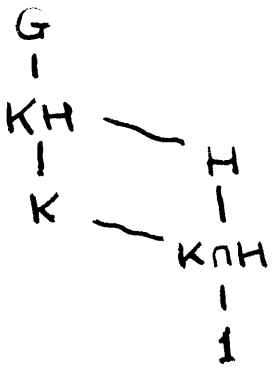
Groups

Paul Taylor
Trinity College
January 1984

1. Revision

This course is concerned with the basic properties of finite abstract groups. Groups should always be seen as acting on something, if necessary themselves: the Representation Theory course dealt with abstract linear representations begining with a space whose basis was the group itself, and for the proof of Sylow's theorems we shall consider permutation representations begining with the underlying set of the group.

Recall the definitions of group, group homomorphism, subgroup, normal subgroup, kernel, quotient, image, direct product, subgroup generated by a subset, etc. Also the basic result that for any homomorphism $\theta : G \to H$ we have $G/\ker\theta \cong \mathrm{im}\theta \leq H$ (first isomorphism theorem). Then if $N, M \trianglelefteq G$ with $N \leq M$ then $M/N \trianglelefteq G/N$ and $G/M \cong (G/N)/(M/N)$ (second isom. thm); indeed the normal subgroups of G/N are exactly of the form M/N. Now define [non-standard] a <u>parallelogram</u> of groups to be a diagram of inclusions of subgroups:



$K \trianglelefteq KH \leq G$

where $K \trianglelefteq G$. Then $K \cap H \trianglelefteq H$ and and the quotients, KH/K and $H/K\cap H$, are isomorphic (third isom. thm).

A subgroup $K \leq G$ is <u>characteristic</u> [non-standard notation: $K \trianglelefteq G$] if for every automorphism $\alpha : G \cong G$, $K\alpha = K$. Thus K is defined in a way which depends only on the *abstract* group structure of G and not on how it acts or on named elements of it. Then $1, G \trianglelefteq G$; $H \trianglelefteq K \trianglelefteq G \Rightarrow H \trianglelefteq G$ (unlike normality) and $H \trianglelefteq K \trianglelefteq G \Rightarrow H \trianglelefteq G$. Examples include $Z(G)$, G' and

any normal Sylow subgroup. A group is said to be characteristically simple if $1, G$ are its only characteristic subgroups; this occurs iff G is a direct power of a simple group. A characteristically simple Abelian group is called elementary Abelian.

2. Permutation actions

An action of a group G on a set X is a function $\alpha: X \times G \to X$ such that $(x,1)\alpha = x$ and $((x,g)\alpha, h)\alpha = (x,gh)\alpha$ for all $x \in X$; $g,h \in G$. This defines a homomorphism $\bar{\alpha}: G \to \mathrm{Symm}(X)$ in the obvious way. An action is faithful if $\bar{\alpha}$ is injective and transitive if $\forall x,y \in X \; \exists g \in G : (x,g)\alpha = y$. We usually write xg for $(x,g)\alpha$. The orbit of $x \in X$ is $xG = \{xg : g \in G\}$ and the stabiliser is $\mathrm{Stab}_G(x) = \{g \in G : xg = x\}$. G acts transitively iff the orbit of a given point is the whole set, and x is a fixed point if $\mathrm{Stab}_G(x) = G$. Some care should be taken when refering to the stabiliser of a subset: for $A \subseteq X$, $\mathrm{Stab}_G(A) = \{g \in G : ag \in A \; \forall a \in A\}$.

There is a direct correspondence between stabilisers of points in a permutation action and subgroups of a group. Clearly $\mathrm{Stab}_G(x) \leq G$, but also if $H \leq G$ consider the permutation action of G on the right cosets of H by right multiplication, then $H = \mathrm{Stab}_G(H)$. Thus we have Lagrange's theorem: $|xG| = |G : \mathrm{Stab}_G(x)|$. Other points in the orbit correspond to conjugates of the subgroup: if $xg = y$ then $g^{-1}\mathrm{Stab}_G(x)\,g = \mathrm{Stab}_G(y)$.

