The Sylow Theorems and Applications

Penelope Drastik

May 28, 2018

Introduction

The Sylow Theorems are important results in group theory which count the number of subgroups of a certain order of a finite group, and identify various properties of such subgroups. We shall state and prove the three Sylow Theorems, expanding on the proofs given in [1], and explore some applications of these results based on [1] and [2].

Group Actions

Definition 1. Let G be a group and X be a set. A **group action** of G on X is a function $\phi : G \times X \to X$ such that $\phi(e, x) = x$ for all $x \in X$ and $\phi(g, \phi(h, x)) = \phi(gh, x)$ for all $g, h \in G, x \in X$. To simplify the notation, we often write $g \cdot x$ to mean $\phi(g, x)$.

Definition 2. Let G be a group acting on a set X. The **orbit** of an element $x \in X$ is the set

$$Gx = \{y \in X : y = g \cdot x \quad \text{for some} \quad g \in G\}$$

The **stabiliser** of an element $x \in X$ is the set

$$Stab(x) = \{g \in G : g \cdot x = x\}$$

The following theorem, a consequence of Lagrange's Theorem, is an important result concerning group actions.

Theorem 1. *(Orbit Stabiliser Theorem) Let G be a group which acts on a finite set X. Then*

$$|Gx| = \frac{|G|}{|Stab(x)|}$$

The Counting Theorem

The following theorem will be used in the proofs of the Sylow Theorems by choosing appropriate sets and group actions. It is called the "Counting Theorem" since it counts modulo p.

Theorem 2 (The Counting Theorem)**.** *Let G be a group of order p^n, where p is prime, and let X be a finite G-set. We define*

$$X_G = \{x \in X : gx = x \quad \forall g \in G\}$$

That is, X_G is the union of all of the one element orbits. Then

$$|X| \equiv |X_G| \mod p$$

Proof. The orbit of $x \in X$ is given by $Gx = \{gx : g \in G\}$. Suppose that there are r orbits in X under the action of G. We construct the set $\{x_1, \ldots, x_r\}$ which contains precisely one element from each orbit. Now, every element of X is in precisely one orbit, so we have

$$|X| = \sum_{i=1}^{r} |Gx_i|$$

However, some orbits may contain only one element.

Suppose that there are s one element orbits, where $0 \leq s \leq r$. Then we have $|X_G| = s$ and, by reordering the x_i if necessary, we have

$$|X| = |X_G| + \sum_{i=s+1}^{r} |Gx_i|$$

Now, by the Orbit-Stabiliser theorem, we know that $|Gx_i|$ divides $|G|$. So we have $|Gx_i| = p^k$ for some $k \in \{1, \ldots, n\}$. (Note that $|Gx_i| \neq 1$ since we have already taken out all the one element orbits with X_G).

So $p \big| |Gx_i|$ for $s+1 \leq i \leq r$.

Hence

$$|X| - |X_G| = \sum_{i=s+1}^{r} |Gx_i| = pB$$

for some $B \in \mathbb{N}$.

We conclude that $|X| - |X_G|$ is divisible by p, and therefore $|X| \equiv |X_G| \mod p$.

□

Cauchy's Theorem

Theorem 3. *Let p be a prime. Let G be a finite group with $p \big| |G|$. Then G has an element of order p and therefore has a subgroup of order p.*

Proof. We define

$$X = \{(g_1, \ldots, g_p) : g_i \in G \quad \text{and} \quad g_1 \cdots g_p = e\}$$

Claim: p divides $|X|$.

Proof of Claim: In forming a p-tuple, let $g_1, \ldots, g_{p-1}$ be any elements of G, and then set $g_p = (g_1 \ldots g_{p-1})^{-1}$. So we have $|X| = |G|^{p-1}$, since $p-1$ elements are chosen freely from G and the other is uniquely determined. Since p divides $|G|$, and therefore divides $|G|^{p-1}$, we conclude that p divides $|X|$.

