangle$ of order p does not equal G. Also let $b \in G$ with $b \notin \langle a \rangle$. Then $\langle a \rangle \cap \langle b \rangle = \{e\}$ (otherwise, if $e \neq c \in \langle a \rangle \cap \langle b \rangle$ then c generates both the First Sylow Theorem (Theorem 36.8), $\langle a \rangle$ is a normal subgroup of order p^1 of group G (of order p^2). Similarly, $\langle b \rangle$ is a normal subgroup of order p of G. Now $\langle a \rangle \vee \langle b \rangle$ is a subgroup of G which properly contains $\langle a \rangle$ (since $b \in \langle a \rangle \vee \langle b \rangle$ but $b \in \langle a \rangle$). Since $|\langle a \rangle| = p$, then $|\langle a \rangle \vee \langle b \rangle|$ must be p^2 and hence $\langle a \rangle \vee \langle b \rangle = G$. So the hypothesis of Lemma 37.5 are satisfied (with $H = \langle a \rangle$) and $K = \langle b \rangle$), and hence $G \cong \langle a \rangle \times \langle b \rangle$. Since $\langle a \rangle$ and $\langle b \rangle$ are cyclic of order p, we have $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$ by the Fundamental (Theorem 11.12), G is abelian. $\square$

Theorem 37.6.

Theorem. 37.6. For a prime number p, every group of order p^2 is abelian.

Proof. If G is not cyclic (and so no element is of order $|G| = p^2$), then every element of G except e must be of order p. Let a be such a element. Then the cyclic subgroup $\langle a \rangle$ of order p does not equal G. Also let $b \in G$ with $b \notin \langle a \rangle$. Then $\langle a \rangle \cap \langle b \rangle = \{e\}$ (otherwise, if $e \neq c \in \langle a \rangle \cap \langle b \rangle$ then c generates both the First Sylow Theorem (Theorem 36.8), $\langle a \rangle$ is a normal subgroup of order p^1 of group G (of order p^2). Similarly, $\langle b \rangle$ is a normal subgroup of order p of G. Now $\langle a \rangle \vee \langle b \rangle$ is a subgroup of G which properly contains $\langle a \rangle$ (since $b \in \langle a \rangle \vee \langle b \rangle$ but $b \in \langle a \rangle$). Since $|\langle a \rangle| = p$, then $|\langle a \rangle \vee \langle b \rangle|$ must be p^2 and hence $\langle a \rangle \vee \langle b \rangle = G$. So the hypothesis of Lemma 37.5 are satisfied (with $H = \langle a \rangle$) and $K = \langle b \rangle$), and hence $G \cong \langle a \rangle \times \langle b \rangle$. Since $\langle a \rangle$ and $\langle b \rangle$ are cyclic of order p, we have $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$ by the Fundamental (Theorem 11.12), G is abelian. □

Theorem 37.7.

Theorem. 37.7. If p and q are prime with $p < q$, then every group G of order pq has a single subgroup of order q and this subgroup is normal in G. Hence G is not simple. If q is not congruent to 1 modulo p, then G is abelian and cyclic.

Proof. By the First Sylow Theorem (Theorem 16.8), G has a subgroup of order q. Since $|G| = pq$, then this subgroup cannot be a subgroup of another subgroup of G of order a power of a prime (by Lagrange's Theorem). So this group of order q is a Sylow q-subgroup. By the Third Sylow Theorem (Theorem 36.11), the number of such subgroups is congruent to 1 modulo q and divides $pq = |G|$; therefore the number of such subgroups must divide p.

Theorem 37.7.

Theorem. 37.7. If p and q are prime with $p < q$, then every group G of order pq has a single subgroup of order q and this subgroup is normal in G. Hence G is not simple. If q is not congruent to 1 modulo p, then G is abelian and cyclic.

Proof. By the First Sylow Theorem (Theorem 16.8), G has a subgroup of order q. Since $|G| = pq$, then this subgroup cannot be a subgroup of another subgroup of G of order a power of a prime (by Lagrange's Theorem). So this group of order q is a Sylow q-subgroup. By the Third Sylow Theorem (Theorem 36.11), the number of such subgroups is congruent to 1 modulo q and divides $pq = |G|$; therefore the number of such subgroups must divide p. Since $p < q$ and this number is $1 \pmod{q}$, then this number must be 1. Hence these is a single subgroup of G of order q, say Q. Now the mapping $i_g : G \to G$ defined as $i_g(x) = gxg^{-1}$ is a homomorphism of G by Exercise 13.29. By Theorem 13.12(3), if Q is a subgroup of G (since i_g is a homomorphism).