When a group acts on itself by conjugation, the stabiliser of a subset X is called its normaliser:

$$N_G(X) = \{g : g^{-1}xg \in X \;\; \forall x \in X\}$$

This must not be confused with the centraliser:

$$C_G(X) = \{g : g^{-1}xg = x \;\; \forall x \in X\}$$

which is the kernel of the action of $N_G(X)$ on X, so $C_G(X) \trianglelefteq N_G(X)$. $|G : N_G(X)|$ is the number of conjugates of X in G. If $H \leq G$, $H \trianglelefteq N_G(H)$; moreover if $H \trianglelefteq J \leq G$ then $J \leq N_G(H)$.

Finally, if $H \leq G$ with $|G:H| = n$ then there's $K \trianglelefteq G$ with $K \leq H \leq G$ and $|G:K| \mid n!$ (in fact $G/K \leq S_n$).

3. Sylow subgroups and p-groups

Let G be a finite group of order $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$; then a Sylow p_i-subgroup of G is a subgroup of order $p_i^{\alpha_i}$. Sylow's theorems state that

(i) Sylow p-subgroups exist for each p
(ii) any two Sylow p-subgroups are conjugate
(iii) the number of them is congruent to 1 mod p.

Of course, given (i) and (ii), the number of Sylow p-subgroups is $|G : N_G(Syp)|$, where Syp is any such subgroup, and hence divides $|G|$. In view of (iii) it must divide $|G : Syp|$, but this is clear anyway since $Syp \leq N_G(Syp) \leq G$. This places strong restrictions on the possible structures of groups. Observe also that if there is only one Sylow p-subgroup then it is normal (and in fact characteristic).

A group of order p^α is called a p-group. From the class equation, the centre of such a group must be nontrivial. Hence there is a series

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$$

~~in which each G_{i+1}/G_i is characteristically simple (and hence a power of the cyclic group C_p)~~, given by $G_{i+1}/G_i \cong Z(G/G_i)$. This is called the upper central series and we shall be studying it in more detail later. We may immediately conclude that there are subgroups of order p^i, $0 \leq i \leq \alpha$, with $p^i \trianglelefteq p^{i+1}$.

Of course it follows immediately that if $p \mid |G|$ then G has an element of order p: [Exercise] Prove this directly.

4. First Sylow theorem

Let S be the set of subsets of G of order p^α (where $|G| = p^\alpha m$ and $p \nmid m$) and let G act on S by right multiplication, so $\tilde{g} : X \mapsto \{xg : x \in X\}$. Exercise: show that $p \nmid |S|$, so that there is some orbit $S_0 \subseteq S$ with $p \nmid |S_0|$. Now consider the (transitive) permutation action of G on S_0, and choose $X \in S_0$ and $H = \mathrm{Stab}_G(X)$.

Now since G acts transitively on S_0 (this being an orbit), $|G:H| = |S_0|$, so $p^\alpha \mid |H|$. But $H \hookrightarrow X$ by $h \mapsto xh$ (for some arbitrary $x \in X$) so $|H| \leq |K| = p^\alpha$ and H is a Sylow p-subgroup of G.

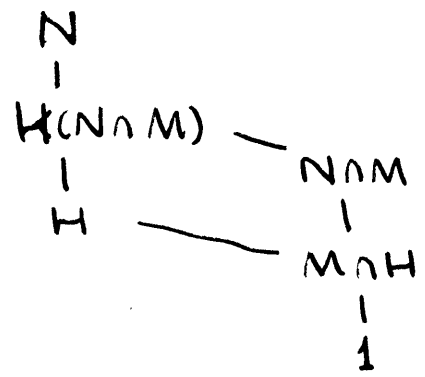
Now let K be another such subgroup. Consider its action on S_0 (ie the restriction to K of the action of G). Since $p \nmid |S_0|$, there's some orbit $S_1 \subseteq S_0$ with $p \nmid |S_1|$. Let $Y \in S_1$ and consider $\mathrm{Stab}_K(Y)$. Clearly $p \nmid |S_1| = |K : \mathrm{Stab}_K(Y)|$ so (since K is a p-group) $\mathrm{Stab}_K(Y) = K$ and $S_1 = \{Y\}$. But as before, $|\mathrm{Stab}_G(Y)| = p^\alpha = |K|$, so $K = \mathrm{Stab}_G(Y)$. Thus by §2, since X, Y are in the same orbit under G, H, K are conjugate.