Returning to the proof of Cauchy's theorem, let σ be the cycle $(123 \cdots p)$ in S_p, the symmetric group with p elements. We let σ act on X by

$$\sigma(g_1, \ldots, g_p) = (g_{\sigma(1)}, \ldots, g_{\sigma(p)}) = (g_2, g_3, \ldots, g_p, g_1)$$

Note that the resulting p-tuple $(g_2, g_3, \ldots, g_p, g_1) \in X$ since if $(g_1, \ldots, g_p) \in X$ then $g_1(g_2 \ldots g_p) = e$. Hence $g_1 = (g_2 \ldots g_p)^{-1}$ and therefore $(g_2 g_3 \cdots g_p) g_1 = e$.

So σ acts on X, and so does $\langle \sigma \rangle$, the subgroup generated by σ, via iteration (or repeated composition). We have $|\langle \sigma \rangle| = p$, since σ is a cycle with p elements, and so we can apply the Counting Theorem to the group $\langle \sigma \rangle$. Thus $|X| \equiv |X_{\langle \sigma \rangle}| \mod p$. Also, since $p \big| |X|$ we have $p \big| |X_{\langle \sigma \rangle}|$.

Now, the p-tuple $(g_1, \ldots, g_p)$ is left fixed by σ (or, equivalently, by $\langle \sigma \rangle$ since its elements are simply iterations of σ) if and only if $g_1 = \cdots = g_p$.

We know that $X_{\langle \sigma \rangle}$ is nonempty since it contains the p-tuple $(e, \ldots, e)$. Since p divides $|X_{\langle \sigma \rangle}|$, there must be at least p elements in $X_{\langle \sigma \rangle}$. So there exists an element $a \in G$ with $a \neq e$ such that $(a, \ldots, a) \in X_{\langle \sigma \rangle}$, and therefore $a^p = e$.

So the element a has order p, and $\langle a \rangle$, the subgroup generated by a, has order p.

□

p-groups

Definition 3. The group G is a **p-group** if every element in G has order of a power of p.

Definition 4. A **p-subgroup** is a subgroup which is itself a p-group.

Definition 5. A **Sylow p-subgroup** P of a group G is a maximal p-subgroup of G. That is, P is a p-subgroup contained in no larger p-subgroup.

Theorem 4. *Let G be a p-group. Then the order of G is a power of p.*

Proof. If $q \neq p$ is a prime which divides $|G|$, then G would have an element of order q by Cauchy's Theorem. This contradicts the definition of a p-group, so we must have $|G| = p^n$ for some $n \in \mathbb{N}$. □

Example 1. Consider the group $(\mathbb{Z}_{36}, +)$. The order of the group is $36 = 2^2 3^2$ and therefore a Sylow 2-subgroup has order 4, and a Sylow 3-subgroup has order 9.

The Normaliser

Let G be a group, and let $\mathcal{S}$ be the collection of subgroups of G. We can turn $\mathcal{S}$ into a G-set by letting G act on $\mathcal{S}$ by conjugation: if $H \in \mathcal{S}$ and $g \in G$ then $g \cdot H = gHg^{-1}$, the conjugate subgroup. We define $G_H = \{g \in G : gHg^{-1} = H\}$.

Theorem 5. *G_H is a subgroup of G.*

Proof. We verify the group axioms. Associativity is inherited from G. We have $e \in G_H$ since $eHe^{-1} = H$. For inverses: if $g \in G_H$ then $gHg^{-1} = H$. Multiply on the left by g^{-1} and on the right by g to obtain $H = g^{-1}Hg = g^{-1}H(g^{-1})^{-1}$. So $g^{-1} \in G_H$. For closure: suppose $g_1, g_2 \in G_H$. So $g_1 H g_1^{-1} = g_2 H g_2^{-1} = H$. We have

$$\begin{aligned}(g_1g_2)H(g_1g_2)^{-1} &= (g_1g_2)H(g_2^{-1}g_1^{-1}) \\ &= g_1(g_2Hg_2^{-1})g_1^{-1} \\ &= g_1Hg_1^{-1} \\ &= H\end{aligned}$$

So $g_1g_2 \in G_H$. Hence G_H is a subgroup of G.

