5 Sylow Theory

Let G be a finite group of order n. If $H \leq G$ then $|H|$ divides n. The converse is not true in that $SL(2,3)$ has order 24 but has no subgroup of order 12. Here is a partial converse.

Theorem 5.1 (Sylow 1872) *Let $|G| = p^m r$ where p is a prime and r is not divisible by p. Then G has a subgroup of order p^m.*

Proof Let $\boldsymbol{S}$ denote the set of all subsets $\mathcal{U}$ of G with $|\mathcal{U}| = p^m$. The number of such subsets is $|\boldsymbol{S}| = \binom{p^m r}{p^m}$ which is *not* divisible by p (check!). For $\mathcal{U} \in \boldsymbol{S}$ and $g \in G$, $\mathcal{U}g = \{ug \colon u \in \mathcal{U}\}$ is also in $\boldsymbol{S}$ and so G acts on the set $\boldsymbol{S}$ by multiplication on the right. By this action $\boldsymbol{S}$ is partitioned into orbits and since p does not divide $|\boldsymbol{S}|$ it follows that for some orbit $\boldsymbol{T}$, p does not divide $|\boldsymbol{T}|$. Let $V \in \boldsymbol{T}$ so that $V = \{x_1, \ldots, x_{p^m}\}$ and let $H = \mathsf{Stab}_G(V) \leq G$. Then the orbit-stabilizer theorem tells us that $|\boldsymbol{T}| = |G : H|$. Since $|G : H||H| = |G| = p^m r$ it follows that p^m divides $|\boldsymbol{T}||H|$ which implies that p^m divides $|H|$ since p does not divide $|\boldsymbol{T}|$. Observe now that for any $h \in H$, $Vh = \{x_1 h, \ldots, x_{p^m} h\} = V$ and so $x_1 h = x_i$ for some i where $1 \leq i \leq p^m$. It follows that $h = x_1^{-1} x_i$ and so $|H| \leq p^m$ and result. $\square$

Let p be a prime number. A group G is called a *p-group* if every element of G has order p^n for some n. So if $|G| = p^m$ for example then G is a finite p-group. The group H in the above is called a *p-subgroup* of G.

Corollary 5.2 (Cauchy 1844) (i) *If G is a finite group such that prime p divides $|G|$ then G contains an element of order p. (ii) The order of a finite p-group G is a power of p.*

Proof (i) Since p divides $|G|$ we know that G has a p-subgroup H by Theorem 5.1 and $H \neq \{e\}$. Choose $x \in H$ with $x \neq e$. Then $|x|$ divides $|H|$ and so $|x| = p^s$ for some $s \geq 1$. Put $k = p^{s-1}$. Then x^k is an element of G of order p.

(ii) If the prime q divides $|G|$ then G has an element of order q by (i). Since every element of G has order p^n it follows that $q = p$ and so $|G|$ is a power of p. $\square$

A p-subgroup P of a finite group G is called a *Sylow p-subgroup* of G if P is not properly contained in any p-subgroup of G. By Theorem 5.1 and Corollary 5.2(ii) every finite group has at least one Sylow p-subgroup for each prime p dividing $|G|$.

Theorem 5.3 *Every p-subgroup of a finite group G is contained in a Sylow p-subgroup.*

Proof Let P_1 be a p-subgroup of G. If P_1 is not a Sylow p-subgroup then there is a p-subgroup P_2 of G such that $P_1 < P_2$ (proper). Repeat to get a chain $P_1 < P_2 < \ldots$ which must terminate at a Sylow p-subgroup since $|G| < \infty$. $\square$

Theorem 5.4 *Let H be a finite p-group of order p^m. Then H has normal subgroups H_j $(0 \leq j \leq m)$ such that $\{e\} = H_0 < H_1 < \cdots < H_m = H$ and $|H_i| = p^j$ $(0 \leq j \leq m)$.*

