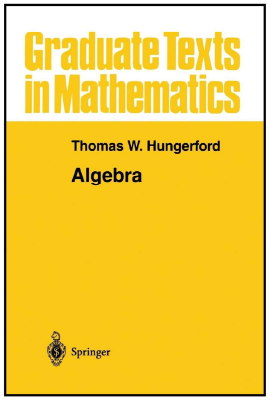
Modern Algebra

Chapter II. The Structure of Groups

II.5. The Sylow Theorems—Proofs of Theorems



Lemma II.5.1

Lemma II.5.1. Fraleigh, Theorem 36.1.
If a group H of order p^n (p prime) acts on a finite set S and if $S_0 = \{x \in S \mid h \star x = x \text{ for all } h \in H\}$ then $|S| \equiv |S_0| \pmod{p}$.

Proof. Recall that the orbit of $x \in S$ under action on S is $\overline{x} = \{h \star x \mid h \in H\}$. So an orbit contains exactly one element if and only if $x \in S_0$. Since the orbits represent equivalence classes, then they partition set S so $S = S_0 \cup \overline{x}_1 \cup \overline{x}_2 \cup \cdots \cup \overline{x}_m$ where $|\overline{x}_i| > 1$ for each i. Hence $|S| = |S_0| + |\overline{x}_1| + |\overline{x}_2| + \cdots + |\overline{x}_m|$. Now $|\overline{x}_i| \mid p^n$ by Corollary II.4.4(i) (since $|H| = p^n$) and so $p \mid |\overline{x}_i|$ for each i since $|\overline{x}_i| > 1$. Therefore $|S| \equiv |S_0| \pmod{p}$. □

Theorem II.5.2

Theorem II.5.2. Fraleigh, Theorem 36.3. Cauchy's Theorem.
If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.

Proof. Let S be the set of p-tuples of group elements with product e:

$$S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}.$$

Now with $|G| = n$, there are n choices for each of $a_1, a_2, \ldots, a_{p-1}$. But, since the product of the p elements must be e, then $a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$ and so there is only one choice for a_p. So $|S| = n^{p-1}$. Since $p \mid |G|$ (or in the notation, $p \mid n$) then $n \equiv 0 \pmod{p}$ and so $|S| \equiv 0 \pmod{p}$. Let the group $\mathbb{Z}_p$ act on set S as follows: for $k \in \mathbb{Z}_p$ let $k \star (a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, \ldots, a_k)$ (that is, the action by k is to cycle the p-tuple around k "slots").

Theorem II.5.2 (continued 1)

Proof (continued). In a group, if $ab = e$ then $ba = (a^{-1}a)(ba) = a^{-1}(ab)a = a^{-1}ea = e$. In G, since $\underbrace{(a_1 a_2 \cdots a_k)}_{a}\underbrace{(a_{k+1} a_{k+2} \cdots a_p)}_{b} = e$ then $a_{k+1} a_{k+2} \cdots a_p a_1 a_2 \cdots a_k = e$ and so $(a_{k+1}, a_{k+2}, \ldots, a_k) \in S$. Hence this action actually maps $G \times S \to S$ as required by the definition of group action. Next, for $e = 0 \in \mathbb{Z}_p$, we have for $x \in S$ that $0 \star x = x$, satisfying the first condition of group action (Definition II.4.1). Now for $k, k' \in \mathbb{Z}_p$ we have

$$(k + k') \star (a_1, a_2, \ldots, a_p) = (a_{1+k+k'}, a_{2+k+k'}, \ldots, a_p, a_1, \ldots, a_{k+k'})$$

$$= k \star (a_{1+k'}, a_{2+k'}, \ldots, a_p, a_1, \ldots, a_{k'}) = k \star (k' \star (a_1, a_2, \ldots, a_p))$$

(where the indices are reduced as appropriate). So the second condition of the definition of group action is also satisfied. Therefore this is actually an example of group action.

Theorem II.5.2 (continued 2)

Theorem II.5.2. Fraleigh, Theorem 36.3. Cauchy's Theorem.
If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.