□

Now by construction, H is a normal subgroup of G_H, and G_H is the largest subgroup of G which has H as a normal subgroup.

Definition 6. We say that G_H is the **normaliser** of H in G, and write $N[H]$.

Theorem 6. *Let G be a group. If H is a finite subgroup of G then $g \in N[H]$ if $ghg^{-1} \in H$ for all $h \in H$.*

Proof. Suppose that $gh_1g^{-1} = gh_2g^{-1}$. By multiplying by g^{-1} on the left and by g on the right, we conclude that $h_1 = h_2$. So the conjugation map $i_g : H \to H$ given by $i_g(h) = ghg^{-1}$ is one-to-one. Since H is finite, we know that i_g is surjective. So we have $gHg^{-1} = H$, and $g \in N[H]$. □

Theorem 7. *(Normaliser Counting Theorem) Let G be a finite group, and H be a p-subgroup of G. Then*

$$(N[H] : H) \equiv (G : H) \mod p$$

Proof. Let $\mathcal{L}$ be the set of left cosets of H in G. Let H act on $\mathcal{L}$ by left translation: so $h \cdot (xH) = (hx)H$ for $h \in H, xH \in \mathcal{L}$.

Claim: $\mathcal{L}$ is an H-set. Proof of claim: We verify the group action axioms. Firstly, $e \cdot xH = (ex)H = xH$ for all $xH \in \mathcal{L}$ as required. Secondly, we have

$$\begin{aligned} g_1 \cdot (g_2 \cdot xH) &= g_1 \cdot (g_2x)H \\ &= (g_1g_2x)H \\ &= (g_1g_2) \cdot xH \end{aligned}$$

for all $g_1, g_2 \in H$ and $xH \in \mathcal{L}$ as required.

Now $|\mathcal{L}| = (G : H)$, the number of left cosets of H in G. We shall determine $\mathcal{L}_H$, the left cosets which are fixed under the action of all elements of H. We have

$$\begin{aligned} xH = h(xH) &\Leftrightarrow H = x^{-1}hxH \quad \forall h \in H \\ &\Leftrightarrow x^{-1}hx \in H \quad \forall h \in H \\ &\Leftrightarrow x^{-1}h(x^{-1})^{-1} \in H \quad \forall h \in H \\ &\Leftrightarrow x^{-1} \in N[H] \\ &\Leftrightarrow x \in N[H] \end{aligned}$$

So the left cosets in $\mathcal{L}_H$ are those which are contained in the normaliser $N[H]$. The number of such cosets is the index $(N[H] : H)$. So we have $|\mathcal{L}_H| = (N[H] : H)$.

Now since H is a p-group, it has order of p^k for some $k \in \mathbb{N}$. So we have $|\mathcal{L}| \equiv |\mathcal{L}_H| \mod p$ by the Counting Theorem (recall that $\mathcal{L}_H$ is the set of orbits of size 1). We conclude that $(G : H) \equiv (N[H] : H) \mod p$.

□

Theorem 8. *Let G be a finite group. Let H be a p-subgroup of G. If p divides $(G : H)$ then $N[H] \neq H$.*

Proof. We know that p divides $(N[H] : H)$ by using the Normaliser Counting Theorem (we have $(N[H] : H) \equiv (G : H) \equiv 0 \mod p$). So $(N[H] : H) \neq 1$, and therefore $N[H] \neq H$. □

The First Sylow Theorem

Theorem 9. *Let G be a finite group, and suppose that $|G| = p^n m$ for n, m integers with $n \geq 1$ and p does not divide m. Then*

1. *G contains a subgroup of order p^i for all $i \in \{1, \ldots, n\}$*

2. *Every subgroup $H \leq G$ of order p^i is a normal subgroup of a subgroup of order p^{i+1} for all $i \in \{1, \ldots, n-1\}$*

Proof. For (1) we shall use induction. For $i = 1$ we apply Cauchy's theorem: we have p divides $p^n m = |G|$ and therefore G has a subgroup of order p.