Proof We proceed by induction on m. The assertion is clearly true if $m = 1$ so suppose $m > 1$ and the result is true for $m - 1$. Since $Z(H) \neq \{e\}$ we have $e \neq z \in Z(H)$. Then $|z| = p^n$ for some $n \geq 1$. Let $H_1 = \langle z^{p^{n-1}} \rangle$. Then H_1 is a subgroup of $Z(H)$ of order p. Since $H_1 \leq Z(H)$ it follows that $H_1 \trianglelefteq H$ so put $\bar{H} = H/H_1$. Then $|\bar{H}| = p^{m-1}$ and by induction $\bar{H}$ has normal subgroups $\bar{H}_i$ $(0 \leq i \leq m-1)$ with $\{e\} = \bar{H}_0 < \bar{H}_1 < \cdots < \bar{H}_{m-1} = \bar{H}$ and $|\bar{H}| = p^i$ for $0 \leq i \leq m-1$. By the correspondence theorem each $\bar{H}_i$ is of the form H_{i+1}/H_1

where $H_1 \trianglelefteq H_{i+1} \trianglelefteq H$. Moreover $H_1 < H_2 < \cdots < H_{m-1} < H_m = H$ and $|H_{i+1}| = |H_1||\bar{H}_i| = p^{i+1}$ for each i. The result now follows. $\Box$

The above result together with Theorem 5.1 immediately yields the following.

Corollary 5.5 *Let G be a finite group and let p^l be any prime power divisor of G. Then G has a subgroup of order p^l.*

Let $H \leq G$ and $K \leq G$. We say that H *normalizes* K or that K *is normalized* by H if $H \leq N_G(K)$ that is $h^{-1}kh \in K$ ($\forall h \in H$, $\forall k \in K$).

Theorem 5.6 *Let G be a finite group and let P be a Sylow p-subgroup of G. Then the following hold.*

(1) *($\forall x \in G$) P^x is a Sylow p-subgroup of G.*

(2) *$P \trianglelefteq G$ if and only if P is the only Sylow p-subgroup of G.*

(3) *If P^* is a Sylow p-subgroup of G (not necessarily distinct from P) then the number of conjugates of P not normalized by P^* is divisible by p.*

Proof (1) Suppose P^x is not a Sylow p-subgroup. Then $P^x < \hat{P}$ where $\hat{P}$ is a Sylow p-subgroup. But then $P = (P^x)^{x^{-1}} < (\hat{P})^{x^{-1}}$ which is a p-subgroup of G, a contradiction.

(2) Suppose that $P \trianglelefteq G$ and that $\hat{P}$ is *any* Sylow p-subgroup. Then $P\hat{P}$ is a p-subgroup of G that contains P and $\hat{P}$ whence $P = P\hat{P} = \hat{P}$ and result.

Conversely if P is the only Sylow p-subgroup then $P^x = P$ ($\forall x \in G$) by (1) and so $P \trianglelefteq G$.

(3) Let $\bar{P}_1$ be a conjugate of P not normalized by P^*, that is, such that $P^* \not\leq N_G(\bar{P}_1)$. Observe that if $x \in P^*$ then $\bar{P}_1^x$ is a conjugate of $\bar{P}_1$ and $P^* \not\leq N_G(\bar{P}_1^x)$ for otherwise we would have that for all $g \in P^*$, $(\bar{P}_1^x)^g = \bar{P}_1^x \Rightarrow xgx^{-1} \in N_G(\bar{P}_1) \Rightarrow N_G(\bar{P}_1)$ contains $\{xgx^{-1} \colon g \in P^*\} = P^*$, a contradiction.

Now observe that

$$
\begin{aligned}
|\{\bar{P}_1^x \colon x \in P^*\}| &= |\text{set of conjugates of } \bar{P}_1 \text{ by elements of } P^*| \\
&= |\text{set of cosets of } N_{P^*}(\bar{P}_1) \text{ in } P^*| \text{ (exercise)} \\
&= |P^* \colon N_{P^*}(\bar{P}_1)| \\
&= |P^* \colon P^* \cap N_G(\bar{P}_1)|
\end{aligned}
$$

which divides $|P^*|$ and so equals p^{α_1} for some $\alpha_1 \geq 0$. Moreover $\alpha_1 \neq 0$ since $P^* \not\leq N_G(\bar{P}_1)$.

Now let $\bar{P}_2$ be another conjugate of P not normalized by P^* such that $\bar{P}_2 \notin \{\bar{P}_1^x \colon x \in P^*\}$. Then $(\bar{P}_2)^x \notin \{\bar{P}_1^x \colon x \in P^*\}$ for any $x \in P^*$. So we get a set $\{\bar{P}_2^x \colon x \in P^*\}$ disjoint from $\{\bar{P}_1^x \colon x \in P^*\}$ all of whose members are not normalized by P^* and $|\{\bar{P}_2^x \colon x \in P^*\}| = p^{\alpha_2}$ where $\alpha_2 > 0$.

