Introduction to Modern Algebra

Part VII. Advanced Group Theory

VII.36. Sylow Theorems

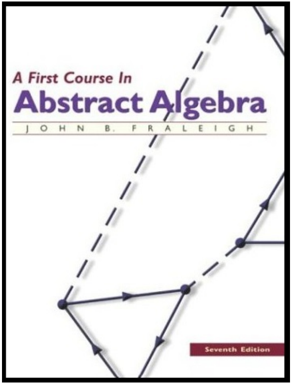

Table of contents

Theorem 36.1.

Theorem. 36.1. Let G be a group of order p^n and let X be a finite G set. Then $|X| \equiv |X_G| (\text{mod } p)$.

Proof. With the notation above, Theorem 16.16 implies that $|Gx_i|$ divides $|G|$ for $i = 1, 2, \ldots, r$. In particular, for $i = s+1, s+2, \ldots, r$ we have that $|Gx_i|$ divides $|G| = p^n$, and so p must divide $|Gx_i|$ for $i = s+1, s+2, \ldots, r$. Hence P divides $\sum_{i=s+1}^{r} |Gx_i| = |X| - |X_G|$ (by equation (2)) and so $|X| - |X_G| \equiv 0 (\mod p)$ and the result follows. □

Theorem 36.1.

Theorem. 36.1. Let G be a group of order p^n and let X be a finite G set. Then $|X| \equiv |X_G| (\text{mod } p)$.

Proof. With the notation above, Theorem 16.16 implies that $|Gx_i|$ divides $|G|$ for $i = 1, 2, \ldots, r$. In particular, for $i = s+1, s+2, \ldots, r$ we have that $|Gx_i|$ divides $|G| = p^n$, and so p must divide $|Gx_i|$ for $i = s+1, s+2, \ldots, r$. Hence P divides $\displaystyle\sum_{i=s+1}^{r} |Gx_i| = |X| - |X_G|$ (by equation (2)) and so $|X| - |X_G| \equiv 0(\text{ mod } p)$ and the result follows. □

Theorem 36.3. Cauchy's Theorem

Theorem 36.3. Cauchy's Theorem.
Let p be a prime. Let G be a finite group and let p divide $|G|$. Then G has an element of order p and (consequently) a subgroups of order p.

Proof. With p given, we form the set X of all p-tuples $(g_1, g_2, \ldots, g_p)$ of elements of G having the property that the product of these elements is e: $X = \{(g_1, g_2, \ldots, g_p) \mid g_i \in G \text{ and } g_1 g_2 \cdots g_n = e\}$.

Theorem 36.3. Cauchy's Theorem

Theorem 36.3. Cauchy's Theorem.
Let p be a prime. Let G be a finite group and let p divide $|G|$. Then G has an element of order p and (consequently) a subgroups of order p.

Proof. With p given, we form the set X of all p-tuples $(g_1, g_2, \ldots, g_p)$ of elements of G having the property that the product of these elements is e: $X = \{(g_1, g_2, \ldots, g_p) \mid g_i \in G \text{ and } g_1 g_2 \cdots g_n = e\}$. Notice that in forming a p-tuple the first $p-1$ elements can be ANY elements of G, as long as the pth element is the inverse of the product of these $p-1$ elements: $g_p = (g_1 g_2 \cdots g_{p-1})^{-1}$ (and conversely, if we have a p-tuple in X then g_p must have this property). Now there are $|G|^{p-1}$ ways to choose the first $p-1$ elements and only 1 way to choose the pth element, hence there are $|G|^{p-1}$ such p-tuples and $|X| = |G|^{p-1}$. Since p divides $|G|$, then p divides $|X|$.

Theorem 36.3. Cauchy's Theorem

Theorem 36.3. Cauchy's Theorem.
Let p be a prime. Let G be a finite group and let p divide $|G|$. Then G has an element of order p and (consequently) a subgroups of order p.

