SOLVABLE GROUPS - A NUMERICAL APPROACH

THANOS GENTIMIS

ABSTRACT. We give all definitions related to solvable groups and show that any group of order up to 100 and not 60 is solvable.

1. Introduction

Naturally all the papers and presentations start by exemplifying the importance of their topics, their various applications. Most of the times a connection to a Fields medal is constructed (like if that matters). Famous quotes and names are referred and generally people try to justify their work right from the very start.

This paper has a totally different approach. NOPE! you cannot use this material to prove big theorems. It has nothing to do with the one million dollars problems. Some of the computations are absolutely boring. The applications are relatively limited and the results are confined in this field only.[1]

Then why even bother? Because it is so darn beautiful to find easy ways in thought-provoking problems that can be stated so simply and are so difficult to solve immediately. I just couldn't resist.[2] It is more productive to give a presentation to people when you are talking about easy stuff.(You can move your hands fast and this time people DO believe you right away!)

To sum up the only application I could think of would be related to Galois theory but I am not that smart and my poor mathematical background doesn't help me make the connection.

2. Preliminaries

What is the worst way to start a presentation? Throw at them a bunch of definitions, confuse them with some properties and put a few examples without going over the details. Well that is exactly how I will start!

For my first trick I will call upon the might of series! Generally in group theory when we want information about a group we break it up into smaller subgroups and their quotients and study their properties. General ideas used are those of series and induction.

Definition 1. *Let G be a finite group. A series in G is just a collection of subgroups of G with the property:*

$$\{e\} = H_0 \leq H_1 \leq H_2 \leq ... \leq H_n = G$$

Date: November 27, 2006.

[1] If I was not the author I would think that It was a bad idea to attend!

[2] That and the fact that it is really easy to talk about this things!!!

Definition 2. *A series will be called finite if n in the above definition is finite. A series will be called normal if $H_i \trianglelefteq H_{i+1}$ for all $i = 0, 1, ..., n-1$.*

Ok some examples (without OF COURSE the details)

Example 1.

$$\{[0]\} \trianglelefteq\ <[8]>\ \trianglelefteq\ <[4]>\ \trianglelefteq\ <[2]>\ \trianglelefteq \mathbb{Z}_{16}$$

Is a normal finite series in $\mathbb{Z}_{16}$.

It is time to give the formal definition of a solvable group. Who made that up I really don't know. Lets say that it was common sense and don't worry about it now.

Definition 3. *A finite (or not[3]) group will be called Solvable if and only if it contains a normal series such that all the quotients are abelian groups.*

Another way to define a group to be solvable is the following.

Definition 4. *A group is said to be solvable if the derived series ends with $\{e\}$.*

Since I am not going to be talking about derived series you can just forget about the above definition.

Notice that we get immediately:

Remark. *Every abelian group is solvable. Since*

$$\{e\} \trianglelefteq G$$

is a good *series!*

So simple to state and difficult to compute even in small numbers sometimes. Pay attention to the following example. We will state it here (and we will even bother to prove it!) but in order to actually prove it we need a few more tricks up our sleave!

Basic Example. *If $|G| = p^k$ where p is prime and k is a natural number then G is solvable.*

Before we attempt to prove it lets state (without proof once more) the Sylow theorems and some interesting corollaries which will make our life easier.

Definition 5. *Let p be a prime number that divides the order of G. Let k be the biggest natural number such that p^k divides G. All the subgroups of G with order p^k are called p-Sylow subgroups of G. We denote their set to be Syl_pG and $\#Syl_pG = N_p$.*

1st Sylow Theorem. *If p is a prime number and p^s divides the order of G then G has at least one subgroup of order p^s.*

Especially for the case of p^k the theorem tells us that Syl_pG is non-empty.

2nd Sylow Theorem. *Every two p-Sylow subgroups of G are conjugate.*

This is not so useful for general computations but it might prove extremely useful in particular cases.

3rd Sylow Theorem. *N_p divides the order of G and it is equivalent to 1modp.*

[3] but we don't want to go there... believe me we DO NOT!