Continuing in this way we see that the set of all conjugates of P not normalized by P^* will have cardinality $p^{\alpha_1} + p^{\alpha_2} + \cdots + p^{\alpha_k}$ where $\alpha_j > 0$ $(1 \leq j \leq k)$ and this is divisible by p. $\square$

Theorem 5.7 *Let G be a finite group and let P be a Sylow p-subgroup of G. Then the following hold.*

(1) *Every Sylow p-subgroup is conjugate to P.*

(2) *If $|G| = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ where p_j are distinct primes and $\alpha_j > 0$ $(1 \leq j \leq m)$ then $|P| = p^{\alpha_i}$ for some i.*

(3) *G has $1+kp$ Sylow p-subgroups.*

(4) *If G has n_p Sylow p-subgroups then $n_p \equiv 1 \pmod p$.*

(5) *If G has n_p Sylow p-subgroups then $n_p = |G : N_G(P)|$ and in particular n_p divides $|G|$.*

(6) *If $|G| = p^m r$ where p does not divide r and G has n_p Sylow p-subgroups then n_p divides r.*

Proof Before proving (1)–(6) we first show that P has a total of $1+kp$ conjugates for some $k \geq 0$. Now by 5.6(3) there are kp conjugates of P not normalized by P. So it is enough to show that there is exactly one conjugate of P, namely P itself, that *is* normalized by P. To prove this let P^x be a conjugate of P. Then P^x is a Sylow p-subgroup of G by 5.6(1). Since $P^x \trianglelefteq N_G(P^x)$ it follows from 5.6(2) that P^x is the only Sylow p-subgroup of $N_G(P^*)$. But if P normalizes P^x then $P \leq N_G(P^x)$ and so P is another Sylow p-subgroup of P^x forcing $P = P^x$ as required.

(1), (3) Since P has $1+kp$ conjugates and since by 5.6(i) every conjugate of P is a Sylow p-subgroup to prove (1) and (3) we need to prove that if P^* is a Sylow p-subgroup of G then P^* is conjugate to P. But by 5.6(3) there are $\hat{k}p$ of the $1+kp$ conjugates of P not normalised by P^*. Since $\hat{k}p \neq 1+kp$ there is a P^g with $P^* \leq N_G(P^g)$. But $P^g \trianglelefteq N_G(P^g)$ and so P^g is the only Sylow p-subgroup of $N_G(P^g)$. Therefore $P^* = P^g$ as required.

(2), (4) These are immediate consequences of (1) and (3).

(5) It follows from the above that

$$
\begin{aligned}
n_p &= |\text{Sylow } p\text{-subgroups of } G| \\
&= |\text{conjugates of } P \text{ in } G| \\
&= |G : N_G(P)|.
\end{aligned}
$$

(6) If $|G| = p^m r$ where p does not divide r then

$r = |G : P| = |G : N_G(P)||N_G(P) : P| = n_p|N_G(P) : P| \Rightarrow n_p$ divides r. □

Note

$|G| = p^m r$ where p does not divide r.

$n_p :=$ number of Sylow p-subgroups of G.

$\boxed{n_p \equiv 1 \pmod{p}}$ and $\boxed{n_p \text{ divides } r}$

Example Let $G = SL(2, p)$. Then $|G| = p(p+1)(p-1)$.

Consider $P = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} : a \in \mathbb{F}_p \right\}$

and $P^* = \left\{ \begin{bmatrix} 1 & 0 \\ b & 1 \end{bmatrix} : b \in \mathbb{F}_p \right\}$.

Since $|P| = |P^*| = p$ it follows that they are conjugate Sylow p-subgroups of G (since p does not divide $(p+1)(p-1)$). In fact $P^\alpha = P^*$ where $\alpha = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$.

We now turn to finite non-Abelian simple groups and apply Sylow theory. Our aim is to find all the non-Abelian simple groups of order ≤ 100.