Proof. With p given, we form the set X of all p-tuples $(g_1, g_2, \ldots, g_p)$ of elements of G having the property that the product of these elements is e: $X = \{(g_1, g_2, \ldots, g_p) \mid g_i \in G \text{ and } g_1 g_2 \cdots g_n = e\}$. Notice that in forming a p-tuple the first $p-1$ elements can be ANY elements of G, as long as the pth element is the inverse of the product of these $p-1$ elements: $g_p = (g_1 g_2 \cdots g_{p-1})^{-1}$ (and conversely, if we have a p-tuple in X then g_p must have this property). Now there are $|G|^{p-1}$ ways to choose the first $p-1$ elements and only 1 way to choose the pth element, hence there are $|G|^{p-1}$ such p-tuples and $|X| = |G|^{p-1}$. Since p divides $|G|$, then p divides $|X|$.

Theorem 36.3. Cauchy's Theorem (Continued 1)

Theorem. 36.3. Cauchy's Theorem.
Let p be a prime. Let G be a finite group and let p divide $|G|$. Then G has an element of order p and (consequently) a subgroups of order p.

Proof (Continued). Let $\sigma = (1, 2, 3, \ldots, p) \in S_p$ and let σ act on X as $\sigma(g_1, g_2, \ldots, g_p) = (g_{\sigma(1)}, g_{\sigma(2)}, \ldots, g_{\sigma(p)}) = (g_2, g_3, \ldots, g_p, g_1)$. Notice that $(g_2, g_3, \ldots, g_p, g_1) \in X$ since $(g_1, g_2, \ldots, g_p) \in X$ implies $g_1 g_2 g_3 \cdots g_p = e$, which in turn implies $g_1 = (g_2 g_3 \cdots g_p)^{-1}$ and that $(g_2 g_3 \cdots g_p) g_1 = e$. So σ acts on X and we consider the subgroup $\langle \sigma \rangle$ of S_p which acts on X.

Theorem 36.3. Cauchy's Theorem (Continued 2).

Theorem 36.3. Cauchy's Theorem.
Let p be a prime. Let G be a finite group and let p divide $|G|$. Then G has an element of order p and (consequently) a subgroups of order p.

Proof (Continued). Now $|\langle\sigma\rangle| = p$ and so by Theorem 36.1 we know that $|X| \equiv |X_{\langle\sigma\rangle}| \pmod{p}$ $(*)$. Since p divides $|X|$ then p must divide $|X_{\langle\sigma\rangle}|$ also. The only p-tuple in X left fixed by σ (and hence left fixed by $\langle\sigma\rangle$) is $(g_1, g_2, \ldots, g_p)$ where $g_1 = g_2 = \cdots = g_p$.

Theorem 36.3. Cauchy's Theorem (Continued 2).

Theorem 36.3. Cauchy's Theorem.
Let p be a prime. Let G be a finite group and let p divide $|G|$. Then G has an element of order p and (consequently) a subgroups of order p.

Proof (Continued). Now $|\langle\sigma\rangle| = p$ and so by Theorem 36.1 we know that $|X| \equiv |X_{\langle\sigma\rangle}| \pmod{p}$ $(*)$. Since p divides $|X|$ then p must divide $|X_{\langle\sigma\rangle}|$ also. The only p-tuple in X left fixed by σ (and hence left fixed by $\langle\sigma\rangle$) is $(g_1, g_2, \ldots, g_p)$ where $g_1 = g_2 = \cdots = g_p$. One such p-tuple is $(e, e, \ldots, e)$. But since $|X_{\langle\sigma\rangle}|$ is a multiple of prime $p \geq 2$, there is some other $(a, a, \ldots, a) \in X_{\langle\sigma\rangle}$ where $a \neq e$. Hence $a^p = e$ and so a has order p (no smaller positive power of a could be e since p is prime [consider Lagrange's Theorem]). Then $\langle a\rangle$ is a subgroup of G of order p. □

Theorem 36.3. Cauchy's Theorem (Continued 2).

Theorem 36.3. Cauchy's Theorem.
Let p be a prime. Let G be a finite group and let p divide $|G|$. Then G has an element of order p and (consequently) a subgroups of order p.

