

§26 Sylow's Theorem

Let G be a finite group. Lagrange's theorem asserts that, if G has a subgroup of order k , then k is a divisor of $|G|$. The converse of Lagrange's theorem, like the converses of many theorems, is wrong. If k is a divisor of $|G|$, then G need not have a subgroup of order k . For instance, A_4 has order 12, 12 is divisible by 6, yet A_4 has no subgroups of order 6.

The converse of Lagrange's theorem becomes true if we impose the additional condition that k be a prime power such that k and $|G|/k$ are relatively prime. In other words, if $|G| = p^a m$, where p is a prime number and $p \nmid m$, then G does have a subgroup H of order p^a . Then any conjugate H^g of H , too, is a subgroup of order p^a and the question arises as to whether G has subgroups of order p^a other than the conjugates of H . The answer turns out to be negative. The conjugates of H are the only subgroups of order p^a .

This theorem was proved by the Norwegian mathematician L. Sylow in 1872. It is a very important tool in the theory of finite groups. We present here a very elegant proof due to H. Wielandt (1959).

26.1 Theorem (Sylow's Theorem): *Let G be a finite group of order $|G| = p^a m$, where p is a prime number and $p \nmid m$ (that is, let p^a be the highest power of p dividing $|G|$). Then the following assertions hold.*

- (1) G has a subgroup H of order p^a .
- (2) If J is any subgroup of G whose order $|J|$ is a power of p , then there is an $x \in G$ such that $J \leq H^x$.
- (3) If n_p denotes the number of subgroups of order p^a , then $n_p \mid m$ and $n_p \equiv 1 \pmod{p}$.

Some remarks will now be in order. If $p^a \parallel |G|$ and $p^{a+1} \nmid |G|$, then a subgroup of G of order p^a is called a *Sylow p -subgroup of G* . Part (1) of Sy-

Sylow's theorem states that every finite group has a Sylow p -subgroup, for all prime numbers p .

If H is a Sylow p -subgroup of G , so is H^g for any $g \in G$. Part (2) of Sylow's theorem states that any subgroup of p -power-order of G is a subgroup of a suitable conjugate of H . In particular, any Sylow p -subgroup of G is contained in a suitable H^x for some $x \in G$, and, since the orders of that Sylow p -subgroup and of H^x coincide, that Sylow p -subgroup must be H^x itself. So any Sylow p -subgroup of G is a conjugate of H .

If a Sylow p -subgroup H of G is normal in G , then all conjugates of H are equal to H , hence H is the unique Sylow p -subgroup of G . Then, for any automorphism α of G , $H\alpha$ is a subgroup of order p^a , and therefore is equal to H . So H is in fact a characteristic subgroup of G in this case.

Part (3) of Sylow's theorem gives us arithmetical information about the possible number Sylow p -subgroups. Two applications of this is given in Lemma 26.5 and in Lemma 26.6.

Proof of Sylow's theorem: The basic idea of the proof is as follows. If there is a Sylow p -subgroup H of G , then H is first of all a *subset* of G having exactly p^a elements and is furthermore such that $Hh = H$ for all $h \in H$. So $H = \{h \in G: Uh = U\}$ for some subset U of G with $|U| = p^a$. In order to find a subgroup of order p^a , so we look at the sets $\{h \in G: Uh = U\}$, for each $U \subseteq G$ with $|U| = p^a$. Such sets are the stabilizers of U 's under the group action described below. A judicious choice of U will produce a subgroup of order p^a .

Step 1. Let $\mathfrak{U} = \{U \subseteq G: |U| = p^a\}$. Then the number $|\mathfrak{U}|$ of elements of \mathfrak{U} (= subsets of G in \mathfrak{U}) is not divisible by p :

There are clearly $\binom{p^a m}{p^a}$ subsets of G in \mathfrak{U} . We are to prove $p \nmid \binom{p^a m}{p^a}$.

We have $\binom{p^a m}{p^a} = \frac{(p^a m)!}{p^a!(p^a m - p^a)!} = \frac{p^a m}{p^a} \frac{p^a m - 1}{p^a - 1} \frac{p^a m - 2}{p^a - 2} \dots \frac{p^a m - (p^a - 1)}{1}$. Now

consider each one of the factors $\frac{p^a m - s}{p^a - s}$ ($s = 1, 2, \dots, p^a - 1$). We write $s =$

$p^b t$, with $t \in \mathbb{Z}$ and $p \nmid t$, and observe that neither the numerator nor the denominator of these numbers

$$\frac{p^a m - s}{p^a - s} = \frac{p^a m - p^b t}{p^a - p^b t} = \frac{p^{a-b} m - t}{p^{a-b} - t}$$

contain p after cancellations are made. Hence their product $\binom{p^a m}{p^a}$ is not divisible by p .