Lemma 5.8 *Let G be a finite non-Abelian simple group and let p be a prime divisor of $|G|$. Then $n_p > 1$.*

Proof Let P be a Sylow p-subgroup of G. By Corollary 4.12 $|G|$ is divisible by at least two primes and so $\{e\} < P < G$. If P is the only Sylow p-subgroup then $P \trianglelefteq G$, a contradiction. $\square$

Theorem 5.9 *If $|G| = pq$ where p, q are distinct primes such that $q \not\equiv 1$ (mod p) then G has a normal Sylow p-subgroup.*

Proof We know that $n_p \equiv 1$ (mod p) and that n_p divides q. Since q is prime either $n_p = 1$ or $n_p = q$. But $q \not\equiv 1$ (mod p) so $n_p = 1$ and G has a normal Sylow p-subgroup. $\square$

Corollary 5.10 *If $|G| = pq$ where p, q are distinct primes then G is not simple.*

Proof We can assume that $1 < q < p$. Then p does not divide $q - 1$ so $q \not\equiv 1$ (mod p) whence result by 5.9. $\square$

Corollary 5.11 *If p and q are distinct primes such that $p \not\equiv 1$ (mod q) and $q \not\equiv 1$ (mod p) then every group of order pq is cyclic.*

Proof Let $|G| = pq$. By 5.9 G has a normal Sylow p-subgroup P and a normal Sylow q-subgroup Q. Since P and Q have prime orders they are cyclic, say, $P = \langle x \rangle$ and $Q = \langle y \rangle$ where $x^p = y^q = e$. Now $x^{-1}y^{-1}xy = x^{-1}(y^{-1}xy) \in P$ and $x^{-1}y^{-1}xy = (x^{-1}y^{-1}x)y \in Q$ therefore $x^{-1}y^{-1}xy \in P \cap Q = \{e\} \Rightarrow xy = yx \Rightarrow |xy| = pq \Rightarrow G = \langle xy \rangle$ is cyclic. $\square$

Example There is precisely one group of order 15 and of order 33 namely C_{15} and C_{33}.

Theorem 5.12 *If $|G| = p^2q$ where p, q are distinct primes then G has either a normal Sylow p-subgroup or a normal Sylow q-subgroup; and so G is not simple.*

Proof Let n_p, n_q denote the number of Sylow p-subgroups, Sylow q-subgroups (respectively) of G. Suppose by way of contradiction that $n_p > 1$ and $n_q > 1$. Now n_p divides q and so $n_p = q$. Also $n_p \equiv 1 \pmod p$ and so $q \equiv 1 \pmod p$ whence $q > p$.

On the other hand n_q divides p^2 so that $n_q = p$ or $n_q = p^2$. Now any element of order q in G generates a subgroup of order q and any two distinct such subgroups intersect in the identity. Whence there are $n_q(q-1)$ distinct elements of order q. So if $n_q = p^2$ then there are in G precisely $p^2q - p^2(q-1) = p^2$ elements *not* of order q. But then, since no element of a Sylow p-subgroup P has order q and since $|P| = p^2$ it follows that P is unique, therefore normal, a contradiction. So $n_q = p$. But $n_q \equiv 1 \pmod q$ which implies $p > q$, our final contradiction. □

Theorem 5.13 *If $|G| = pqr$ where p, q and r are distinct primes then G is not simple.*

Proof We may assume that $p > q > r$. Suppose by way of contradiction that G is simple. Let n_p, n_q, n_r denote the number of Sylow p, q, r-subgroups (respectively). Then $n_p > 1$, $n_q > 1$ and $n_r > 1$. As in the proof of 5.12 the n_p Sylow p-subgroups contain $n_p(p-1)$ distinct elements of order p; and similarly for n_q and n_r. Therefore

$$|G| = pqr \geq 1 + n_p(p-1) + n_q(q-1) + n_r(r-1).$$

Now n_p divides qr and $n_p \equiv 1 \pmod p$. Since $n_p > 1$ and $p > q$ and $p > r$ it follows that $n_p = qr$. Also n_q divides pr and $n_q \equiv 1 \pmod q$. Since $n_q > 1$ and $q > r$ it follows that $n_q \geq p$. Finally $n_r > 1$ and n_r divides pq so that $n_r \geq q$. Now we have $pqr \geq 1 + qr(p-1) + p(q-1) + q(r-1) \Rightarrow 0 \geq (p-1)(q-1)$ which is false, a contradiction. □

Lemma 5.14 *If $n < 5$ then S_n has no non-Abelian simple subgroups.*

Proof Easy if $n < 4$. We know S_4 is not simple since $1 \neq A_4 \trianglelefteq S_4$. Let H be a non-Abelian simple subgroup of S_4. Since $|S_4| = 2^3.3$ it follows that $|H|$ must be divisible by both 2 and 3 (H is not a p-group). Hence $|H| = 6$ or 12. But $6 = 2.3$ is ruled out by 5.10; and $12 = 2^2.3$ is ruled out by 5.12. □

