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 $q - 1$. It is a well known result of elementary number theory that $\mathbb{F}_q^\times$ is cyclic (existence of primitive roots). We will prove this result later, when we discuss fields.

Since the order of $\mathrm{Aut}C_q$ equals $q - 1$, ϕ 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 ϕ is not trivial. Then ϕ is injective. Since $\mathrm{Aut}C_q$ is cyclic, it has unique subgroup $< f >$ of order p, which then coincides with the image of ϕ. 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 ϕ 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 for which $q - 1$ is the smallest positive integer k such that $q | i^k$ (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 $144 > 120 = 5! \geq k!$, π 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 ≤ 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, π 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 π establishes an isomorphism between G and A_5.

(2) It remains to show that G has a subgroup of index ≤ 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 ≤ 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 49 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. $C_G(B) < N_G(Q) = H$. This however contradicts (2), where we showed that $|N_G(Q)| = 7 \cdot 13$.

Cyclic, abelian, and nilpotent numbers

We say that a positive integer n is **cyclic** (**abelian**, **nilpotent**) if every group of order n is cyclic (resp. abelian, nilpotent). It is our goal now to give an explicit description of such numbers.

Our main tool is the following

Proposition 1. *Let G be a finite group such that every proper subgroup of G is nilpotent. Then G is not simple.*

Before we prove this result let us recall some basic facts about nilpotent groups which are given as problems in 3rd and 4th assignments.

(i) A finite group is nilpotent iff it is a direct product of its Sylow subgroups (i.e. all Sylow subgroups are normal).

(ii) If Q is a proper subgroup of a $p-$group P then Q is a proper subgroup of $N_P(Q)$ (i.e. $N_P(Q)$ is strictly larger than Q). By the above characterization of nilpotent groups the same remains true for a proper subgroup of a nilpotent group (prove it!).

(iii) Subgroups and quotient groups of nilpotent groups are nilpotent.

Proof of Proposition 1: Consider a group G with all proper subgroups nilpotent and suppose that it is simple.

We show that any two maximal subgroups of G have trivial intersection. In fact, let H_1, H_2 be maximal subgroups such that $B = H_1 \cap H_2$ has largest possible order. Suppose that B is not trivial. Thus $N_G(B)$ is a proper subgroup of G, hence it is contained in a maximal subgroup H_3. Since H_i are nilpotent, we see that

$$H_3 \supseteq N_G(B) \supseteq N_{H_i}(B) \supsetneq B$$

for $i = 1, 2$ (the first two inclusions are obvious and the third follows from (ii)). It follows that $H_3 \cap H_i$ has more elements than B for $i = 1, 2$. By the definition of B we see that $H_3 = H_i$ for $i = 1, 2$, i.e. $H_1 = H_2$, a contradiction.

Let $\mathcal{M}$ be the set of all maximal subgroups of G. Each non trivial element belongs to exactly one maximal subgroup. Thus, $|G| - 1 = \sum_{H \in \mathcal{M}} (|H| - 1)$. The group G acts on $\mathcal{M}$ by conjugation. If $H \in \mathcal{M}$, then $N_G(H) = H$ (since the normalizer is a proper subgroup which contains H). Thus the orbit of H contains $|G|/|H|$ elements. Let $O_1, ..., O_s$ be the orbits of the action of G on $\mathcal{M}$ and chose $H_i \in O_i$. Thus

$$|G| - 1 = \sum_{i=1}^{s} (|G|/|H_i|)(H_i - 1) = |G| \sum_{i=1}^{s} (1 - |H_i|^{-1}).$$

It follows that $\sum_{i=1}^{s} (1 - |H_i|^{-1}) = 1 - |G|^{-1} < 1$. Since $1 - |H_i|^{-1} \geq 1/2$ for all i, we see that $s = 1$ and $|H_1| = |G|$. Thus $G = H_1$, a contradiction. $\square$

Exercise. Show that G in the proposition is solvable

Here is another result we need:

Proposition 2. *Let P be a $p-$group of order p^n. If q is a prime divisor of $|\mathrm{Aut}P|$ then $q | p(p-1)(p^2-1)...(p^n-1)$.*

Proof: Suppose that $q||\mathrm{Aut}P|$ for some prime $q \neq p$. Thus $\mathrm{Aut}P$ has an element f of order q. Let $C =< f >$ be the cyclic subgroup of $\mathrm{Aut}P$ generated by f and $\phi : C \longrightarrow \mathrm{Aut}P$ the inclusion. Consider the semidirect product $G = P \rtimes_\phi C$. Note that C is a Sylow $q-$subgroup of G. Let t_q be the number of Sylow $q-$subgroups in G. Since f is nontrivial, C is not normal in G, i.e. $t_q > 1$. By Sylow's theorem, $t_q | p^n$ so $t_q = p^i$ for some $1 \leq i \leq n$. Moreover, $q | (t_q - 1) = (p^i - 1)$. It follows that $q | p(p-1)(p^2-1)...(p^n-1)$. $\square$

Remark. A different technique allows to prove a stronger result. Namely, let Φ be the Frattini subgroup of P. Then there is a natural homomorphism $\mathrm{Aut}P \longrightarrow$

$\mathrm{Aut}P/\Phi$. It turns out that the kernel of this homomorphism os a $p-$group. Now, P/Φ is an abelian group of exponent p and order p^i for some $1 \leq i \leq n$. Thus P/Φ can be thought of as a vector space of dimension i over the field with $p-$elements. It follows that $\mathrm{Aut}P/\Phi \simeq GL_i(\mathbb{F}_p)$, so $|\mathrm{Aut}P/\Phi| = p^{i(i-1)/2}(p-1)...(p^i-1)$.