Also another good tool in this theory coming again as a consequence of Sylow's theorems is this:

4th Sylow theorem (Not exactly !). *If p divides the order of G and $n = N_p$ is the number of p-Sylow subgroups in G then there exists a homomorphism $\phi : G \to S_n$ with $Ker\phi \leq N_G(P)$ and n divides $Im\phi$.*

These theorems will prove valuable[4] (as all the counting theorems in finite group theory).

Lets add here three corollaries which are derived immediately by the theorems above.

Corollary 1. *If G has only one p-Sylow subgroup H then H is normal.*

Corollary 2. *If $H \trianglelefteq G$ and $|\frac{G}{H}| = p$ or p^2 then $\frac{G}{H}$ is abelian.*

Corollary 3. *The center $Z(G)$ of any group G of order p^k, with p prime is non-trivial. We call these groups p-groups.*

Now it is time to state a powerful inductive theorem-tool. Things that follow are too difficult to prove, so we will only write them down. [5]

3. Main Theorems

Theorem-Tool. *If G is a group and H is a normal subgroup of G such that H is solvable and G/H is solvable then G is solvable.*

I could comment on the proof but it is absolutely technical and nothing of value comes from it. Most of the papers that use it give references or leave it as a straightforward exercise for the reader[6]. One can definitely see the inductive character of this Tool-Theorem.

Time to turn back to our basic example and try to prove it. Lets give it the form of a theorem.

Theorem 1. *If $|G| = p^k$ where p is a prime number then G is solvable. In other words every p-group where p is a prime is solvable.*

Proof. By induction on k.

1st Step. For $k = 1$ our group is a cyclic group of prime order thus it is solvable by definition.

2nd step. Let the statement hold for all $n \leq k$.

3d Step. We will prove that it holds for $k = n + 1$. By corollary 3 since G is a p-group $Z(G) \neq \{e\}$. Also $Z(G)$ is a normal subgroup of G and $Z(G)$ is abelian. Thus $Z(G)$ is solvable. Now $G/Z(G)$ is again a p-group or trivial. If it is trivial then $G = Z(G)$ thus G is abelian hence it is solvable. If it is not trivial then $|G/Z(G)| \leq p^n$. So by the inductive step it is solvable. Using the tool theorem G is also solvable and we are done.

□

[4] Never underestimate a procedure that counts something! Mathematicians should be able to ... count!

[5] Famous familiar quote!

[6] They don't say it is easy so It might not even be true!!! Hehe fortunately it is and it can be found in books like Zassenhause's or Robinson's.

Theorem 2. *If $|G| = p^k q^s$ where p and q are prime numbers $k, s \in \mathbb{N}$ and $1 mod p \neq q^t$ for $t = 1, 2, .., s$ then G is solvable.*

Proof. Since N_p divides $|G|$ and it is equal to $1 mod p$ and since $q^t \neq 1 mod p$ for $t = 1, 2, .., s$ we get that $N_p = 1$. Let P be the only p-Sylow subgroup of G. P is a normal subgroup of G. Since the order of P is p^k where p is prime we have that P is a p-group and by our basic example-theorem P is solvable. Also $[G : P] = q^s$ thus $\frac{G}{P}$ is a q-group and again by our basic example-theorem $\frac{G}{P}$ is solvable. By the tool theorem, now G is solvable. □

Remark. *A weaker version of the theorem above is: If $|G| = pq$ where p and q are distinct prime numbers $(p < q)$ is solvable. This is exactly our previous theorem for $k = s = 1$*

A harder to prove but still true version of the theorem above is the Burnside theorem. We will not be using it (very much) but it is something I know and it is related to solvable groups thus we include it.

Theorem 3. ***(Burnside)*** *Any group of order $p^k \cdot q^s$ p,q primes is solvable.*

We are not going to use it because this is like a "tank" in this theory and we are only after small flies![7]

Theorem 4. *If $|G| = pqr$ where $p < q < r$ primes then G is solvable.*[8]

Proof. Since N_r divides the order of G and $N_r = 1 mod r$, N_r can either be 1 or qp[9].

