## APPLICATIONS OF SYLOW THEOREM

We are going to discuss now how Sylow theorem can be used to investigate finite groups, in particular to show that a particular finite group is not simple/is solvable/is abelian. Let $G$ be a group, $p$ a prime and $|G| = p^a m$ with $(m, p) = 1$. The following techniques are very useful in proving that $G$ is not simple:

- we know that the number $t_p$ of Sylow $p-$subgroups of $G$ divides $m$ and $p|(t_p - 1)$. Inspect the divisors of $m$ to show that $t_p = 1$ is the only possibility.
- if the above does not work, perhaps you can conclude that either $t_p = 1$ or $t_p$ is quite large. Assuming the latter case, count the number of $p-$**elements** (i.e. elements of $p-$power order) to show that you get too many, or that it forces that $t_q = 1$ for some other prime $q||G|$.
- try several different primes and show that counting for all of them at once leads to a contradiction (too many elements) unless $t_q = 1$ for some $q$.
- try to find a subgroup of $G$ of relatively small index and study the corresponding permutation representation on left cosets. Show that the kernel of this representation is not trivial, so it provides a normal subgroup.
- combine all the above methods and apply them not only to $G$ but to some subgroups of $G$ (like centralizers or normalizers of some $p-$subgroups,...).

The best way to get a better understanding of the above ideas is to work out several examples.

**Groups of order** $pq$ We are now going to discuss groups $G$ of order $pq$, where $p$ and $q$ are primes.

**Exercise.** a) Prove that a group of order $p^2$ is abelian (use the fact that it has a nontrivial center).

b) Prove that group of order $p^2$ is either cyclic or isomorphic to a direct product of two cyclic groups of order $p$.

We assume now that $p < q$. Let us first analyze the number $t_q$ of Sylow $q-$subgroups. We have $t_q|p$ so $t_q \leq p$. But also $q|(t_q - 1)$ so either $t_q = 1$ or $t_q > q$. Since $q > p$, we see that the only possibility is that $t_q = 1$. Thus $G$ has a normal Sylow $q-$subgroup $C_q$. Since its order is $q$, it is cyclic and contains all elements of $G$ of order $q$. Choose a generator $a$ for $C_q$.

The group $G$ has a subgroup $C_p$ of order $p$. It is cyclic. Note that $C_p \cap C_q = \{1\}$, since $p \neq q$. Also, $C_q C_p = G$ (just count the elements). It follows that $G$ is a semidirect product $C_q \rtimes_\phi C_p$ for some homomorphism $\phi : C_p \longrightarrow \mathrm{Aut}C_q$.

Recall now that $\mathrm{Aut}C_q$ is isomorphic to the multiplicative group of the field $\mathbb{F}_q$ of order $q$. In fact, for $f \in \mathrm{Aut}C_q$ we have $f(a) = a^i$ for some $i$ prime to $q$ and the map which assigns to $f$ the residue of $i$ modulo $q$ is an isomorphism from $\mathrm{Aut}C_q$ onto $\mathbb{F}_q^\times$. In particular, the order of $\mathrm{Aut}C_q$ equals $q-1$. Recall now that $\mathbb{F}_q^\times$ is cyclic (existence of primitive roots).

Since the order of $\mathrm{Aut}C_q$ equals $q-1$, $\phi$ has to be trivial unless $p|(q-1)$. Thus, if $p \nmid (q-1)$ then $G$ is the direct product of $C_p$ and $C_q$, hence it is cyclic of order $pq$ (this also follows from Sylow theorem).

Suppose now that $p|(q-1)$ and $\phi$ is not trivial. Then $\phi$ is injective. Since $\mathrm{Aut}C_q$ is cyclic, it has unique subgroup $< f >$ of order $p$, which then coincides with the image of $\phi$. Thus there is $b \in C_p$ such that $\phi(b) = f$. Clearly $C_p =< b >$. So we see that $G$ is uniquely defined by the requirement that $\phi$ is not trivial. It is not hard to see that $G$ has a presentation $< a, b | a^q = 1 = b^p, bab^{-1} = a^i >$, where $i$ is such that $f(a) = a^i$.