Theorem 37.7.

Theorem. 37.7. If p and q are prime with $p < q$, then every group G of order pq has a single subgroup of order q and this subgroup is normal in G. Hence G is not simple. If q is not congruent to 1 modulo p, then G is abelian and cyclic.

Proof. By the First Sylow Theorem (Theorem 16.8), G has a subgroup of order q. Since $|G| = pq$, then this subgroup cannot be a subgroup of another subgroup of G of order a power of a prime (by Lagrange's Theorem). So this group of order q is a Sylow q-subgroup. By the Third Sylow Theorem (Theorem 36.11), the number of such subgroups is congruent to 1 modulo q and divides $pq = |G|$; therefore the number of such subgroups must divide p. Since $p < q$ and this number is $1 (\mathrm{mod}\ q)$, then this number must be 1. Hence these is a single subgroup of G of order q, say Q. Now the mapping $i_g : G \to G$ defined as $i_g(x) = gxg^{-1}$ is a homomorphism of G by Exercise 13.29. By Theorem 13.12(3), if Q is a subgroup of G (since i_g is a homomorphism).

Theorem 37.7 (Continued 1).

Proof (Continued). Also, i_g is one to one ($gag^{-1} = gbg^{-1}$ implies $a = b$). So $i_g[Q]$ is a subgroup of G of order q; that is, $i_g[Q] = Q$ for all $g \in G$. Then, $gQg^{-1} = Q$ for all $g \in G$ and by Theorem 14.13(2), Q is a normal subgroup of G. Therefore, G is not simple.

Likewise, there is a Sylow p-subgroup P of G, and the number of these, n, divides pq and is congruent to 1 modulo p. Then n must be either 1 or q. Now suppose $q \not\equiv 1 (\text{mod } p)$ as hypothesized. Since n is either 1 or q and $n \equiv 1 (\text{mod } p)$, then it must be that $n = 1$. As argued above, it must be that $ig[P] = P$ for all $g \in G$ and P is a normal subgroup of G.

Theorem 37.7 (Continued 1).

Proof (Continued). Also, i_g is one to one ($gag^{-1} = gbg^{-1}$ implies $a = b$). So $i_g[Q]$ is a subgroup of G of order q; that is, $i_g[Q] = Q$ for all $g \in G$. Then, $gQg^{-1} = Q$ for all $g \in G$ and by Theorem 14.13(2), Q is a normal subgroup of G. Therefore, G is not simple.

Likewise, there is a Sylow p-subgroup P of G, and the number of these, n, divides pq and is congruent to 1 modulo p. Then n must be either 1 or q. Now suppose $q \not\equiv 1 (\text{mod } p)$ as hypothesized. Since n is either 1 or q and $n \equiv 1 (\text{mod } p)$, then it must be that $n = 1$. As argued above, it must be that $ig[P] = P$ for all $g \in G$ and P is a normal subgroup of G.

Theorem 37.7 (Continued 2).

Proof (Continued). Since every element in Q other than e is of order q and every element of P other than e is of order p¡ then $Q \cap P = \{e\}$. Since P and and Q are normal subgroups by Lemma 34.4, $Q \vee P = QP = PQ$. Now $Q \vee P$ is a subgroup of G which properly contains Q (and P) and so is of an order dividing $|G| = pq$. So it must be that $G = Q \vee P$ and by Lemma 37.5 $G \cong Q \times P$. Since Q is cyclic of order q and P is cyclic of order P, then Q and P are abelian and by the Fundamental Theorem of Finitely Generated Abelian Groups (Theorem 11.12), $Q \cong \mathbb{Z}_q$ and $P \cong \mathbb{Z}_p$. So $G \cong Q \times P = \mathbb{Z}_q \times \mathbb{Z}_p$. Since p and q are relatively prime, G is cyclic and hence abelian (by Theorem 6.1). □

Theorem 37.7 (Continued 2).