Proof (Continued). Now $|\langle\sigma\rangle| = p$ and so by Theorem 36.1 we know that $|X| \equiv |X_{\langle\sigma\rangle}| (\text{mod } p)$ $(*)$. Since p divides $|X|$ then p must divide $|X_{\langle\sigma\rangle}|$ also. The only p-tuple in X left fixed by σ (and hence left fixed by $\langle\sigma\rangle$) is $(g_1, g_2, \ldots, g_p)$ where $g_1 = g_2 = \cdots = g_p$. One such p-tuple is $(e, e, \ldots, e)$. But since $|X_{\langle\sigma\rangle}|$ is a multiple of prime $p \geq 2$, there is some other $(a, a, \ldots, a) \in X_{\langle\sigma\rangle}$ where $a \neq e$. Hence $a^p = e$ and so a has order p (no smaller positive power of a could be e since p is prime [consider Lagrange's Theorem]). Then $\langle a\rangle$ is a subgroup of G of order p. □

Lemma 36.6.

Lemma 36.6. Let H be a p-subgroup of a finite group G. Then $(N[H] : H) \equiv (G : H) (\mathrm{mod}\ p)$.

Proof. First, recall that $(G : H)$ is the number of left cosets of H in G. Let L be the set of left cosets of H in G, and let H act on L by "left translation" so that $h(xH) = (hx)H$. Then L is an H-set since $(h_1 h_2)(xh) = (h_1(h_2 x))h$ for all $h_1, h_2, h \in H$ and for all $x \in G$ (by associativity, and so $(h_1 h_2)(xH) = h_1(h_2 xH)$). Also, by definition, $|L| = (G : H)$.

Now L_H is the set of left cosets that are fixed under action by all elements of H (by definition of the symbols "L_H"). Now $xH = h(xH)$ for all $h \in H^*$ if and only if $xh_1 = h(xh_2)$ for some $h_1, h_2 \in H$; that is $h_1 = (x^{-1}hx)h_2$ or equivalently $H = (x^{-1}hx)H$, which holds if and only if $x^{-1}hx \in H$ for all $h \in H$. Thus $xH = h(xH)$ for all $h \in H$ if and only if $x^{-1}hx = x^{-1}h(x^{-1})^{-1} \in H$ for all $h \in H$, or if and only if $x^{-1} \in N[H]$.

Lemma 36.6.

Lemma 36.6. Let H be a p-subgroup of a finite group G. Then $(N[H] : H) \equiv (G : H) (\text{mod } p)$.

Proof. First, recall that $(G : H)$ is the number of left cosets of H in G. Let L be the set of left cosets of H in G, and let H act on L by "left translation" so that $h(xH) = (hx)H$. Then L is an H-set since $(h_1 h_2)(xh) = (h_1(h_2 x))h$ for all $h_1, h_2, h \in H$ and for all $x \in G$ (by associativity, and so $(h_1 h_2)(xH) = h_1(h_2 xH))$. Also, by definition, $|L| = (G : H)$.

Now L_H is the set of left cosets that are fixed under action by all elements of H (by definition of the symbols "L_H"). Now $xH = h(xH)$ for all $h \in H^*$ if and only if $xh_1 = h(xh_2)$ for some $h_1, h_2 \in H$; that is $h_1 = (x^{-1}hx)h_2$ or equivalently $H = (x^{-1}hx)H$, which holds if and only if $x^{-1}hx \in H$ for all $h \in H$. Thus $xH = h(xH)$ for all $h \in H$ if and only if $x^{-1}hx = x^{-1}h(x^{-1})^{-1} \in H$ for all $h \in H$, or if and only if $x^{-1} \in N[H]$.

Lemma 36.6 (Continued).

Lemma 36.6. Let H be a p-subgroup of a finite group G. Then $(N[H] : H) \equiv (G : H) (\text{mod } p)$.

Proof (Continued). Now consider the cosets of H in $N[H]$; these are of the form xH such that $x \in N[H]$. So the cosets of H in $N[H]$ are exactly the same as the cosets of H in L_H. That is, $(N[H] : H) = |L_H|$.