5. Third Sylow Theorem

Let $\mathcal{P}$ be the set of Sylow p-subgroups of G (which is nonempty) with the (transitive) conjugation action of G. Let $H \in \mathcal{P}$ and $N = N_G(H)$, so $H \trianglelefteq N \leq G$. Consider the action of N on $\mathcal{P} \setminus \{H\}$; it suffices to show that the sizes of the orbits are divisible by p.

Let $K \in \mathcal{P} \setminus \{H\}$ and $M = N_G(K)$. Observe that K is a normal Sylow subgroup of M and hence the only one, so $H \notin M$, ie $M \cap H \neq H$. The size of the orbit of K under N is $|N : N \cap M|$. Its easy to see that M, N are conjugate.

Now we have a parallelogram of subgroups of N:



so $H(N \cap M)/H \cong (N \cap M)/(M \cap H)$, whence $|H : M \cap H| \mid |N : N \cap M|$. But $|H : M \cap H| \neq 1$ and is a p-power, so $p \mid |N : N \cap M|$ and the result follows.

This result is extremely powerful for finding the structure

of finite groups given their order. For instance a group of order $p^a m$ where $m < p$ must have a normal subgroup of order p^a. Since the Sylow p-subgroups account for all of the elements of p-power order and must intersect in p-power subgroups, element-counting arguments frequently give valuable information as regards the number of Sylow subgroups.

The conjugation action on the Sylow subgroups may afford convenient permutation representations of groups. For instance the least permutation representation of $GL(3,2)$ is that on the seven Sylow 3-subgroups. From this it is easy to show that this is the unique simple group of this order, $168 = 2^3.3.7$. Element-counting arguments suffice (with some labour) to show that the only simple group of lower order is A_5, of order 60.

A_n is simple for $n \neq 4$. Proofs of this will be found in [MacDonald 1968] pp. 220-1, [Stewart]

7. Series of subgroups within groups.

A series (or normal series) is a chain

$$1 = G_0 \leq G_1 \leq G_2 \leq \ldots \leq G_n = G$$

with $G_i \trianglelefteq G_{i+1}$. It is said to be invariant if also $G_i \trianglelefteq G$ for each i. One series is said to be a refinement of another if the second is obtained by deleting some of the intermediate terms of the first; a maximally refined series is called a composition series and a maximally refined invariant series is called a chief series. Two series are similar if they have the same quotients G_{i+1}/G_i up to isomorphism: note that we reckon the set of quotient groups *with multiplicities*. The quotients in a composition or chief series are called composition factors and chief factors respectively. [Exercise: show that composition (chief) factors must be (characteristically) simple groups]

The Jordan-Hölder theorem, which will be proved in the next section, states that any two (invariant) series have similar (invariant) refinements. Hence we may speak unambiguously of *the* composition (chief) factors of a group. This shows some of the importance of classifying finite simple groups, although the composition factors of a group do not determine it up to isomorphism. A finite Abelian group is, however, determined by its chief factors.

A group is said to be <u>soluble</u> if it has a series with Abelian factors, so a finite group is soluble iff its composition factors are cyclic. The original source of interest was in Galois theory, which explains the name. The class of soluble groups may be characterised as the closure of the Abelian groups under <u>extension</u>, so $G \in \mathfrak{C}$ whenever $N, G/N \in \mathfrak{C}$ for some $N \trianglelefteq G$. The "fastest descending" series with Abelian factors is the <u>derived series</u>:

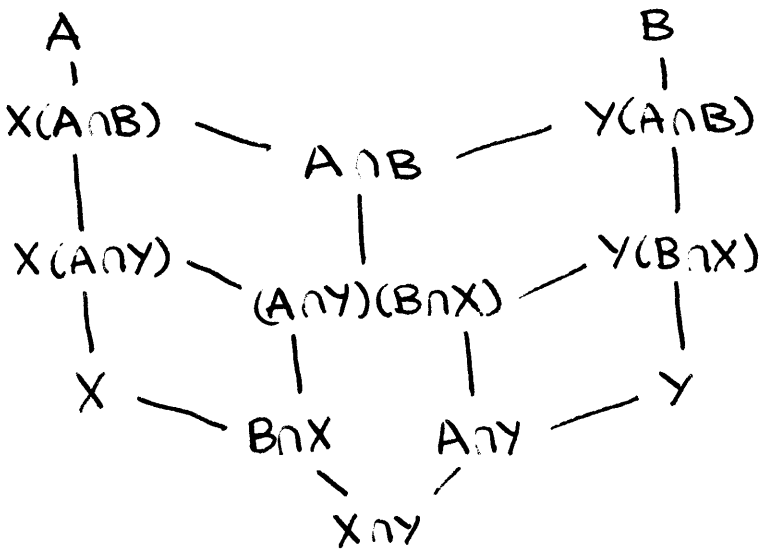
$$G \trianglerighteq G' \trianglerighteq G'' \trianglerighteq \cdots$$