Proof (continued). Now $S_0 = \{x \in S \mid k \star x = x \text{ for all } k \in \mathbb{Z}_p\}$ so $(a_1, a_2, \ldots, a_p) \in S_0$ if and only if $a_1 = a_2 = \cdots = a_p$. Next $(e, e, \ldots, e) \in S_0$ so $|S_0| \neq 0$. By Lemma II.5.1 $|S| \equiv |S_0| \pmod{p}$. By above, $|S| \equiv 0 \pmod{p}$, so $|S_0| \equiv 0 \pmod{p}$. Since $|S_0| \neq 0$ then S_0 must contain at least p elements. That is, there exists $a \neq e$ such that $(a, a, \ldots, a) \in S_0 \subseteq S$. By the definition of S, $aa \cdots a = a^p = e$. Since p is prime, it must be that the order of a is p. □

Corollary II.5.3

Corollary II.5.3. Fraleigh, Corollary 36.4.
A finite group G is a p-group if and only if $|G|$ is a power of p.

Proof. If G is a p-group and q is a prime which divides $|G|$, then G contains an element of order q by Cauchy's Theorem (Theorem II.5.2). Since every element of G has order a power of p (by definition of p-group), then $q = p$. So the only prime divisor of $|G|$ is p and $|G|$ is a power of prime p. Conversely, if $|G|$ is a power of prime p then by Lagrange's Theorem (Corollary I.4.6) every element of G is an order dividing this power of p and so every element is of order a power of prime p. □

Corollary II.5.4

Corollary II.5.4. The center $C(G)$ of a nontrivial finite p-group G contains more than one element.

Proof. Consider the class equation of G (see Note II.4.A):

$$|G| = |C(G)| + \sum [G : C_G(x_i)]$$

where $C_G(x)$ is the centralizer of x:

$$C_G(x) = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\}.$$

Since each $[G : C_G(x_i)] > 1$ (by convention, see Note II.4.A) and $[G : C_G(x_i)]$ divides $|G| = p^n$ ($n \geq 1$; by Corollary II.4.4(i)) then p divides each $[G : C_G(x_i)]$. Since G is a p-group by hypothesis, by Corollary II.5.3, $|G|$ is a power of p and so p divides $|G|$. So p must divide $|C(G)|$ from the class equation. Since $e \in C(G)$ then $|C(G)| \geq 1$ and so $|C(G)|$ has at least p elements (and hence more than one element). □

Lemma II.5.5

Lemma II.5.5. If H is a p-subgroup of a finite group G, then $[N_G(H) : H] \equiv [G : H] \pmod{p}$.

Proof. Recall that $N_G(H)$ is the normalizer of H:

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\} = \{g \in G \mid gH = Hg\}.$$

Let S be the set of left cosets of H in G and let H act on S by left translation. Then

$$|S| = [G : H]. \qquad (*)$$

Also by the definition of S_0, ($xH \in S_0$) if and only if ($hxH = xH$ for all $h \in H$) if and only if ($x^{-1}hxH = H$ for all $h \in H$) if and only if ($x^{-1}hx \in H$ for all $h \in H$) if and only if ($x^{-1}Hx = H$) if and only if ($xHx^{-1} = H$) if and only if ($x \in N_G(H)$). Therefore $|S_0|$ is the number of cosets xH with $x \in N_G(H)$.

Lemma II.5.5 (continued)

Lemma II.5.5. If H is a p-subgroup of a finite group G, then $[N_G(H) : H] \equiv [G : H] \pmod{p}$.

Proof (continued). Now $N_G(H)$ is a group (by Theorem II.4.2, where the group action is conjugation) and H is a subgroup of $N_G(H)$. So $[N_G(H) : H]$ is the number of left cosets of H in $N_G(H)$ and hence

$$|S_0| = [N_G(H) : H]. \qquad (**)$$

By Lemma II.5.1, $|S| \equiv |S_0| \pmod{p}$ and so by $(*)$ and $(**)$, $[N_G(H) : H] \equiv [G : H] \pmod{p}$. □

Corollary II.5.6

Corollary II.5.6. Fraleigh Corollary 36.7
If H is a p-subgroup of a finite group G such that p divides $[G : H]$, then $N_G(H) \neq H$.