Since H is a p-group, it has a power of p by Corollary 36.4. By Theorem 36.1 $|L| \equiv |L_H| (\text{mod } p)$, or in the symbols of the index, $(G : H) \equiv (N[H] : H) (\text{mod } p)$. □

Lemma 36.6 (Continued).

Lemma 36.6. Let H be a p-subgroup of a finite group G. Then $(N[H] : H) \equiv (G : H) \pmod{p}$.

Proof (Continued). Now consider the cosets of H in $N[H]$; these are of the form xH such that $x \in N[H]$. So the cosets of H in $N[H]$ are exactly the same as the cosets of H in L_H. That is, $(N[H] : H) = |L_H|$.

Since H is a p-group, it has a power of p by Corollary 36.4. By Theorem 36.1 $|L| \equiv |L_H| \pmod{p}$, or in the symbols of the index, $(G : H) \equiv (N[H] : H) \pmod{p}$. □

Corollary 36.7.

Corollary 36.7. Let H be a p-subgroup of a finite group G. If p divides $(G : H)$ then $N[H] \neq H$.

Proof. Since we hypothesize $(G : H) \equiv 0 (\text{mod } p)$, then by Lemma 36.6 we have $(N[H] : H) \equiv 0 (\text{mod } p)$. But since $(N[H] : H)$ is the number of left cosets of H in $N[H]$ then it is at least one (of course H itself is a left coset). But since p divides $(N[H] : H)$, then $(N[H] : H)$ is not 1. So $(N[H] : H) = |N[H]|/|H| > 1$ and $N[H] \neq H$. □

Theorem 36.8. First Sylow Theorem.

Theorem 36.8. First Sylow Theorem. Let G be a finite group and let $|G| = p^m$ where $n \geq 1$ and where p does not divide m. Then

(1) G contains a subgroup of order p^i for each i where $1 \leq i \leq n$, and

(2) every subgroup H of G of order p^i is a normal subgroups of a subgroup of order p^{i+1} for $1 \leq i < n$.

Proof. First, by Cauchy's Theorem (Theorem 36.3), G has a subgroup of order p. We now give an inductive proof of (1). We know G has a subgroup of order p^1. Suppose G has a subgroup of order p^i for $1 \leq i < n$, say subgroup H. Now $(G : H) = |G|/|H|$, $|G| = p^n m$ and $|H| = p^i$ for $i < n$. So p divides $(G : H)$. By Lemma 36.6, $(N[H] : H) \equiv (G : H) (\mathrm{mod}\ p)$ and so p divides $(N[H] : H)$.

Theorem 36.8. First Sylow Theorem.

Theorem 36.8. First Sylow Theorem. Let G be a finite group and let $|G| = p^m$ where $n \geq 1$ and where p does not divide m. Then

(1) G contains a subgroup of order p^i for each i where $1 \leq i \leq n$, and

(2) every subgroup H of G of order p^i is a normal subgroups of a subgroup of order p^{i+1} for $1 \leq i < n$.

Proof. First, by Cauchy's Theorem (Theorem 36.3), G has a subgroup of order p. We now give an inductive proof of (1). We know G has a subgroup of order p^1. Suppose G has a subgroup of order p^i for $1 \leq i < n$, say subgroup H. Now $(G : H) = |G|/|H|$, $|G| = p^n m$ and $|H| = p^i$ for $i < n$. So p divides $(G : H)$. By Lemma 36.6, $(N[H] : H) \equiv (G : H) (\text{mod } p)$ and so p divides $(N[H] : H)$.

Theorem 36.8. First Sylow Theorem (Continued).

Theorem 36.8. First Sylow Theorem (Continued).