where $G^{(r+1)} = \langle [x,y] : x,y \in G^{(r)} \rangle$, in the sense that if G_i is the i^{th} term from the top of a series with Abelian factors then $G^{(i)} \leq G_i$. Thus if a group has any series with Abelian factors then it has an invariant one.

A <u>central series</u> is an invariant series $1 = G_0 \leq G_1 \leq G_2 \leq \ldots$ with $G_{i+1}/G_i \leq Z(G/G_i)$ and $G = G_r$ for some r. A group possessing a central series is called <u>nilpotent</u> and is clearly soluble. By means of the upper central series we've already seen that any finite p-group is nilpotent and [<u>exercise</u>] any subgroup, product or quotient of nilpotent groups is nilpotent; we shall show that every finite nilpotent group is in fact a direct product of p-groups. If (G_i) is a central series with $G_r = G$ then $\gamma_{r-i}(G) \leq G_i \leq Z_i(G)$ where $\gamma_0(G) = G$, $\gamma_{i+1}(G) = \langle [x,y] : x \in G, y \in \gamma_i(G) \rangle$ defines the <u>lower central series</u>. Thus the upper and lower central series have the same length, which is called the <u>nilpotency class</u> of G; it is the shortest possible length of a central series for G.

8. Zassenhaus' lemma and the Jordan-Hölder theorem.

Let $A, B \leq G$ and $X \trianglelefteq A$, $Y \trianglelefteq B$. Consider the diagram of subgroups, whose cells are parallelograms:



This having been verified, it follows that

$$X(A\cap B)/X(A\cap Y) \cong Y(A\cap B)/Y(B\cap X)$$

which is known as Zassenhaus' lemma or the fourth isomorphism theorem.

Let

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_i \trianglelefteq \ldots \trianglelefteq G_m = G$$
$$1 = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_j \trianglelefteq \ldots \trianglelefteq H_n = G$$

be two series for a group G. We shall refine these to

$$1 = G_0 \trianglelefteq \ldots \trianglelefteq G_{i-1,n} = G_i = G_{i,0} \trianglelefteq \ldots \trianglelefteq G_{i,j} \trianglelefteq \ldots \trianglelefteq G_{i,m} = G_{i+1} \trianglelefteq \ldots G$$
$$1 = H_0 \trianglelefteq \ldots \trianglelefteq H_{j-1,m} = H_j = H_{j,0} \trianglelefteq \ldots \trianglelefteq H_{j,i} \trianglelefteq \ldots \trianglelefteq H_{j,m} = H_{j+1} \trianglelefteq \ldots G$$

where $G_{ij} = G_i(G_{i+1}\cap H_j)$ and $H_{ji} = H_j(H_{j+1}\cap G_i)$. Thus with $X = G_i \trianglelefteq A = G_{i+1}$ and $Y = H_{j-1} \trianglelefteq B = H_j$ we apply the lemma to get

$$G_{i,j}/G_{i,j-1} = \frac{G_i(G_{i+1}\cap H_j)}{G_i(G_{i+1}\cap H_{j-1})} \cong \frac{H_{j-1}(H_j\cap G_i)}{H_{j-1}(H_j\cap G_{i-1})} = H_{j-1,i}/H_{j-1,i-1}$$

so that the refinements are indeed similar.

9. Nilpotent groups

We shall only go as far into the rich theory of nilpotent groups as to classify the finite ones as products of p-groups. This is easily seen to be equivalent to showing that all the Sylow subgroups are normal. Observe that a group is nilpotent iff all its quotients (except 1) have nontrivial centre.