As an example, note that all 3's are cancelled in

$$\binom{18}{9} = \binom{3^2 2}{3^2} = \frac{18}{9} \frac{17}{8} \frac{16}{7} \frac{15}{6} \frac{14}{5} \frac{13}{4} \frac{12}{3} \frac{11}{2} \frac{10}{1} = \frac{2}{1} \frac{17}{8} \frac{16}{7} \frac{5}{2} \frac{14}{5} \frac{13}{4} \frac{4}{1} \frac{11}{2} \frac{10}{1}$$

Step 2. G acts on \mathfrak{U} when we put $Ug = \{ug : u \in U\}$ for $U \in \mathfrak{U}$, $g \in G$:

The mapping $U \rightarrow Ug$ is one-to-one (Lemma 8.1(2)) and onto (by definition of Ug). Hence $|Ug| = |U| = p^a$ and Ug is an element of \mathfrak{U} . Now $(Ug_1)g_2 = U(g_1g_2)$ for all $U \in \mathfrak{U}$, $g_1, g_2 \in G$ by Lemma 19.2 and also $U1 = \{u1 : u \in U\} = \{u : u \in U\} = U$ for all $U \in \mathfrak{U}$. Thus G acts on \mathfrak{U} .

Step 3. There is an orbit of \mathfrak{U} under the action of Step 2 such that the number of elements (of \mathfrak{U} ; equivalently, the number of subsets of G) in it is not divisible by p :

The orbit of any $U \in \mathfrak{U}$ is $\{Ug \in \mathfrak{U} : g \in G\}$. Now \mathfrak{U} is partitioned into disjoint orbits. If $\mathfrak{U}_1, \mathfrak{U}_2, \dots, \mathfrak{U}_k$ are the orbits, then

$$\mathfrak{U} = \mathfrak{U}_1 \cup \mathfrak{U}_2 \cup \dots \cup \mathfrak{U}_k.$$

Counting the number of elements and keeping in mind that the orbits are pairwise disjoint, we get

$$|\mathfrak{U}| = |\mathfrak{U}_1| + |\mathfrak{U}_2| + \dots + |\mathfrak{U}_k|.$$

If $|\mathfrak{U}_1|, |\mathfrak{U}_2|, \dots, |\mathfrak{U}_k|$ were all divisible by p , their sum $|\mathfrak{U}|$ would be divisible by p , too, contrary to Step 1. Thus at least one of the numbers $|\mathfrak{U}_1|, |\mathfrak{U}_2|, \dots, |\mathfrak{U}_k|$ is not divisible by p , as contended.

Let $U_0 \in \mathfrak{U}$ be such that the number of elements (of \mathfrak{U}) in its orbit is not divisible by p . This is the judicious choice we have alluded to. We put $H = \text{Stab}_G(U_0)$.

Step 4. $H \leq G$ and $|H| = p^a$:

H is a subgroup of G by Lemma 25.7. As to the second assertion, first we note that the orbit of U_0 is equal to $|G:H|$ (Lemma 25.10) and, by the choice of U_0 , this index $|G:H|$ is not divisible by p . So $p \nmid |G/H|$, so $p \nmid p^a m / |H|$. Writing $|H| = p^b n$, where $n \in \mathbb{N}$, $p \nmid n$ and, by Lagrange's theorem, $b \leq a$ and $n|m$, we get $p \nmid p^{a-b} m / n$. This is possible only in case $p^{a-b} = p^0$. Hence $a = b$ and $|H| = p^a n \geq p^a$. On the other hand, if

$U_0 = \{u_1, u_2, \dots, u_{p^a}\}$, then, for any $h \in H = \text{Stab}_G(U_0)$, we have

$$\begin{aligned} u_1 h &\in U_0 h = U_0 = \{u_1, u_2, \dots, u_{p^a}\} \\ h &\in \{u_1^{-1} u_1, u_1^{-1} u_2, \dots, u_1^{-1} u_{p^a}\} \\ H &\subseteq \{u_1^{-1} u_1, u_1^{-1} u_2, \dots, u_1^{-1} u_{p^a}\} \\ |H| &\leq p^a. \end{aligned}$$

From $|H| \geq p^a$ and $|H| \leq p^a$, we get $|H| = p^a$.