Now let H be a subgroup of order p^i for $i < n$.

Claim: Since $i < n$, we have $p \mid (G : H)$

Proof of Claim: We use Lagrange's Theorem. We have $|G| = p^n m$ and $|H| = p^i$, for $i < n$. Now $(G : H) = \frac{|G|}{|H|} = mp^{n-i}$, where $n - i > 0$. So p divides $(G : H)$.

Returning to the proof of the theorem: since $p \mid (G : H)$, we have $p \big| (N[H] : H)$ (by the Normaliser Counting Theorem). Now since H is a normal subgroup of $N[H]$, we know that the quotient $N[H]/H$ exists. We have p divides $|N[H]/H| = (N[H] : H)$. Now we apply Cauchy's theorem to conclude that $N[H]/H$ has a subgroup K of order p.

Claim: If $\gamma : N[H] \to N[H]/H$ is the canonical homomorphism (that is, it sends $n \mapsto nH$) then $\gamma^{-1}(K) = \{x \in N[H] : \gamma(x) \in K\}$ is a subgroup of $N[H]$.

Proof of Claim: We have $\gamma(e) = eH = H \in K$ so $e \in \gamma^{-1}(K)$, so $\gamma^1(K)$ is nonempty and contains the identity e. Suppose $g_1, g_2 \in \gamma^{-1}(K)$. So $\gamma(g_1), \gamma(g_2) \in K$. Since K is a subgroup, we have $\gamma(g_1)\gamma(g_2) \in K$. So, using the homomorphism property, $\gamma(g_1 g_2) \in K$. Hence $g_1 g_2 \in \gamma^{-1}(K)$, and therefore $\gamma^{-1}(K)$ is closed. Suppose $g \in \gamma^{-1}(K)$. Then $\gamma(g) \in K$, and since K is a subgroup we have $\gamma(g)^{-1} \in K$. Since homomorphisms respect inverses, we have $\gamma(g^{-1}) \in K$ and therefore $g \in \gamma^{-1}(K)$. Hence $\gamma^{-1}(K)$ has inverses, and we conclude that it is a subgroup of $N[H]$.

Since $\gamma^{-1}(K)$ is a subgroup of the normaliser $N[H]$, it is also a subgroup of G (because the subgroup relation is transitive). Now $\gamma^{-1}(K)$ contains H

and is of order p^{i+1}, since it contains the elements in p cosets, each of which is of order p^i.

For (2): We know that H is a subgroup of $\gamma^{-1}(K)$, which is a subgroup of $N[H]$. Since H is normal in $N[H]$, it is also normal in the potentially smaller group $\gamma^{-1}(K)$.

□

Note that if $|G| = p^n m$ then the First Sylow Theorem says that the Sylow p-subgroups are the subgroups of order p^n.

Example 2. Consider a group of order $40 = 2^3 5$. By the First Sylow Theorem, we conclude that there exist subgroups of order 8 and order 5.

The Second Sylow Theorem

Theorem 10. *Let G be a finite group, and P_1, P_2 be Sylow p-subgroups of G. Then P_1 and P_2 are conjugate subgroups of G.*

Proof. Let $\mathcal{L}$ be the collection of all left cosets of P_1 in G. Let P_2 act on $\mathcal{L}$ as follows: if $y \in P_2$, and $xP_1 \in \mathcal{L}$ then $y \cdot (xP_1) = (yx)P_1$.

Claim: $\mathcal{L}$ is a P_2-set.

Proof of Claim: We have $e \cdot (xP_1) = (ex)P_1 = xP_1$ as required for all $xP_1 \in \mathcal{L}$. Also, for all $g, h \in P_2$ and all $xP_1 \in \mathcal{L}$, we have

$$\begin{aligned} g \cdot (h \cdot xP_1) &= g \cdot ((hx)P_1) \\ &= (g(hx))P_1 \\ &= ((gh)x)P_1 \\ &= (gh) \cdot (xP_1) \end{aligned}$$

as required. So $\mathcal{L}$ is a P_2-set.