Corollary 5.15 *If G is a finite non-Abelian simple group and $H < G$ then $|G : H| \geq 5$.*

Proof If $|G : H| = n$ then G/H_G can be embedded in S_n by 4.7. Since $H_G \leq H < G$ and G is simple, this forces $H_G = 1$ and G embeds in S_n, hence $n \geq 5$ by 5.14. □

Lemma 5.16 *Suppose that $|G| = 2r$ where $r > 1$ is odd. Then G is not a simple group.*

Proof Using Sylow we see that G has an element of order 2, t say. Now G embeds in S_{2r} by Cayley's theorem and, identifying G with its image, $|G : A_{2r} \cap G| = |G\,A_{2r} : A_{2r}| = 1$ or 2. But t is a product of r transpositions. To see this observe that the corresponding action is multiplication on the right and so

$$g_1 t = g_2 \Rightarrow g_1 \neq g_2 \quad \text{and} \quad g_2 t = g_1 t^2 = g_1$$

so t 'pairs off' the elements of G. Therefore $G \not\subseteq A_{2r} \Rightarrow G\,A_{2r} = S_{2r} \Rightarrow A_{2r} \cap G$ is a subgroup of index 2 (and so of order $r > 1$) in G. Since subgroups of index 2 are normal the result follows. □

Lemma 5.17 *(i) If G is a finite non-Abelian simple group of order $p^m r$ where p does not divide r then n_p, the number of Sylow p-subgroups of G, is greater than 4. (ii) If $|G| = 2^3.q^m$ where $m \geq 1$ and q is prime and G is a non-Abelian simple group then $q = 7$.*

Proof (i) Since n_p is the index of a normalizer and $n_p \neq 1$ the result follows from 5.15.

(ii) Since $n_q > 4$ and $n_q \mid 8$ we get $n_q = 8$. But $n_q \equiv 1 \pmod{q} \Rightarrow 8 \equiv 1 \pmod{q} \Rightarrow q = 7$. $\square$

Lemma 5.18 *Let $n = p^m r$ where $m \geq 1$, $r > 1$ and p does not divide r. If there is a simple group G of order n then p^m divides $(r-1)!$; in particular there are no simple groups of order $2^m.5$ for any $m \geq 4$.*

Proof Let H be a Sylow p-subgroup of G. Then G/H_G embeds in $S_{|G:H|} = S_r$. But $H_G = 1$ and so $|G|$ divides $|S_r| \Rightarrow p^m \mid (r-1)!$. $\square$

Lemma 5.19 If $|G| = 56$ or 84 then G is *not* simple.

Proof Exercise.

Theorem 5.20 *Let n be a positive integer such that $n \leq 100$ and $n \neq 60$. Then there is no non-Abelian simple group of order n.*

Proof Let G be a non-Abelian simple group of order n. Then $n > 1$ and

$$n = \prod_{i=1}^{s} p_i^{m_i}$$

where $s, m_1, \ldots, m_s$ are positive integers and $p_1, \ldots, p_s$ are distinct primes. We may assume that $p_1 < p_2 < \cdots < p_s$.

Now G is not a p-group so $s > 1$.

If $s \geq 4$ then $n \geq 2.3.5.7 > 100$, a contradiction, so $s = 2$ or 3. By 5.10, 5.12 and 5.13 $\sum_{i=1}^{s} m_i > 3$.

If $\sum_{i=1}^{s} m_i \geq 7$ then $n > 2^7 > 100$, a contradiction. Hence

$$4 \leq \sum_{i=1}^{s} m_i \leq 6.$$

Suppose first that $s = 2$. If p_1 and p_2 are both odd then $n \geq 3^3.5 > 100$ so it can be assumed that

$$n = 2^l p^m$$

where $4 \leq l + m \leq 6$ and p is an odd prime.

If $1 \leq l \leq 2$ then a Sylow p-subgroup of G would have index at most 4, contradicting 5.15. Hence

$$3 \leq l \leq 5 \quad \text{and} \quad 1 \leq m \leq 3.$$

Let the number of Sylow p-subgroups of G be n_p. Then $n_p > 4$ by 5.17(i). We also know that n_p divides 2^l whence n_p divides 2^5. Now $n_p \neq 32$ for then $p = 31$ (since $n_p \equiv 1 \pmod{p}$) and $n \geq 2^3.31 > 100$. This leaves

$$n_p = 8 \quad \text{and} \quad p = 7$$

$$\text{or} \quad n_p = 16 \quad \text{and} \quad p = 3$$

$$\text{or} \quad n_p = 16 \quad \text{and} \quad p = 5.$$

If $n_p = 8$ and $p = 7$ then $|G| < 100$ implies $|G| = 2^3.7 = 56$ which is ruled out by 5.19.