Proof (Continued). Since every element in Q other than e is of order q and every element of P other than e is of order p¡ then $Q \cap P = \{e\}$. Since P and and Q are normal subgroups by Lemma 34.4, $Q \vee P = QP = PQ$. Now $Q \vee P$ is a subgroup of G which properly contains Q (and P) and so is of an order dividing $|G| = pq$. So it must be that $G = Q \vee P$ and by Lemma 37.5 $G \cong Q \times P$. Since Q is cyclic of order q and P is cyclic of order P, then Q and P are abelian and by the Fundamental Theorem of Finitely Generated Abelian Groups (Theorem 11.12), $Q \cong \mathbb{Z}_q$ and $P \cong \mathbb{Z}_p$. So $G \cong Q \times P = \mathbb{Z}_q \times \mathbb{Z}_p$. Since p and q are relatively prime, G is cyclic and hence abelian (by Theorem 6.1). □

Lemma 37.8.

Lemma 37.8. If H and K are finite subgroups of a group G, then $|HK| = \frac{|H|\cdot|K|}{|H\cap K|}$.

Proof. Recall that $HK = \{hk \mid h \in H, k \in K\}$. Let $|H| = r$, $|K| = s$, and $|H \cap K| = \varphi$. We have $|HK| \leq rs$. We now count "repetition" in HK. If $h_1k_1 = h_2k_2$, then let $x = h_2^{-1}h_1 = k_2k_1^{-1}$. Since $x = h_2^{-1}h_1$ then $x \in H$. Since $x = k_2k_1^{-1}$ then $x \in K$; so $x \in H \cap K$.

Lemma 37.8.

Lemma 37.8. If H and K are finite subgroups of a group G, then $|HK| = \frac{|H|\cdot|K|}{|H\cap K|}$.

Proof. Recall that $HK = \{hk \mid h \in H, k \in K\}$. Let $|H| = r$, $|K| = s$, and $|H \cap K| = \varphi$. We have $|HK| \leq rs$. We now count "repetition" in HK. If $h_1 k_1 = h_2 k_2$, then let $x = h_2^{-1} h_1 = k_2 k_1^{-1}$. Since $x = h_2^{-1} h_1$ then $x \in H$. Since $x = k_2 k_1^{-1}$ then $x \in K$; so $x \in H \cap K$. So a repetition of a representation of an element of HK corresponds to an element of $H \cap K$. Conversely, let $y \in H \cap K$ and define $h_3 = h_1 y^{-1}$ and $k_3 = yk_1$ (where h_1, k_1 are as above). Then $h_3 k_3 = (h_1 y^{-1})(yk_1) = h_1 k_1$. So each $y \in H \cap K$ yields a representation of $h_1 k_1$ (namely, $h_3 k_3$). So there is a one-to-one correspondence between the elements of $H \cap K$ and the repetitions of representations of elements of HK. So $|HK| = \frac{rs}{t}$ and the result follows. □

Lemma 37.8.

Lemma 37.8. If H and K are finite subgroups of a group G, then $|HK| = \frac{|H|\cdot|K|}{|H\cap K|}$.

Proof. Recall that $HK = \{hk \mid h \in H, k \in K\}$. Let $|H| = r$, $|K| = s$, and $|H \cap K| = \varphi$. We have $|HK| \leq rs$. We now count "repetition" in HK. If $h_1 k_1 = h_2 k_2$, then let $x = h_2^{-1} h_1 = k_2 k_1^{-1}$. Since $x = h_2^{-1} h_1$ then $x \in H$. Since $x = k_2 k_1^{-1}$ then $x \in K$; so $x \in H \cap K$. So a repetition of a representation of an element of HK corresponds to an element of $H \cap K$. Conversely, let $y \in H \cap K$ and define $h_3 = h_1 y^{-1}$ and $k_3 = yk_1$ (where h_1, k_1 are as above). Then $h_3 k_3 = (h_1 y^{-1})(yk_1) = h_1 k_1$. So each $y \in H \cap K$ yields a representation of $h_1 k_1$ (namely, $h_3 k_3$). So there is a one-to-one correspondence between the elements of $H \cap K$ and the repetitions of representations of elements of HK. So $|HK| = \frac{rs}{t}$ and the result follows. □