Now, since P_1, P_2 are Sylow p-subgroups, they are maximal. Let $n \in \mathbb{N}$ be such that $|P_1| = |P_2| = p^n$.

Since $|P_2|$ is a power of a prime, we can apply the Counting Theorem to conclude that $|\mathcal{L}_{P_2}| = |\mathcal{L}| \mod p$.

We have $|\mathcal{L}| = (G : P_1)$ from the definition of $\mathcal{L}$. Now, $|\mathcal{L}|$ is not divisible by p because $|P_1| = p^n$, and so by Lagrange's theorem, we have $(G : P_1) = |G|/|P_1| = m$, where p does not divide m.

So $|\mathcal{L}_{P_2}| \not\equiv 0 \mod p$, and therefore $|\mathcal{L}_{P_2}| \neq 0$ (that is, $\mathcal{L}_{P_2}$ is nonempty).

Let $xP_1 \in \mathcal{L}_{P_2}$. Then we have $y \cdot (xP_1) = xP_1$ for all $y \in P_2$, and so $x^{-1}yxP_1 = x^{-1}xP_1 = P_1$ for all $y \in P_2$. Hence $x^{-1}yx \in P_1$ for all $y \in P_2$.

Now, $x^{-1}P_2x$ is a subgroup of P_1. Since $|P_1| = |P_2|$ we have $P_1 = x^{-1}P_2x$ (because the conjugate map is one-to-one). So we conclude that P_1 and P_2 are conjugate subgroups.

□

The Third Sylow Theorem

Theorem 11. *Let G be a finite group with $p \mid |G|$. Then the number of Sylow p-subgroups is congruent to 1 mod p, and divides $|G|$.*

Proof. Let P be a Sylow p-subgroup of G. Let $\mathcal{S}$ be the set of all Sylow p-subgroups of G.

Claim: P acts on $\mathcal{S}$ by conjugation.

Proof of claim: We verify the group action axioms. Firstly, if $S \in \mathcal{S}$ then $e \cdot S = eSe^{-1} = S$ as required. Secondly, if $S \in \mathcal{S}$ and $g, h \in P$ then

$$\begin{aligned} g \cdot (h \cdot S) &= g \cdot (hSh^{-1}) \\ &= ghSg^{-1}g^{-1} \\ &= (gh)S(gh)^{-1} \\ &= (gh) \cdot (S) \end{aligned}$$

Returning to the proof of the theorem: Since P is a group with order of a prime power, we can apply the Counting Theorem to conclude that $|\mathcal{S}| \equiv |\mathcal{S}_P| \mod p$.

We now find $\mathcal{S}_P$. If $S \in \mathcal{S}_P$ then $gSg^{-1} = S$ for all $g \in P$. So P is a subgroup of the normaliser $N[S]$.

Now by definition, we know that S is a subgroup of $N[S]$. Since P and S are both Sylow p-subgroups of G, they are also Sylow p-subgroups of (the potentially smaller) $N[S]$. However, by the Second Sylow Theorem, P and S are conjugate in $N[S]$.

Since S is a normal subgroup of $N[S]$, it is its only conjugate in $N[S]$, from the definition of a normal subgroup. So we must have $S = P$, and therefore $\mathcal{S}_P = \{P\}$. Now since $|\mathcal{S}| \equiv |\mathcal{S}_P| \equiv 1 \mod p$, the number of Sylow p-subgroups is congruent to 1 mod p.

Now let G act on $\mathcal{S}$ by conjugation. Since all Sylow p-subgroups are conjugate, there is only one orbit in $\mathcal{S}$ under G. If $P \in \mathcal{S}$ then $|\mathcal{S}|$ is the number of elements in the orbit of P, or equivalently (by the Orbit-Stabiliser Theorem) $(G : G_P)$.

But $(G : G_P)$ divides $|G|$, by Lagrange, so the number of Sylow p-subgroups divides $|G|$.