Proof. Since p divides $[G : H]$ by hypothesis, then $[G : H] \equiv 0 \pmod{p}$. So from Lemma II.5.5, $[N_G(H) : H] \equiv 0 \pmod{p}$. Since $[N_G(H) : H] \geq 1$ ($eH = H$ is one coset of H) then we must have that $[N_G(H) : H]$ is at least p. So $[N_G(H) : H] > 1$ and $N_G(H) \neq H$ (if $N_G(H) = H$ then there is only one coset of H in $N_G(H)$). □

Theorem II.5.7

Theorem II.5.7. Fraleigh, Theorem 36.8. First Sylow Theorem.
Let G be a group of order $p^n m$ with $n \geq 1$, p prime, and $(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of G of order p^i $(i < n)$ is normal in some subgroup of order p^{i+1}.

Proof. Since $p \mid |G|$, G contains an element a (and therefore a subgroup $\langle a \rangle$) of order p by Cauchy's Theorem (Theorem II.5.2). Now perform induction on i and assume that G has a subgroup H of order p^i where $1 \leq i < n$ (so H is a p-subgroup of G by Corollary II.5.3) we now construct a group H_1 of order p^{i+1} where $H_1 < G$ and $H \triangleleft H_1$). Now $[G : H] = |G|/|H|$ by Lagrange's Theorem (Corollary I.4.6) and since $|H| \leq p^{n-1}$ then $p \mid [G : H]$. Next $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ so $H \triangleleft N_G(H)$ by Theorem I.5.1(v). By Corollary II.5.6, $N_G(H) \neq H$ and so $|N_G(H)/H| = [N_G(H) : H] > 1$. By Lemma II.5.5

$$1 < |N_G(H)/H| = [N_G(H) : H] \equiv [G : H] \equiv 0 \pmod{p}.$$

Theorem II.5.7

Proof (continued). Hence $p \mid |N_G(H)/H|$ and $N_G(H)/H$ contains an element bH (and a subgroup $\langle bH \rangle$) of order p by Cauchy's Theorem (Theorem II.5.2). By Corollary I.5.12, this group $\langle bH \rangle$ is of the form H_1/H where $H_1 < N_G(H)$ and $H < H_1$ (in the notation of Corollary I.5.12, $\langle bH \rangle < N_G(H)/H = G/N$ and $K = H_1$; so $K = H_1 < G$, $N = H < H_1 = K$ and $K/N = H_1/H$). Since H is normal in $N_G(H)$ and $H_1 < N_G(H)$ then H is normal in H_1. Finally,

$$\begin{aligned} |H_1| &= |H||H_1/H| \text{ by Lagrange's Theorem} \\ &= p^i p = p^{i+1}. \end{aligned}$$

So $H \triangleleft H_1$ and $|H_1| = p^{i+1}$ and the result follows by induction for all appropriate i. □

Corollary II.5.8

Corollary II.5.8. Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $(p, m) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of G if and only if $|H| = p^n$.

(ii) Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.

(iii) If there is only one Sylow p-subgroup P, then P is normal in G.

Proof. (i) H is a p-subgroup if and only if $|H|$ is some power of p by Corollary II.5.3. By the First Sylow Theorem (Theorem II.5.7), if $|H| = p^i$ for $0 \leq i < n$ then H is not a Sylow p-subgroup. The only possible Sylow p-subgroups are subgroups of order a power of p by Corollary II.5.3, so (by Lagrange's Theorem) if $|H| = p^n$ then H is a maximal p-subgroup and H is a Sylow p-subgroup; conversely, by the First Sylow Theorem, a Sylow p-subgroup must be of order p^n.

Corollary II.5.8 (continued)

Corollary II.5.8. Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $(p, m) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of G if and only if $|H| = p^n$.

(ii) Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.

(iii) If there is only one Sylow p-subgroup P, then P is normal in G.

Proof (continued). (ii) This follows from Exercise I.5.6 and part (i).

(iii) If there is only one Sylow p-subgroup P, then by (ii) gPg^{-1} is also a Sylow p-subgroup, so it must be that $gPg^{-1} = P$ for all $g \in G$. That is, by Theorem I.5.1 (and definition), P is normal in G. □

Theorem II.5.9

Theorem II.5.9. Fraleigh, Theorem 36.10. Second Sylow Theorem. If H is a p-subgroup of a finite group G, and P is any Sylow p-subgroup of G, then there exists $x \in G$ such that $H < xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Proof. Let S be the set of left cosets of P in G and let H act on S by left translation. Now $S_0 = \{xP \in S \mid h(xP) = xP \text{ for all } h \in H\}$ and $[G : P] = |S| \equiv |S_0| \pmod{p}$ by Lemma II.5.1. But $p \nmid [G : P]$ since $[G : P] = |G|/|P| = m$ (where $(m, p) = 1$). So $|S_0| \neq 0$ and there exists $xP \in S_0$. Now $(xP \in S_0)$ if and only if $(hxP = xP$ for all $x \in H$ (by the definition of S_0)) if and only if $(x^{-1}hxP = P$ for all $h \in H)$ if and only if $(x^{-1}Hx < P)$ if and only if $(H < xPx^{-1})$, giving the first claim.