By Step 4, H is a Sylow p -subgroup of G . This completes the proof of part (1). We proceed to the proof of part (2). Let $J \leq G$ be such that $|J| = p^b$, where $b \geq 0$.

Step 5. There is an $x \in G$ such that $J \leq H^x$:

Let $\mathfrak{R} = \{Ha : a \in G\}$ be the set of all right cosets of H in G . Then G acts on \mathfrak{R} by right multiplication (Example 25.12(b)) and its subgroup J also acts on \mathfrak{R} . Since the order of J is a power of p , we can apply Lemma 25.20 and conclude

$$|\mathfrak{R}| \equiv |\text{Fix}_{\mathfrak{R}}(J)| \pmod{p},$$

hence $|\text{Fix}_{\mathfrak{R}}(J)| \equiv |\mathfrak{R}| = |G:H| = m \not\equiv 0 \pmod{p}$

$$|\text{Fix}_{\mathfrak{R}}(J)| \neq 0$$

$$\text{Fix}_{\mathfrak{R}}(J) \neq \emptyset.$$

So there is a right coset Hx in $\text{Fix}_{\mathfrak{R}}(J)$. Thus $\text{Stab}_J(Hx) = J$. But $\text{Stab}_J(Hx) = J \cap \text{Stab}_G(Hx) = J \cap H^x$ by Example 25.12(b). So we obtain $J \cap H^x = J$, which means $J \leq H^x$.

This completes the proof of part (2). In view of the remarks preceding the proof, all Sylow p -subgroups of G are conjugate; and a normal Sylow p -subgroup of a finite group is the unique Sylow p -subgroup of that group.

Let $N := N_G(H) = \{g \in G: H^g = H\}$ be the normalizer of H in G . Then $H \triangleleft N$, $N \leq G$ and, since $p \nmid |N:H|$, H is a Sylow p -subgroup of N . Thus H is the unique Sylow p -subgroup of N .

We now prove part (3). Let n_p be the number of Sylow p -subgroups of G .

Step 6 $n_p = |G:N|$:

Let $\mathfrak{X} = \{H^x \leq G: x \in G\}$. Then \mathfrak{X} is the set of all Sylow p -subgroups of G . We want to evaluate $n_p = |\mathfrak{X}|$. Here G acts on \mathfrak{X} by conjugation, because $(H^x)^g = H^{xg} \in \mathfrak{X}$; $(H^{g_1})^{g_2} = H^{(g_1g_2)}$; and $H^1 = 1^{-1}H1 = H$ for all $H \in \mathfrak{X}, g_1, g_2 \in G$. Lemma 25.10 gives now

$$|\text{orbit of } H| = |G:\text{Stab}_G(H)|.$$

But the orbit of $H = \{H^x \leq G: x \in G\} = \mathfrak{X}$ and $\text{Stab}_G(H) = N_G(H) = N$. Thus

$$n_p = |\mathfrak{X}| = |G:N|,$$

as was to be proved.

Step 7. $n_p |m$ and $n_p \equiv 1 \pmod{p}$:

Of course $n_p = |G:N|$ divides $|G:N||N:H| = |G:H| = m$.

Now we want to prove $n_p \equiv 1 \pmod{p}$. This will be done by applying Lemma 25.20. In order to apply Lemma 25.20, we need the action of a group of p -power order on a finite set. Our group of p -power order will be H , as this is the only group of p -power order available to us. H acts on $\mathfrak{R}_1 = \{Na: a \in G\}$ the set of all right cosets of N in G by right multiplication (Example 25.12(b), Example 25.2(h)). Lemma 25.20 yields

$$|\mathfrak{R}_1| \equiv |\text{Fix}_{\mathfrak{R}_1}(H)| \pmod{p}.$$

Since $n_p = |G:N| = |\mathfrak{R}_1|$, the claim will be established when we show that $|\text{Fix}_{\mathfrak{R}_1}(H)| = 1$.

From the equivalences

$$\begin{aligned}
Na \in \text{Fix}_{\mathfrak{R}_1}(H) &\Leftrightarrow \text{Stab}_H(Na) = H \\
&\Leftrightarrow (Na)h = Na \text{ for all } h \in H \\
&\Leftrightarrow Nah a^{-1} = N \text{ for all } h \in H \\
&\Leftrightarrow aha^{-1} \in N \text{ for all } h \in H \\
&\Leftrightarrow h^{a^{-1}} \in N \text{ for all } h \in H \\
&\Leftrightarrow H^{a^{-1}} \subseteq N \\
&\Leftrightarrow H^{a^{-1}} \text{ is a Sylow } p\text{-subgroup of } N \\
&\Leftrightarrow H^{a^{-1}} \text{ the unique Sylow } p\text{-subgroup } H \text{ of } N \\
&\Leftrightarrow H^{a^{-1}} = H \\
&\Leftrightarrow a^{-1} \in N_G(H) = N \\
&\Leftrightarrow a \in N \\
&\Leftrightarrow Na = N,
\end{aligned}$$

it follows that $\text{Fix}_{\mathfrak{R}_1}(H) = \{N\}$. Thus $|\text{Fix}_{\mathfrak{R}_1}(H)| = 1$ and $n_p \equiv 1 \pmod{p}$.