We proved the following

**Theorem 1.** *Let $G$ be a group of order $pq$ where $p < q$ are primes. If $p \nmid (q-1)$ then $G$ is cyclic. If $p|(q-1)$ then either $G$ is cyclic or $G$ is non abelian given by a presentation $< a, b | a^q = 1 = b^p, bab^{-1} = a^i >$, where $i$ is any integer such that $q|i^p - 1$ and $i - 1$ is not divisible by $q$ (different choices of $i$ produce isomorphic groups). In any case, $G$ has a normal subgroup of order $q$.*

## Groups of order 144

We are now going to show that there is no simple group of order 144. Several important techniques will be described in the course of the proof.

Suppose to the contrary that $G$ is a simple group of order $144 = 2^4 3^2$.

(1) We claim that $G$ has no proper subgroups of index smaller than 6. In fact, if $k = [G : H] \leq 5$ then the permutation representation on the left cosets of $H$ is a nontrivial homomorphism $\pi : G \longrightarrow S_k$. Since $144 > 120 = 5! \geq k!$, $\pi$ can not be injective, so $\ker \pi$ is a nontrivial proper normal subgroup, a contradiction.

(2) Consider the set $Syl_3$ of Sylow 3−subgroups of $G$. Its cardinality $t_3$ divides 16 and is congruent to 1 modulo 3. Thus $t_3 \in \{1, 4, 16\}$. We can not have $t_3 = 1$, since this would mean that $G$ has a normal Sylow 3−subgroup. Recall the following important fact:
**the number $t_p$ of Sylow $p-$subgroups of $G$ equals $[G : N_G(P)]$, where $P$ is any Sylow $p-$subgroup of $G$.**
Thus $t_3 = [G : N_G(P)] \geq 6$ by (1). We see that $t_3 = 16$ is the only possibility.

(3) Suppose that $P, P'$ are different Sylow 3−subgroups. They have order 9, hence are abelian. We claim that $P \cap P' = \{1\}$. Suppose not. Then $Q = P \cap P'$ has order 3. The normalizer $N_G(Q)$ is a proper subgroup of $G$ and it contains both $P$ and $P'$. In particular, the order of $N_G(Q)$ is divisible by 9 and larger than 9, i.e it is $2^u \cdot 9$ for some $1 \leq u \leq 3$. It follows that $1 < [G : N_G(Q)] = 2^{4-u} \leq 8$. By (1), we have $[G : N_G(Q)] = 8$ and consequently $|N_G(Q)| = 18$. But then both $P, P'$ are of index 2 in $N_G(Q)$, so they are normal. We see that both $P, P'$ are normal Sylow 3−subgroups of $N_G(Q)$, so $P = P'$, a contradiction.

(4) Thus any two distinct Sylow 3−subgroups of $G$ have trivial intersection. The total number of nontrivial elements in these groups (i.e. the number of nontrivial 3−elements in $G$) equals $t_3(9 - 1) = 128$ by (2). There are 16 elements left. Since $G$ has a subgroup of order 16, these element form the unique subgroup of order 16 in $G$, i.e. $t_2 = 1$. Thus $G$ has a normal Sylow 2−subgroup, a contradiction.

## Simple groups of order 60

The goal now is to prove that if $G$ is a simple group of order 60 then $G \cong A_5$.
Let $G$ be simple, $|G| = 60 = 2^2 \cdot 3 \cdot 5$.

(1) We claim that if $G$ has a proper subgroup of index $\leq 5$, then $G \cong A_5$. In fact, suppose $[G : H] = k \leq 5$. Consider the permutation representation of $G$ on left cosets of $H$. It is a nontrivial homomorphism $\pi : G \longrightarrow S_k$. Since $G$ is simple, $\pi$ is injective. Thus $60|k!$, so $k = 5$ (since $k \leq 5$). Thus $\pi(G)$ is a subgroup of index 2 in $S_5$, hence normal. We have seen that the only nontrivial proper normal subgroup of $S_5$ is $A_5$ so $\pi$ establishes an isomorphism between $G$ and $A_5$.