□

Example 3. Let $p = 5, q = 7$. If G is a group with order $pq = 35$ then it has a single subgroup of order 7 which is normal in G (and so G is not simple).

Now $q = 7 \equiv 2 \bmod 5 = p$ and so G is abelian and cyclic. We can then conclude that $G \cong \mathbb{Z}_{35} \cong \mathbb{Z}_5 \times \mathbb{Z}_7$ by the Chinese Remainder Theorem.

Applications

Theorem 12. *If p is prime then $(p-1)! \equiv -1$ mod p.*

Proof. We will work with S_p, the symmetric group on p elements for p prime. Now p divides $p!$ but p^2 does not divide $p!$, and so the Sylow p-subgroups of S_p are the (cyclic) subgroups of order p.

There are $(p-1)!$ elements in S_p which are p-cycles, since there are $p-1$ choices of where to send the first element, $p-2$ choices where to send the second, and so on until the last one is uniquely determined.

Now, since p prime, every Sylow p-subgroup is generated by a p-cycle in S_p, and so each contains $p-1$ cycles of length p, and the identity. Note that each p-cycle is in precisely one of these subgroups - if σ is a p-cycle satisfying $\sigma \in \langle \sigma_1 \rangle$ and $\sigma \in \langle \sigma_2 \rangle$ then $\langle \sigma_1 \rangle = \langle \sigma_2 \rangle$.

So there are $(p-1)!/(p-1) = (p-2)!$ distinct Sylow p-subgroups in S_p. Now, the 3rd Sylow Theorem says that

$$(p-2)! \equiv 1 \mod p$$

and so $(p-1)! \equiv (p-1) \equiv 1 \bmod p$. □

Theorem 13. *Every finite p-group is solvable.*

Proof. If $G = p^r$ for some $r > 1$ then by the First Sylow Theorem, G has a subgroup H_i with order p^i which is normal in a subgroup H_{i+1} of order p^{i+1} for $1 \leq i < r$. Then

$$\{e\} = H_0 \lhd \cdots \lhd H_r = G$$

is a composition series for G. We have

$$|H_i/H_{i-1}| = p^i/p^{i-1} = p$$

so H_i/H_{i-1} is cyclic (all groups with prime order are cyclic) and therefore abelian, and G is solvable. □

Definition 7. Let G be a group and H, K be subgroups. The **product** of H and K is the set

$$\{hk : h \in H, k \in K\}$$

Definition 8. If H, K are subgroups of a group G then we define the **join** $H \vee K$ to be the subgroup generated by $H \cup K$.

Lemma 1. *Suppose G is a group and H, K are normal subgroups. If $H \cap K = \{e\}$ and $H \vee K = G$ then $G \cong H \times K$.*

Proof. We will show that $hk = kh$ for all $k \in K, h \in H$. We have

$$hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$$

Since H is normal, we have $h(kh^{-1}k^{-1} \in H$. Since K is normal, we have $(hkh^{-1})k^{-1} \in K$. So we conclude that $hkh^{-1}k^{-1} \in H \cap K$, and so

$$hkh^{-1}k^{-1} = e \Rightarrow hk = kh$$

We define a function $\phi : H \times K \to G$ by $\phi(h, k) = hk$.

Now ϕ is a homomorphism because

$$\begin{aligned}\phi((h,k)(h',k')) &= \phi(hh',kk') \\ &= hh'kk' \\ &= hkh'k' \\ &= \phi(h,k)\phi(h','k)\end{aligned}$$

If $\phi(h,k) = e$ then $hk = e \Rightarrow h = k^{-1}$. But then $h, k \in H \cap K$ and so $h = k = e$. Hence $\ker(\phi) = \{(e,e)\}$ and ϕ is one-to-one.

Since H, K are normal, we have $HK = H \vee K$. We also have $H \vee K = G$ by hypothesis. So we conclude that ϕ is onto, and therefore is an isomorphism. Hence $H \times K \cong G$.