This completes the proof. □

26.2 Definition: Let p be a prime number. A finite group G is called a *finite p -group* if $|G| = p^a$ for some integer $a \geq 0$.

26.3 Theorem: Let G be a finite p -group, with $|G| = p^a > 1$.

- (1) G has a normal subgroup of order p .
- (2) There are normal subgroups H_i of G such that $|H_i| = p^i$ ($i = 0, 1, 2, \dots, a$) and
$$1 = H_0 \leq H_1 \leq H_2 \leq \dots \leq H_{a-1} \leq H_a = G.$$

Proof: (1) From Theorem 25.17, we know $Z(G) \neq 1$. Let $z \in Z(G)$ with $z \neq 1$, and let $o(z) = p^k$ ($1 \leq k \leq a$). Then $o(z^{p^{k-1}}) = p$. Thus $\langle z^{p^{k-1}} \rangle$ is a subgroup of order p and is normal in G (Theorem 23.3).

(2) We make induction on a . If $a = 1$, then $|G| = p$ and G has normal subgroups H_0 and H_1 , namely $H_0 = 1$ and $H_1 = G$, with $|H_0| = 1$ and $|H_1| = p$ such that $H_0 \leq H_1$.

Assume now that $a \geq 2$ and that the claim is true for any finite p -group of order p^{a-1} . By part (1), there is $H_1 \triangleleft G$ with $|H_1| = p$. We consider the

factor group G/H_1 , which has order $|G/H_1| = |G|/|H_1| = p^a/p = p^{a-1}$. By induction, there are normal subgroups, say H_{i+1}/H_1 , of G/H_1 with $|H_{i+1}/H_1| = p^i$ ($i = 0, 1, \dots, a-1$) and

$$1 = H_1/H_1 \leq H_2/H_1 \leq H_3/H_1 \leq \dots \leq H_{a-1}/H_1 \leq H_a/H_1 = G/H_1.$$

By Theorem 21.2, each $H_i \trianglelefteq G$ ($i = 1, 2, \dots, a$) and

$$H_1 \leq H_2 \leq \dots \leq H_{a-1} \leq H_a = G.$$

Here $|H_{i+1}| = |H_{i+1}/H_1||H_1| = p^i p = p^{i+1}$ for $i = 0, 1, \dots, a-1$. Thus, when we put $H_0 = 1$, the claim is proved for finite p -groups of order p^a . \square

26.4 Theorem: *Let G be a finite group and let p be a prime number. Suppose $p^b \parallel |G|$, where $b \geq 0$. Then G has a subgroup of order p^b .*

Proof: Let us write $|G| = p^a m$, with $m \in \mathbb{N}$ and $p \nmid m$. Then G has a Sylow p -subgroup H of order p^a , and, by Theorem 26.3(2), H has a subgroup J of order p^b . Hence J is a subgroup of G with $|J| = p^b$. \square

Theorem 26.4 generalizes Sylow's theorem (1) to the case where p^b is any prime power divisor of $|G|$ (not necessarily the highest power of p dividing $|G|$). Part (2) of Sylow's theorem does not generalize: two subgroups J_1 and J_2 , of the same order p^b , are not necessarily conjugate in G , or even isomorphic. Part (3) of Sylow's theorem, however, is true in the more general case: if $p^b \parallel |G|$, then the number of subgroups of order p^b in G is congruent to 1 modulo p .

We close this paragraph with two applications of Sylow's theorem.

26.5 Lemma: *Let p and q be distinct prime numbers and let G be a group of order pq . Then either a Sylow p -subgroup or a Sylow q -subgroup of G is normal in G . In fact, if $p > q$, then a Sylow p -subgroup of G is normal in G .*

Proof: Suppose $p > q$ and let n_p be the number of Sylow p -subgroups of G . Then n_p divides $|G|/p = q$, so $n_p = 1$ or q , and $n_p \equiv 1 \pmod{p}$. So $n_p = q$ implies $p \mid q-1$, which is not compatible with $p > q$. Thus $n_p = q$ is impossible and $n_p = 1$. Then there is a unique Sylow p -subgroup of G , and it is normal in G .