Case a Let $N_r = 1$ then G has only one r-Sylow subgroup H which is normal cyclic of order r (thus solvable) and $|G/H| = qp$ which by the remark is solvable. From the tool-Theorem G is solvable.
Case b) If $N_r = p \cdot q$. We will show that this leads to contradiction.
• Consider N_q the number of q-Sylow subgroups. N_q divides $|G|$ and $N_q = 1$modq thus N_q can be 1, or $r \cdot p$, or r.
i) If $N_q = r \cdot p$ we get $r \cdot p \cdot (q - 1)$ elements of order q living inside the rp different q-Sylow subgroups. Consider also the $p \cdot q \cdot (r - 1)$ elements of order p living inside the pq different r-Sylow subgroups and thus we have:

$$pqr - pq + rpq - rp = pqr + p(rq - q - r)$$

elements inside G.
• But since $p \geq 2$ we have that $q > 2 (\Rightarrow q - 1 > 1)$ and since $r > q$ we get:

$$rq - q - r = (q - 1)r - q > r - q > 0$$

Thus:

$$pqr - pq + rpq - rp = pqr + p(rq - q - r) > pqr = |G|$$

and we get a contradiction.
ii) If $N_q = r$ then G must contain $r(q - 1)$ elements of order q living inside the r different q-Sylow subgroups. Also consider the $pq(r - 1)$ elements of order r living inside the the pq different r-Sylow subgroups. So we have

$$r(q - 1) + pq(r - 1) = pqr - pq + rq - r$$

[7] Never use a tank to kill a fly, its not sportsmanlike!

[8] You can definitely skip this proof

[9] This is easy we learned that in kindergarten.

elements in G.
• But:

$$q > p \Rightarrow q - 1 \geq p \Rightarrow (q-1)r \geq pr > pq$$

Thus:

$$(q-1)r > pq \Rightarrow qr - r - pq > 0$$

So:

$$pqr - pq + rq - r > pqr = |G|$$

which is again a contradiction.
iii) If $N_q = 1$. Let Q be the only normal q-Sylow subgroup of G.
• Consider G/Q which is a group of order $p \cdot r$. The $pq(r-1)$ elements of order r in G are distributed among the cosets of Q in G. Since every coset has exactly q elements we need at least $p(r-1)$ different cosets to cover all the elements of order r in G.
• We claim that each of those cosets has order r if we consider it as an element in G/Q.
• This is true since let a be an element of order r in G that belongs to one of those cosets. Then the coset is exactly $a \cdot Q$.
• The order of the coset must divide the order of the coset group. Thus it can be either r or p or rp.
• If it is r we are done.
• It cannot be rp since $(a \cdot Q)^r = a^r \cdot Q = e \cdot Q$ which is the identity element. Thus $o(a \cdot Q) \leq r$.
• Finally it cannot be p since then $(a \cdot Q)^p = e \cdot Q \Rightarrow a^p \cdot Q = e \cdot Q \Rightarrow a^p \in Q$. But a^p belongs to an r-Sylow subgroup. Thus $a^p \in R \bigcap Q$ where R is an r-Sylow subgroup.
• But $R \bigcap P = \{e\}$ since if $g \in R \bigcap P$ then $o(g)|o(R)$ and $o(g)|o(Q)$ thus $o(g)|r$ and $o(g)|Q$ which means $o(g)|r$ and $o(g)|q$ but q,r are different primes thus order of g is exactly 1 which means that $g = e$. So $a^p = e$ which is a contradiction since $o(a) = r$ thus r divides p which cannot happen since both of them are different primes (in fact $r > p$).
• So we have at least $p(q-1)$ elements in G/Q with order r. But G/Q has order $p \cdot r$. The number of r-Sylow subgroups in G/Q must divide pr and it must be 1modr .
• Obviously it is exactly one meaning G/Q has exactly one r-Sylow subgroup. So it has at most $r-1$ elements of order r all of them inside this r-Sylow subgroup.
• Thus $p(r-1) \leq r - 1 \Rightarrow p \leq 1$ which is a contradiction.
• So case b leads to a contradiction and we are done. □

One could say that in small orders the problem of Solvability is very much related to the problem of Simplicity. So ... heads up!!! More definitions coming.