Proof (Continued). By definition of $N[H]$, H is a normal subgroup of $N[H]$, so we can form $N[H]/H$, and we see that p divides $(N[H] : H) = |N[H]/H|$ (since $(N[H] : H)$ is the number of cosets of H in $N[H]$ and $N[H]/H$ is the quotient group of these cosets). So by Cauchy's Theorem (Theorem 36.3), group $N[H]/H$ has a subgroup K of order p. If $\gamma : N[H] \to N[H]/H$ is the canonical homomorphism ($\gamma(x) = x + H$), then by Theorem 13.12(4) $\gamma^{-1}[K] = \{x \in N[H] \mid \gamma(x) \in K\}$ is a subgroup of $N[H]$ and hence of G. Now the canonical homomorphism $\gamma(x) = x + H$ is "many to one" (for insight, see the diagram in the notes for Section 13; each colored rectangle contains all of the elements ???? to that coset). Now all cosets of H are the same size by Lemma from page 5 of the notes for Section 10 (see also the boxed comment on page 100); this size is $|H| = p^i$.

Theorem 36.8. First Sylow Theorem (Continued).

Theorem 36.8. First Sylow Theorem (Continued).
Proof (Continued). By definition of $N[H]$, H is a normal subgroup of $N[H]$, so we can form $N[H]/H$, and we see that p divides $(N[H] : H) = |N[H]/H|$ (since $(N[H] : H)$ is the number of cosets of H in $N[H]$ and $N[H]/H$ is the quotient group of these cosets). So by Cauchy's Theorem (Theorem 36.3), group $N[H]/H$ has a subgroup K of order p. If $\gamma : N[H] \to N[H]/H$ is the canonical homomorphism ($\gamma(x) = x + H$), then by Theorem 13.12(4) $\gamma^{-1}[K] = \{x \in N[H] \mid \gamma(x) \in K\}$ is a subgroup of $N[H]$ and hence of G. Now the canonical homomorphism $\gamma(x) = x + H$ is "many to one" (for insight, see the diagram in the notes for Section 13; each colored rectangle contains all of the elements ???? to that coset). Now all cosets of H are the same size by Lemma from page 5 of the notes for Section 10 (see also the boxed comment on page 100); this size is $|H| = p^i$.

Theorem 36.8. First Sylow Theorem (Continued).

Theorem 36.8. First Sylow Theorem (Continued).

Proof (Continued). So the canonical homomorphism is "p^i to one". Since $|K| = p$ then $\gamma^{-1}[K] = p^i p = p^{i+1}$. So G has a subgroup, namely $\gamma^{-1}[K]$ of order p^{i+1} and it follows by Mathematical Induction that G has a subgroup of order p^i for $1 \leq i \leq n$.

Second, we have from above that $H < \gamma^{-1}[K] \leq N[H]$ where $|\gamma^{-1}[H]| = p^{i+1}$. Since H is normal in $N[H]$ (notice by Definition 36.5 $N[H]$ is the largest subgroup of G having H as a normal subgroups), then trivially H is a normal subgroup of $\gamma^{-1}[K]$ (by Theorem 14.13(2), say). So $\gamma^{-1}[K]$ is the desired group in the claim. □

Theorem 36.8. First Sylow Theorem (Continued).

Theorem 36.8. First Sylow Theorem (Continued).
Proof (Continued). So the canonical homomorphism is "p^i to one". Since $|K| = p$ then $\gamma^{-1}[K] = p^i p = p^{i+1}$. So G has a subgroup, namely $\gamma^{-1}[K]$ of order p^{i+1} and it follows by Mathematical Induction that G has a subgroup of order p^i for $1 \leq i \leq n$.

Second, we have from above that $H < \gamma^{-1}[K] \leq N[H]$ where $|\gamma^{-1}[H]| = p^{i+1}$. Since H is normal in $N[H]$ (notice by Definition 36.5 $N[H]$ is the largest subgroup of G having H as a normal subgroups), then trivially H is a normal subgroup of $\gamma^{-1}[K]$ (by Theorem 14.13(2), say). So $\gamma^{-1}[K]$ is the desired group in the claim. □

Theorem 36.10. Second Sylow Theorem.

Theorem 36.10. Second Sylow Theorem. Let P_1 and P_2 be Sylow p-subgroups of a finite group G. Then P_1 and P_2 are conjugate subgroups of G. That is, for some $g \in G$, we have $P_2 = gP_1g^1$.