In general, if P, Q are (normal) Sylow p,q-subgroups resp. then they commute pointwise. For if $x \in P$, $y \in Q$ then $[x,y] \cdot P \cap Q = 1$ because the order must divide both p^α and q^β. Also, the normaliser of a Sylow subgroup $H \leq G$ of any finite group is self-normalising, ie $N_G(N_G(H)) = N_G(H)$, so the following lemma is now sufficient to characterise nilpotent groups.

A proper subgroup of a nilpotent group is also a proper subgroup of its normaliser. For if $1 = G_0 \leq \dots \leq G_r = G$ is the (lower) central series (so $G_{i-1} = \langle [x,y] : x \in G \ y \in G_i \rangle$) then for some $0 \leq k \leq r-1$, $G_k \leq H$ but $G_{k+1} \not\leq H$ since $1 = G_0 \leq H$ and $G = G_r \not\leq H$. Then $[G_{k+1}, G] = G_k \leq H$ so $[G_{k+1}, H] \leq H$, ie G_{k+1} normalises H and $H \cup G_{k+1} \leq N_G(H)$. But by the choice of k, $G_{k+1} \not\leq H$, so $H < N_G(H)$.

It follows that a finite group is nilpotent iff every maximal subgroup is normal. For if $M < G$ is maximal, $N_G(M) = G$ by the above lemma. Conversely, if H is a non-normal Sylow subgroup, let $N_G(H) \leq M < G$ with M maximal, so $N_G(M) \leq N_G(N_G(H)) = N_G(H) < G$ and M is not normal.

Another characterisation of finite nilpotent groups is that elements of coprime order commute. This is because of the general result that elements (and indeed subgroups) of p-power order are contained in Sylow p-subgroups. It is in fact true that in any nilpotent group elements of finite coprime order commute, but the proof of this is outside the scope of the course.

10. Hall subgroups.

Lagrange's theorem states that the order of a subgroup divides the order of the group, and Sylow's theorem provides subgroups of all possible prime-power

orders, so it is natural to ask for what other orders subgroups must exist. We shall answer this question for soluble groups and subgroups whose order and index are coprime, ie $|H| = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ and $|G| = p_1^{\alpha_1} \dots p_k^{\alpha_k} p_{k+1}^{\alpha_{k+1}} \dots p_r^{\alpha_r}$ ($p_1, \dots, p_r$ being distinct primes). A Hall subgroup is one whose order and index are coprime. We shall show that a group is soluble iff it has Hall subgroups of all possible orders.

~~In order to show the existence of Hall subgroups for soluble groups it will suffice to find Sylow complements, ie subgroups of order m where $|G| = p^\alpha m$ and $p \nmid m$.~~

As with Sylow subgroups, any two Hall subgroups (of the same order) of a finite soluble group are conjugate; also, any subgroup of order $p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ is contained in a Hall subgroup of order $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. The proof will of course be by induction on the order of the group and is based on the existence of nontrivial normal subgroups since there's nothing to prove in the case of a cyclic group. Two cases arise, which will be dealt with in the next two sections:

(i) G has a normal subgroup K of order $m_1 n_1$, where $|G| = mn$, $m_1 | m$, $n_1 | n$ and $n_1 < n$

(ii) every nontrivial normal subgroup has order divisible by n.

11 Hall subgroups: case (i)

By the induction hypothesis, G/K is soluble and has a Hall subgroup S/K of order m/m_1. Again by induction $S < G$ has a Hall subgroup H of order m. Now $|H \cap K| \leq m_1$, whilst $|HK| \mid mn$, so $m_1 \mid |H \cap K|$, so $|H \cap K| = m_1$. Then HK/K is a Hall subgroup of G/K, so again by induction it's conjugate to $H'K/K$ where H' is another Hall subgroup of G. So

$$H'K = x^{-1} HK x$$

for some $x \in G$. Then $x^{-1}Hx$ and H' are Hall subgroups of $H'K < G$ so, by induction, conjugate:

$$H' = y^{-1} x^{-1} H x y$$

Finally, let J be an arbitrary subgroup of order dividing

m. Then $JK/K \leq G/K$ has order dividing m/m_1 and so by induction is contained in a Hall subgroup S/K. Finally applying the induction hypothesis to S, J is contained in a Hall subgroup of it and hence of G.