(2) It remains to show that $G$ has a subgroup of index $\leq 5$. Suppose not. Consider the set $Syl_2(G)$. Let $P \in Syl_2$. Thus $t_2 = [G : N_G(P)] \geq 6$. But $t_2$ divides 15, so $t_2 = 15$ is the only possibility.

(3) Let $P, P'$ be different Sylow 2−subgroups. They have order 4, hence are abelian. We claim that $P \cap P' = \{1\}$. Suppose not, then $Q = P \cap Q'$ has order 2 and the normalizer $N_G(Q)$ is a proper subgroup of $G$ and it contains both $P$ and $P'$. In particular, the order of $N_G(Q)$ is divisible by 4 and larger than 4. It follows that $[G : N_G(Q)]$ is a proper divisor of 15, hence does not exceed 5. This contradicts (2).

(4) We see that any two distinct Sylow 2−subgroups of $G$ have trivial intersection. We count now the number of nontrivial 2−elements. It equals $t_2(4 - 1) = 45$ by (2). We also count nontrivial 5−elements. Note that $t_5 > 1$ and $5|(t_5 - 1)$, so $t_5 \geq 6$. Since Sylow 5−subgroups of $G$ have order 5, distinct Sylow 5−subgroups have trivial intersection. Thus the number of nontrivial 5−elements is $t_5(5 - 1) = 4t_5 \geq 24$. This implies that $G$ gas at least $45 + 24 = 69$ elements, a contradiction.

## Groups of order 9555

We discuss one more example and prove that groups of order 9555 are not simple. Suppose that $G$ is a simple group of order $9555 = 3 \cdot 5 \cdot 7^2 \cdot 13$.

(1) We claim that $G$ has no subgroups of index $\leq 12$. In fact, if $[G : H] = k \leq 12$, then the permutation representation $\pi : G \longrightarrow S_k$ on the left cosets of $H$ cannot be injective, since $13 \nmid k!$.

(2) Let $Q \in Syl_{13}(G)$ and $H = N_G(Q)$. Thus $t_{13} = [G : H] \geq 13$. Since $1 < t_{13} | 3 \cdot 5 \cdot 7^2$ and $13 | (t_{13} - 1)$, it is easy to see that $t_{13} = 3 \cdot 5 \cdot 7$ is the only possibility. Thus $|H| = 7 \cdot 13$. In particular, $H$ is cyclic.

(3) Let $B$ be the Sylow $7-$subgroup of $H$. Thus $B$ is central in $H$. By Sylow's theorem, $B$ is contained in a Sylow $7-$subgroup $D$ of $G$. Since $|D| = 7^2$, $D$ is abelian so $D$ centralizes $B$. Thus $C_G(B)$ contains both $H$ and $D$, so its order is at least $7^2 \cdot 13$. By (1), the order of $C_G(B)$ is exactly $7^2 \cdot 13$ (otherwise its index in $G$ would be too small).

(4) Note that $Q$ is a Sylow $13-$subgroup of $C_G(B)$. The number of Sylow $13-$subgroups of $C_G(B)$ divides $7^2$ and is congruent to 1 mod 13, so it equals 1. In other words, $C_G(B)$ has unique Sylow $13-$subgroup, namely $Q$. Thus $Q$ is normal in $C_G(B)$, i.e. $C_G(B) < N_G(Q)$. This however contradicts (2), where we showed that $|N_G(Q)| = 7 \cdot 13$.

**Simple groups of prder $p^2qr$.**

Let $G$ be a finite simple group of order $p^2qr$, where $p, q, r$ are distinct prime numbers. We will prove that $G$ is isomorphic to $A_5$.

Since $G$ is simple, the action of $G$ on the left cosets of any proper subgroup $H$ has trivial kernel. This implies that $p^2qr$ divides $[G : H]!$, hence

(1) If $H < G$ then $[G : H] \geq \max\{2p, q, r\}$.

Since the number of Sylow subgroups is equal to the index of the normalizer of a Sylow subgroup, we get

(2) Let $t_p = |Syl_p(G)|$, $t_q = |Syl_q(G)|$, $t_r = |Syl_r(G)|$. By (1), each of these numbers is greater or equal than $\max\{2p, q, r\}$.