□

26.6 Lemma: *Let p and q be distinct prime numbers and let G be a group of order p^2q . Then either a Sylow p -subgroup or a Sylow q -subgroup of G is normal in G .*

Proof: Let n_p, n_q be the number of Sylow p and Sylow q -subgroups of G , respectively. The claim is that either $n_p = 1$ or $n_q = 1$. Suppose, by way of contradiction, that $n_p > 1$ and $n_q > 1$.

Since n_p divides $|G|/p^2 = q$, and since q is prime, we have $n_p = q$. From $q = n_p \equiv 1 \pmod{p}$, we get $p \leq q - 1$, so $q > p$. Besides, n_q divides $|G|/q = p^2$, so $n_q = p$ or p^2 . Here $n_q = p$ is impossible, because $n_q \equiv 1 \pmod{q}$ and $q > p$. Thus $n_q = p^2$.

Let Q_1, Q_2, \dots, Q_{p^2} be the Sylow q -subgroups of G . An element of order q is a nonidentity element in one of these subgroups, and any two distinct of them have a trivial intersection: $Q_i \cap Q_j = 1$. Hence

$$\{g \in G: o(g) = q\} = (Q_1 \setminus \{1\}) \cup (Q_2 \setminus \{1\}) \cup \dots \cup (Q_{p^2} \setminus \{1\}),$$

where the union is taken over pairwise disjoint sets. Counting the number of elements on the right hand side, we see that there are exactly $p^2(q-1)$ elements of order q in G . So there are exactly $|G| - p^2(q-1) = p^2$ elements in

$$G \setminus \{g \in G: o(g) = q\} = \{g \in G: o(g) \neq q\}.$$

Let P be a Sylow p -subgroup of G . Then $P \subseteq \{g \in G: o(g) \neq q\}$, and, since both of these sets have p^2 elements, we have $P = \{g \in G: o(g) \neq q\}$. Therefore $\{g \in G: o(g) \neq q\}$ is the unique Sylow p -subgroup of G and n_p is equal to 1, a contradiction. So G has either a normal Sylow p -subgroup or a normal Sylow q -subgroup. □

Exercises

1. Find Sylow 2- and Sylow 3-subgroups of S_4 , A_4 , $SL(2, \mathbb{Z}_3)$, $GL(2, \mathbb{Z}_3)$.
2. Find a Sylow p -subgroup of D_{2n} ($n \in \mathbb{N}$).
3. Let G be a finite group with exactly one Sylow p -subgroup. Prove that every subgroup and every factor group of G , too, has exactly one Sylow p -subgroup.
4. Let G be a finite group and $K \triangleleft G$. If P is a Sylow p -subgroup of G , show that $P \cap K$ is a Sylow p -subgroup of K and PK/K is a Sylow p -subgroup of G/K .
5. Let G be a finite group and $H \leq G$. Show that, if P is a Sylow p -subgroup of G , then $P \cap H$ is not necessarily a Sylow p -subgroup of H .
6. Let G be a finite group, $H \leq G$ and let P_1 be a Sylow p -subgroup of H . Show that there is a Sylow p -subgroup P of G such that $P \cap H = P_1$.
7. Let $P \leq K \triangleleft G$, where G is a finite group and P is a Sylow p -subgroup of K . Show that $G = N_G(P)K$.
8. Let G be a finite group and $H, J \leq G$. Suppose J is a finite p -group and $|H| \not\equiv 1 \pmod{p}$, where p is a prime number. Prove that $H \cap C_G(J) \neq 1$.
9. Let G be a finite p -group. Show that, if $1 \neq H \triangleleft G$, then $H \cap Z(G) \neq 1$.
10. Let G be a finite p -group and $H < G$. Prove that $H < N_G(H)$.
11. Let p, q, r be distinct prime numbers and let G be a group of order pqr . Show that G has a nontrivial proper normal subgroup.
12. Let G be a finite p -group, with $|G| = p^a > 1$, and let $K \leq G$. Prove that there are subgroups H_i of G such that
 - (i) $|H_i| = p^i$ for all $i = 0, 1, 2, \dots, a$,
 - (ii) $K = H_j$ for some $i = 0, 1, 2, \dots, a$,
 - (iii) $1 = H_0 \triangleleft H_1 \triangleleft H_2 \triangleleft \dots \triangleleft H_{a-1} \triangleleft H_a = G$.