Exercise. Let G be a nilpotent group, so that $G = P_1 \times ... \times P_s$, P_i a Sylow subgroup of G. Show that $\mathrm{Aut}G \simeq \mathrm{Aut}P_1 \times ... \times \mathrm{Aut}P_s$.

Corollary 1. *Let G be a nilpotent group of order $n = p_1^{a_1}...p_s^{a_s}$. If $q||AutG|$ then $q|m_1...m_s$, where $m_i = p_i(p_i-1)...(p_i^{a_i}-1)$*

Proof: This follows directly from Proposition 2 and the above exercise.

Theorem 2. *Let $n = p_1^{a_1}p_2^{a_2}...p_k^{a_k}$, where $p_1 < p_2 < ... < p_k$ are primes and $a_i > 0$ for all i.*

(1) *n is nilpotent iff it has the following property*

$$p_i \nmid (p_j - 1)(p_j^2 - 1)...(p_j^{a_j} - 1) \text{ for all } i, j \quad (*)$$

(2) *n is abelian iff n satisfies (*) and $1 \leq a_i \leq 2$ for all i.*

(3) *n is cyclic iff n satisfies (*) and $a_i = 1$ for all i, i.e. $(n, \phi(n)) = 1$, where ϕ is the Euler function.*

Proof: We first prove that the conditions on n are sufficient. Suppose that that G is a group of smallest possible order which is not nilpotent and such that $|G|$ satisfies (*).

Note that if n satisfies (*) then every divisor of n also satisfies (*). Thus every proper subgroup of G is nilpotent, hence $|G|$ is not simple. Let K be a proper nontrivial normal subgroup of G. Since K is nilpotent, it has a normal nontrivial Sylow $p-$subgroup H for some prime p. Since $|G/H|$ is a proper divisor of $|G|$, it satisfies (*) and it is smaller than $|G|$. It follows that both G/H is nilpotent. In particular, it has a normal Sylow $p-$subgroup. The preimage of this subgroup in G is a normal Sylow $p-$subgroup P of G. Let A be a normal subgroup of G of largest possible order among the normal subgroups which are direct products of Sylow subgroups of G. If $A = G$ then G is nilpotent and we are done. Suppose that A is a proper subgroup. Then G/A is nilpotent and $(|A|, |G|/|A|) = 1$. Let

$\pi : G \longrightarrow G/A$ be the projection. Let q be a prime divisor of $|G|/|A|$ and Q a Sylow $q-$subgroup of G. Then $\pi(Q)$ is a Sylow $q-$subgroup of G/A, hence it is normal. By the correspondence theorem, $B = AQ$ is a normal subgroup of G. Since $A \cap Q = \{1\}$, B is a semidirect product $B = A \rtimes_\phi Q$. By Corollary 1 and the condition (*), we have $q \nmid |\mathrm{Aut}A$. Thus ϕ has to be trivial, so $B = A \times Q$. This contradicts our choice of A. Thus G can not exist.

Suppose now that $|G|$ satisfies (*), so G is nilpotent. Let P_i be the Sylow p_i-subgroup of G, so $G = P_1 \times P_2 ... \times P_k$ by (i). If $1 \leq a_i \leq 2$ for all i then P_i is abelian for all i, hence G is abelian. If furthermore $a_i = 1$ for all i, then P_i is cyclic for all i and G is cyclic (why?).

Now we show that the conditions on $|G|$ are necessary. Suppose that n does not satisfy (*) so there are i, j such that $p_i|(p_j - 1)(p_j^2 - 1)...(p_j^{a_j} - 1)$. Note that $i \neq j$. Let $m = n/p_i^{a_i} p_j^{a_j}$. Note that the number $p^{(a_j-1)a_j/2}(p_j - 1)(p_j^2 - 1)...(p_j^{a_j} - 1)$ is the order of $GL_{a_j}(\mathbb{F}_{p_j})$. It follows that $\mathbb{F}_{p_j}^{a_j}$ has an automorphism f of order p_i. But as a group, $H = \mathbb{F}_{p_j}^{a_j}$ is a direct product of a_j copies of the cyclic group of order p_j and f is an automorphism of H of order p_i. Let C be the cyclic group of order $p_i^{a^i}$ and choose a generator g of C. We have an homomorphism $\phi : C \longrightarrow \mathrm{Aut}H$ defined by $\phi(g) = f$. Consider the group $B = H \rtimes_\phi C$. It has order $p_i^{a_i} p_j^{a_j}$. Note that C is the Sylow p_i-subgroup of B, but it is not normal. In fact, if $a \in H$ is such that $f(a) \neq a$, then $aga^{-1} = (af(a)^{-1})g \notin C$. Thus B is not nilpotent. Let C_m be the cyclic group of order m. The group $G = B \times C_m$ has order n and is not nilpotent.

Suppose now that n satisfies (*) but $a_i \geq 3$ for some i. Set $m = n/p_i^3$. We use the fact that for every prime p there is a nonabelian group of order p_3 (use the fact the direct product of two copies of the cyclic group of order p has an automorphism of order p). Let P be a nonabelian group of order p_i^3 and let C_m be the cyclic group of order m. Then $G = P \times C_m$ has order n and is nonabelian.

Finally, suppose that n satisfies (*) but $a_i > 1$ for some i. Set $m = n/p_i^2$. The group $G = C_{p_i} \times C_{p_i} \times C_m$ is not cyclic. $\square$