Recall that $t_p | qr$, $p | t_p - 1$, $t_q | p^2r$, $q | t_q - 1$, $t_r | p^2q$, $r | t_r - 1$.

(3) If $r$ is the largest among $p, q, r$ then $t_r = pq$ and $p | r - 1$.

In order to prove (3) note that $t_r | p^2q$ and $t_r > r$ (as $r | t_r - 1$). It follows that $t_r \in \{p^2, pq, p^2q\}$.

If $t_r = p^2$ then $r|p^2-1 = (p-1)(p+1)$, so $r|p-1$ or $r|p+1$. As $r > p$, we must have $r = p+1$. This means that $p = 2$ and $r = 3$. However this contradicts the assumption that $r > q$.

Suppose now that $t_r = p^2q$. Then $G$ has $p^2q(r-1)$ elements of order $r$ (as any two different Sylow $r$-subgroups have trivial interesction). Furthermore, $G$ has at least $p^2+1$ non-trivial elements of order a power of $p$ (as $t_p > 1$) and it has $t_q(q-1)$ elements of order $q$. Thus $p^2qr > p^2q(r-1)+p^2+t_q(q-1)$, i.e. $p^2 > t_q$. Since $t_q|p^2r$ and $p < r \leq t_q < p^2 < pr$, we must have $t_q = r$. This means that the normalizer $M$ of a Sylow $q$-subgroup has order $p^2q$. Since we have $p^2qr - p^2q$ elements of order $r$, the remaining elements constitute $M$. Thus $M$ is a normal subgroup of $G$, a contradiction.

Thus $t_r = pq$ is the only option left. Consider a Sylow $r$-subgroup $S$ of $G$ and let $N$ be its normalizer in $G$. Thus $|N| = pr$. Suppose that $N$ is abelian and $Q$ is its Sylow $p$-subgroup. Then $Q$ has order $p$ and it is contained in a Sylow $p$-subgroup $P$ of $G$. Both $S$ and $P$ centralize $Q$, so the centralizer of $Q$ in $G$ has order $p^2r$ and index $q$, which contradicts (1) (as $q < r$). Thus $N$ is not abelian, which can only happen if $p|r-1$.

(4) Any two distinct Sylow $p$-subgroups of $G$ have a trivial intersection.

Indeed, suppose two distinct Sylow $p$-subgroups $P_1, P_2$ of $G$ have a non-trivial intersection $Q = P_1 \cap P_2$. Then $Q$ is centralized by $P_1$ and $P_2$ (as $P_i$ have order $p^2$, hence are abelian). Thus the centralizer $C_G(Q)$ has order divisible by $p^2$ and bigger than $p^2$. It follows that the order of $C_G(Q)$ is either $p^2q$ or $p^2r$. Without loss of generality, we may assume that $|C_G(Q)| = p^2q$. Then $r$, being the index of a proper subgroup $C_G(Q)$, is the largest of $p, q, r$ by (1). By (3), we have $t_r = pq$ and $p|r-1$. Note that $C_G(Q)$ has two different Sylow $p$-subgroups $P_1$ and $P_2$, hence it has exactly $q$ Sylow $p$-subgroups. It follows that $p|q-1$. Let $T$ be a Sylow $q$-subgroup of $C_G(Q)$. Since $Q$ is central in $C_G(Q)$, the normalizer of $T$ in $C_G(Q)$ contains both $T$ and $Q$ and therefore it has either $pq$ or $p^2q$ elements. In the former case, $C_G(Q)$ has exactly $p$ Sylow $q$-subgroups and $q|p-1$, contradicting the divisibility $p|q-1$. Thus

$T$ is normal in $C_G(Q)$. Then $C_G(Q)$ must be the normalizer of $T$ in $G$ and $t_q = r$. It follows that $q|r-1$. We know from (3) that $p|r-1$, so $pq|r-1$ and $r > pq$. On the other hand $pq = t_r > r$, a contradiction.

(5) $t_p \neq qr$.