Proof. We will let one of the subgroups act on left cosets of the other. Let L be the set of left cosets of P_1 and let P_2 act on L by $y(xP_1) = (yx)P_1$ for $y \in P_2$. Then L is a P_2-set. By Theorem 36.1, the number of cosets fixed by all elements of P_2 satisfies $|L_{P_2}| \equiv |L| (\mathrm{mod}\ p)$, and $|L| = (G : P_1)$ (by definition of index). By the First Sylow Theorem and the note above, if $|G| = p^n m$ where $p \nmid m$ then $|P_1| = p^n$, and since all cosets of P_1 are of the same size (see the note on page 5 of the notes for Section 10 or the boxed comment on page 100), then there are m left cosets of P, and $|L| = (G : P) = m$.

Theorem 36.10. Second Sylow Theorem.

Theorem 36.10. Second Sylow Theorem. Let P_1 and P_2 be Sylow p-subgroups of a finite group G. Then P_1 and P_2 are conjugate subgroups of G. That is, for some $g \in G$, we have $P_2 = gP_1g^1$.

Proof. We will let one of the subgroups act on left cosets of the other. Let L be the set of left cosets of P_1 and let P_2 act on L by $y(xP_1) = (yx)P_1$ for $y \in P_2$. Then L is a P_2-set. By Theorem 36.1, the number of cosets fixed by all elements of P_2 satisfies $|L_{P_2}| \equiv |L| (\text{mod } p)$, and $|L| = (G : P_1)$ (by definition of index). By the First Sylow Theorem and the note above, if $|G| = p^n m$ where $p \nmid m$ then $|P_1| = p^n$, and since all cosets of P_1 are of the same size (see the note on page 5 of the notes for Section 10 or the boxed comment on page 100), then there are m left cosets of P, and $|L| = (G : P) = m$.

Theorem 36.10. Second Sylow Theorem (Continued).

Theorem 36.10. Second Sylow Theorem (Continued). Let P_1 and P_2 be Sylow p-subgroups of a finite group G. Then P_1 and P_2 are conjugate subgroups of G. That is, for some $g \in G$, we have $P_2 = gP_1g^1$.

Proof (Continued). So P does not divide $|L|$ and hence $|L_{P_2}| \neq 0$. Let $xP_1 \in L_{P_2}$. Then $yxP_1 = xP_1$ for all $y \in P_2$. So $x^{-1}yxP_1 = P_1$ for all $y \in P_2$. That is, $x^{-1}yx \in P_1$ for all $y \in P_2$, or $x^{-1}P_2x \subseteq P_1$ (in fact $x^{-1}P_2x$ is a subgroup of P_1; see page 141). Since $|P_1| = |P_2|$, then $x^{-1}P_2x = P_1$, or $P_2 = gP_1g^{-1}$ for $g = x^{-1}$, and P_1 and P_2 are conjugate subgroups of group G. □

Theorem 36.10. Second Sylow Theorem (Continued).

Theorem 36.10. Second Sylow Theorem (Continued). Let P_1 and P_2 be Sylow p-subgroups of a finite group G. Then P_1 and P_2 are conjugate subgroups of G. That is, for some $g \in G$, we have $P_2 = gP_1g^1$.

Proof (Continued). So P does not divide $|L|$ and hence $|L_{P_2}| \neq 0$. Let $xP_1 \in L_{P_2}$. Then $yxP_1 = xP_1$ for all $y \in P_2$. So $x^{-1}yxP_1 = P_1$ for all $y \in P_2$. That is, $x^{-1}yx \in P_1$ for all $y \in P_2$, or $x^{-1}P_2x \subseteq P_1$ (in fact $x^{-1}P_2x$ is a subgroup of P_1; see page 141). Since $|P_1| = |P_2|$, then $x^{-1}P_2x = P_1$, or $P_2 = gP_1g^{-1}$ for $g = x^{-1}$, and P_1 and P_2 are conjugate subgroups of group G. □