12. Hall subgroups: case (ii)

Let K be a minimal normal subgroup of G and hence characteristically simple. It's therefore an elementary Abelian p-group. On the other hand its order is divisible by n, so it's a normal and hence characteristic Sylow subgroup, and is contained in every nontrivial normal subgroup. Let $n = p^\alpha$. In fact if G is any group with a normal subgroup K such that G/K and K have coprime orders m, n, resp. then G has a subgroup of order m [MacDonald 1968 pp 139-142].

Let L/K be a minimal normal subgroup of G/K; since the latter is soluble, L/K will be elementary Abelian so $|L| = p^\alpha q^\beta$. Let $Q \leq L$ be a Sylow q-subgroup, so $L = KQ$. Now $G = L N_G(Q)$ since $Q \leq L \trianglelefteq G$, for $g^{-1}Qg \leq L$ so $g^{-1}Qg = l^{-1}Ql$ (for some $l \in L$ by Sylow's second theorem) and $l^{-1}g \in N_G(Q)$; so $G = LN_G(Q) = KQN_G(Q) = KN_G(Q)$. We shall show that $K \cap N_G(Q) = 1$ so $|N_G(Q)| = |G/K| = m$ as required.

Put $D = K \cap N_G(Q) \trianglelefteq N_G(Q)$, since $K \trianglelefteq G$; also $D \trianglelefteq K$ since K is Abelian, so $D \trianglelefteq KN_G(Q) = G$. But $K \trianglelefteq G$ is minimal so unless $K \leq N_G(Q)$ (whence $N_G(Q) = G$ and $Q \trianglelefteq G$, $\#$ to hypothesis of case (ii)), $D = 1$.

Let $H, H' \leq G$ with $|H| = |H'| = m$. Then $G = HL = H'L$ since $|HL|, |H'L| \geq mn$; also $G/L \cong H/(H \cap L) \cong H'/(H' \cap L)$, so $|H \cap L| = |H' \cap L| = q^\beta$. But then $H \cap L$, $H' \cap L$ are conjugate in L to Q and their normalisers in G have order m. Now $H \cap L \trianglelefteq H$ so $H \leq N_G(H \cap L)$, whence $H = N_G(H \cap L)$ which is conjugate to $N_G(Q)$ and hence to $N_G(H' \cap L) = H'$.

Now let $S \leq G$ with $m' = |S| | m$, say $m' < m$. Then $|SK| = m' p^\alpha < |G|$ and we may apply the inductive hypothesis to the soluble group SK. For $(|G:H|, |G:SK|) = 1$ so $|G: H \cap SK| = |G:H||G:SK| = mn/m'$ and so S, $H \cap SK$ are Hall subgroups of SK and hence conjugate. Then S lies in a conjugate of the Hall subgroup $H = N_G(Q)$.

12. Converse of Hall's theorem.

That the existence of all Hall subgroups of a finite group entails its solubility relies on Burnside's $p^\alpha q^\beta$ theorem, that a group of such order is soluble; a proof of this will be found in Representation Theory. This result provides the foundation of an induction on the number of prime divisors of $|G|$, which we may therefore assume to be at least 3, so let $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ and $S_1, S_2, \dots, S_k \leq G$ with $|G:S_i| = p_i^{\alpha_i}$. This is a <u>system of Sylow complements</u>.

Observe that $\{S_i \cap S_j : i \neq j\}$ affords a system for S_i, so that by induction each S_i is soluble. Let $N \lhd S_1$ be minimal, $p = p_1$, $\alpha = \alpha_1$, $\beta = \alpha_2$, $q = q_2$, $|N| = q^b$. Consider $S_1 \cap S_3$: $|G : S_1 \cap S_3| = p^\alpha p_3^{\alpha_3}$ so $\exists\, Q \leq S_1 \cap S_3$ with $|Q| = q^\beta$. Then $N \leq Q$ since N is contained in some (and hence, being normal, every) Sylow q-subgroup of S_1.
Claim $1 < M = \langle N^g : g \in G \rangle \lhd G$ whence G is soluble.

for considering orders, it's clear that $G = S_1 S_3$. Then if $g = s_1 s_3$ (with $s_1 \in S_1$, $s_3 \in S_3$), $N^g = (N^{s_1})^{s_3} = N^{s_3}$ since $N \lhd S_1$. But $N \leq Q \leq S_1 \cap S_3 \leq S_3$ so $N^{s_3} \leq S_3$ and $M \leq S_3$ (in fact $M \trianglelefteq S_3$).