□

Theorem 14. *Suppose that $p < q$ are primes. Then every group G of order pq has a single subgroup of order q which is normal in G, and therefore G is not simple. If $q \not\equiv 1$ mod p then G is abelian and cyclic.*

Remark. *Note that since G is cyclic, we have $G = \mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$.*

Proof. By the First Sylow Theorem, G has a Sylow q-subgroup. By the Third Sylow Theorem, the number of such subgroups is equal to 1 mod q and divides pq (hence divides p). Since $p < q$, we must have exactly one Sylow q-subgroup, denoted by Q. Now Q is normal in G, since under conjugation it is sent to itself, and therefore G is not simple.

Similary, there is at least one Sylow p-subgroup P of G. The number of such subgroups divides pq and must be congruent to 1 mod p. So it is either 1 or q.

If $q \not\equiv 1$ mod p then there is exactly one subgroup, P, and it is normal in G.

If $q \equiv 1 \bmod p$ then every element of Q, apart from e, has order q, and every element of P, apart from e, has order p. So $Q \cap P = \{e\}$.

Now we consider the subgroup $P \vee Q$. It contains Q as a proper subgroup, and the order of $P \vee Q$ divides pq, which is the order of G. So we must have $P \vee Q = G$.

Using Lemma 1, we conclude that since P, Q are normal, $G \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_q$. Hence G is abelian and cyclic. □

Theorem 15. *Let p be a prime. Then every group of order p^2 is abelian.*

Proof. If G is not cyclic, then every element except for e must have order p because the only options are 1 (the identity), p, and p^2 (not possible since G is not cyclic). We fix $a \in G$. So $\langle a \rangle$ is a subgroup of order p, and is a proper subgroup of G. Now fix $b \in G$, with $b \notin \langle a \rangle$. We have

$$\langle a \rangle \cap \langle b \rangle = \{e\}$$

since, if there exists $c \neq e$ with $c \in \langle a \rangle \cap \langle b \rangle$, then c generates both $\langle a \rangle$ and $\langle b \rangle$. We would then have $\langle a \rangle = \langle b \rangle$, which is a contradiction.

By the First Sylow Theorem, the subgroup $\langle a \rangle$ is normal in some subgroup of G with order p^2, and so $\langle a \rangle$ is normal in G. Similarly, $\langle b \rangle$ is normal in G.

Now $\langle a \rangle \vee \langle b \rangle$ is a subgroup of G, and its order must divide p^2. Therefore $\langle a \rangle \vee \langle b \rangle = G$.

Using Lemma 1, we have $G \cong \langle a \rangle \times \langle b \rangle$. Since $\langle a \rangle$ and $\langle b \rangle$ are abelian, then G is also abelian. We have $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$. □

Example 4. If G is a group of order p^r for $r > 1$ then G is not simple. By the First Sylow Theorem, there exists a non-trivial subgroup of order p^{r-1} which is normal in a subgroup of order p^r (and this subgroup must be G).

For example, if the order of G is 27 then there is a normal subgroup of order 9, and so G is not simple.

Example 5. Every group of order 15 is cyclic (and therefore abelian, and not simple since 15 is composite). We have $15 = 3 \times 5$ and $5 \not\equiv 1 \bmod 3$ so apply Theorem 14. But now consider groups of order 6. We have $6 = 2 \times 3$, so by Theorem 14 we conclude that G is not simple, however, $3 \equiv 1 \bmod 2$ so G is not necessarily cyclic or abelian. An example of such a group is the dihedral group.

Example 6. No group G of order 20 is simple. Now G contains a number of Sylow 5-subgroups congruent to 1 mod 5. Also, the number of Sylow 5-subgroups divides 20, so there must only be one. This subgroup is normal since all conjugates of it are itself.

Bibliography

[1] Fraleigh, J., 2002. *A First Course in Abstract Algebra*. Addison Wesley.

[2] Clark, P. *Wilson's Theorem: An Algebraic Approach*.
`http://alpha.math.uga.edu/~pete/wilson_easy.pdf`