If H is a Sylow p-subgroup, then $|H| = |P|$ by Corollary II.5.8(i). Also, $|P| = |xPx^{-1}|$ by Corollary II.5.8(ii), so $|H| = |xPx^{-1}|$ and it must be that $H = xPx^{-1}$ (since $H < xPx^{-1}$ by above) and so two Sylow p-subgroups P and H must be conjugates. □

Theorem II.5.10

Theorem II.5.10. Fraleigh, Theorem 36.11. Third Sylow Theorem. If G is a finite group and p a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \geq 0$.

Proof. By the Second Sylow Theorem (Theorem II.5.9) any two Sylow p-subgroups are conjugate, so if P is a Sylow p-subgroup then the number of conjugates of P is the number of Sylow p-subgroups. But by Corollary II.4.4(iii) the number of conjugates of P in G is $[G : N_G(P)]$ and this is a divisor of $|G|$.

Let S be the set of all Sylow p-subgroups of G and let P act on S by conjugation. Then $Q \in S_0 = \{Q \in S \mid xQx^{-1} = Q \text{ for all } x \in P\}$ if and only if $P < N_G(Q) = \{x \in G \mid xQx^{-1} = Q\}$. So both P and Q (not necessarily distinct) are Sylow p-subgroups of G and hence of $N_G(Q)$ (since $N_G(Q) < G$) and are therefore conjugate in $N_G(Q)$.

Theorem II.5.10 (continued)

Theorem II.5.10. Fraleigh, Theorem 36.11. Third Sylow Theorem. If G is a finite group and p a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \geq 0$.

Proof (continued). Since Q is normal in $N_G(Q)$ (by the definition of $N_G(Q)$, the normalizer of Q in G) then every conjugate of Q in $N_G(Q)$ equals Q and so $P = Q$. Therefore $S_0 = \{P\}$. By Lemma II.5.1, $|S| \equiv |S_0| \equiv 1 \pmod{p}$. Hence $|S| = kp + 1$ for some $k \geq 0$. □

Theorem II.5.11

Theorem II.5.11. If P is a Sylow p-subgroup of a finite group G, then $N_G(N_G(P)) = N_G(P)$.

Proof. Every conjugate of P is a Sylow p-subgroup of G by the Second Sylow Theorem (Theorem II.5.9). Every conjugate of P is a Sylow p-subgroup of any subgroup of G that contains it by Corollary II.5.8(ii). Since P is normal in $N = N_G(P) = \{x \in G \mid xPx^{-1} = P\}$, then P is the only Sylow p-subgroup of N by the Second Sylow Theorem (Theorem II.5.9; all Sylow p-subgroups of N must be conjugates, but any conjugate of P in N equals P). Therefore, $x \in N_G(N_G(P)) = N_G(N)$ if and only if $xNx^{-1} = N$ by the definition of normalizer and this implies that $xPx^{-1} < N$ since $P < N$, and so xPx^{-1} is a Sylow p-subgroup of N by Corollary II.5.8(ii). Since P is the only Sylow p-subgroup of N then $P = xPx^{-1}$ and so $x \in N_G(P) = N$. Therefore $N_G(N_G(P)) \subseteq N_G(P)$.

Theorem II.5.11 (continued)

Theorem II.5.11. If P is a Sylow p-subgroup of a finite group G, then $N_G(N_G(P)) = N_G(P)$.

Proof (continued). Now "clearly" the normalizers of any subgroup of G contains all the elements of that subgroup and so $x \in N_G(P)$ implies $x \in N_G(N_G(P))$ and $N_G(P) \subseteq N_G(N_G(p))$.

Hence $N_G(N_G(P)) = N_G(P)$. □