If $n_p = 16$ then n_p divides $2^l \Rightarrow l \geq 4$. Then $m = 1$ since $2^4.3^2 > 100$. Thus if $n_p = 16$ and $p = 3$ then a Sylow 2-subgroup of G has index 3 in G contradicting 5.15; and if $n_p = 16$ and $p = 5$ then $|G| = 80 = 2^4.5$ contradicting 5.18.

Now let $s = 3$. Then

$$\sum m_i \geq 4 \quad \Rightarrow \quad \text{either } n = 2^2.3.7 = 84$$
$$\text{or} \qquad n = 2.3^2.5 = 90.$$

But $|G| = 84$ is ruled out by 5.19 and $|G| = 90 = 2.45$ is not allowed by 5.16. $\square$

SCRATCH CARD

Theorem 5.21 *If $|G| = 60$ and G is a non-Abelian simple group then $G \cong A_5$.*

Proof Since $|G| = 60 = 2^2.3.5$ it follows that G has n_p Sylow p-subgroups for $p \in \{2, 3, 5\}$. Since n_5 divides $12 = 2^2.3$ and $n_5 \equiv 1$ (mod 5) we have $n_5 = 1$ or $n_5 = 6$. But $n_5 = 1$ is ruled out since G would then have a normal Sylow 5-subgroup. So G contains $6(5 - 1) = 24$ elements of order 5.

Since $n_3 \equiv 1$ (mod 3) and n_3 divides $20 = 2^2.5$ it follows that $n_3 = 4$ or $n_3 = 10$. But $n_3 = 4$ implies that G has a subgroup of index 4 which contradicts 5.17 and so G contains $10(3 - 1) = 20$ elements of order 3.

Finally $n_2 \equiv 1$ (mod 2) and n_2 divides 15 forces $n_2 \in \{1, 3, 5, 15\}$ and as before $n_2 = 1$ or 3 is ruled out.

Suppose first that $n_2 = 5$. Then G must contain a Sylow 2-subgroup H with $|G : N_G(H)| = 5$. Therefore G is isomorphic to a subgroup $\hat{G}$ of S_5 (via action on the cosets). But $|\hat{G}| = |G| = 60$ so that $|S_5 : \hat{G}| = 2 \Rightarrow S_5/\hat{G}$ is Abelian $\Rightarrow [S_5, S_5] \leq \hat{G}$. But $[S_5, S_5] = A_5$ (exercise) and so $G \cong A_5$.

Finally suppose that $n_2 = 15$. Let $e \neq x \in P$ where P is a Sylow 2-subgroup of G. Then since $|P| = 4$ we see that $P \leq C_G(x)$ and so $|G : C_G(x)|$ divides $|G : P| = 15 = 3.5$. Therefore $|G : C_G(x)| \in \{1, 3, 5, 15\}$. But $G = C_G(x) \Rightarrow \langle x \rangle \trianglelefteq G$ a contradiction; and G contains no subgroup of index 3 by 5.17. Also if $|G : C_G(x)| = 5$ then $G \cong A_5$ as in the previous case (same argument!). This leaves $|G : C_G(x)| = 15$ for *any* choice of x and P. This implies that $C_G(x) = P$ since both have order 4. It follows that if P_1 is another Sylow 2-subgroup of G then $P \cap P_1 = \{e\}$ for otherwise if $e \neq y \in P \cap P_1$ then $C_G(y)$ would contain both P and P_1 and would be of order greater than 4 therefore index less than 15, a contradiction. But this means that there would be $15(4 - 1) = 45$ elements of G of order 2 or 4 contradicting the fact that there are only $60 - (20 + 24) = 16$ elements of G not of order 3 or 5. □

Remarks

1. **Feit–Thompson Theorem (1963) (249 pages)** *If G is a non-Abelian finite simple group then G has even order.*

2. $|G| = p_1 \ldots p_k$ (distinct primes and $k > 1$) $\Rightarrow G$ not simple.