Indeed, suppose that $t_p = qr$, then by (4) the group $G$ has $qr(p^2-1)$ non-trivial elements of $p$-power order. We also have $t_q(q-1)$ elements of order $q$ and $t_q \geq r$. Similarly, we have $t_r(r-1)$ elements of order $r$ and $t_r \geq q$. Thus

$$p^2qr \geq 1+qr(p^2-1)+r(q-1)+q(r-1) = p^2qr+qr-q-r+1 = p^2qr+(q-1)(r-1),$$

a contradiction.

From (5) we see that $t_p = q$ or $t_p = r$. Without loss of generality we may assume that $t_p = r$. Then $r$ is the largest among $p, q, r$ by (2). Applying (3) we have

(6) $t_p = r$, $t_r = pq$, $p|r-1$, $r > q$.

(7) $t_q = pr$ and $p|q-1$.

Indeed, $t_q|p^2r$ and $t_q \geq r > p$. Thus $t_q \in \{r, p^2, pr, p^2r\}$. We consider now each possibility.

If $t_q = r$ then $q|r-1$. Since $p|r-1$ by (6), we get $pq|r-1$, so $r > pq = t_r$, a contradiction.

Suppose that $t_q = p^2$. Let $T$ be a Sylow $q$ subgroup of $G$ and $N$ its normalizer in $G$. Then $|N| = qr$. Since $r > q$, $N$ has a normal Sylow $r$-subgroup $R$. This hower implies that $N$ normalizes $R$. Since $t_r = pq$, the normalizer of $R$ in $G$ has order $pr$ and contains $N$, a contradiction.

Suppose now that $t_q = p^2r$. Then $G$ has $p^2r(q-1)$ elements of order $q$. By (4) and (6), $G$ has $r(p^2-1)$ non-trivial elements of order a power of $p$ and it has $pq(r-1)$ elements of order $r$. Thus

$$p^2qr \geq 1+p^2r(q-1)+r(p^2-1)+pq(r-1) = 1+p^2qr-r+pqr-pq = p^2qr+(r-1)(pq-1)$$

which is clearly false. This shows that $t_q = p^2r$ is not possible.

Thus $t_q = pr$ is the only option left. Consider a Sylow $q$-subgroup $S$ of $G$ and let $N$ be its normalizer in $G$. Thus $|N| = pq$. Suppose that $N$ is abelian and $Q$ is its Sylow $p$-subgroup. Then $Q$ has order $p$ and it is contained in a Sylow $p$-subgroup $P$ of $G$. Both $N$ and $P$ centralize $Q$, so the centralizer $C_G(Q)$ has order $p^2q$. Note that $N$ is the normalizer of $S$ in $C_G(Q)$, so $C_Q(G)$ has $p$ distinct Sylow $q$-subgroups. It follows that $q|p-1$. Since $q|t_q - 1 = pr - 1 = (p-1)r + (r-1)$, we conclude that $q|r-1$. Since $p|r-1$ by (6), we get $pq|r-1$, so $r > pq = t_r$, a contradiction. It follows that $N$ can not be abelian. Thus $Q$ is not normal in $N$, which is only possible if $q > p$ and $p|q-1$.

(8) $p = 2$, $q = 3$, $r = 5$.

To justify this consider the normalizer $N$ of a Sylow $p$-subgroup $P$ of $G$. We have $|N| = p^2q$. Let $S$ be a Sylow $q$-subgroup of $N$. If $S$ was normal in $N$, then $N$ would be the normalizer of $S$ in $G$ and $t_q = r$, which is false by (7). Thus $S$ is not normal in $N$ and therefore $N$ has either $p$ or $p^2$ Sylow $q$-subgroups. As $q > p$ by (7), the former is not possible and $N$ has $p^2$ Sylow $q$-subgroups. Thus $q|p^2 - 1 = (p-1)(p+1)$. As $q > p$, we conclude that $q|p+1$ and $q = p+1$. This is only possible if $p = 2$ and $q = 3$. Since $r|t_r - 1 = pq - 1 = 5$, we conclude that $r = 5$.

This means that $G$ is a simple group of order 60, hence $G \cong A_5$.