Definition 6. *A finite group G is called simple if it has no non-trivial normal subgroups.*

Remark. *Again by definition a cyclic group of prime order is not considered simple*[10].

[10] I haven't got the slightest clue why!

Example 2. *The smallest simple group is A_5 which is the alternating group of S_5 AKA[11] the group of all even permutations of S_5. One should know that $|A_5| = \frac{5!}{2} = 60$.*

This example is left as a really hard (close to impossible), time-consuming, totally boring, extremely unnerving and useless exercise to the poor reader.

So how do we apply all this things to solid problems? A good exercise is to show that all groups with order up to 100 except 60 are solvable with as little use of Burnside's theorem as possible. For 60 we get our first example of a non-solvable group which is A_5.

In order to make things easier I will use this small but really handy lemma which can be found in [4].

Lemma 1. *If a group G has a subgroup H such that $|G|$ does not divide the $i(H)$ factorial ($i(H)$[12]!), then H contains a non-trivial normal subgroup of G.*[13] .

Now lets prove these following small lemmas.

Lemma 2. *If $|G| = 2^k \cdot 3$ for $k \geq 2$ then G is solvable.*

Proof. By induction on k.

1st Step It obviously holds for $k = 1$ where $|G| = 6$ since then G has only one 3-Sylow subgroup H which is normal,cyclic, abelian, of order 3 and the quotient G/H is cyclic abelian of order 2.

2nd Step Let the proposition hold for all k=1,2,...,n.

3d Step We will prove that it holds for k=n+1. From Sylow's theorems we know that G contains at least on 2-Sylow subgroup of order 2^{k+1}. Lets call that H. Then $i(H) = 3$ thus $2^{k+1} \cdot 3$ does not divide $3! = 6$. Thus H contains a normal subgroup of G lets say K. But $|K| = 2^m$ thus by our basic example H is solvable. Also $|G/K| = 3 \cdot 2^{k-m}$ thus by step 2 G/K is solvable. Finally from our tool theorem G is solvable.

□

Lemma 3. *If $|G| = 3^k \cdot 2^2$ then G is solvable.*

Proof. By induction on k.

1st Step It obviously holds for k=2 where $|G| = 12$ since then $|G| = 2^2 \cdot 3$ and it is in the previous lemma's category.

2nd Step Let the proposition hold for all k=1,2,...,n, with $n \geq 1$

3d Step We will prove that it holds for k=n+1. Thus $n + 1 \geq 2$. From Sylow's theorems we know that G contains at least on 3-Sylow subgroup of order 3^{n+1}. Lets call that H. Then $i(H) = 2^2$ thus $3^{n+1} \cdot 2^2 = 3^2 \cdot 2^2 \cdot 3^{n+1-2} = 36 \cdot \cdot 3^{n+1-2}$ does not divide $2^2! = 24$. Thus H contains a normal subgroup of G lets say K. But $|K| = 3^m$ thus by our basic example H is solvable. Also $|G/K| = 2^2 \cdot 3^{k-m}$ thus by step 2 G/K is solvable. Finally from our tool theorem G is solvable.

□

Lemma 4. *If $|G| = 2^k \cdot 5$ then G is solvable.*

[11] AKA means <u>also know as</u>... these are stuff you learn when doing a phd in the States!

[12] i(h)= index of the subgroup meaning the cardinality of G/H.

[13] The proof for this is really small and digestible. It is not my style though!

Proof. By induction on k.

1st Step It obviously holds for $k = 1, 2, 3$ where $|G| = 10, 20, 40$ respectively because we can use theorem 1 in those cases.

2nd Step Let the proposition hold for all $k = 1, 2, ..., n$, with $n \geq 3$.

3d Step We will prove that it holds for $k = n+1$. We have that $k = n+1 \geq 4$. From Sylow's theorems we know that G contains at least on 2-Sylow subgroup of order 2^{n+1}. Lets call that H. Then $i(H) = 5$ thus $2^{n+1} \cdot 5 = 2^4 \cdot 5 \cdot 2^{n+1-4} = 80 \cdot 2^{n+1-4}$ does not divide $5! = 120$. Thus H contains a normal subgroup of G lets say K. But $|K| = 2^m$ thus by our basic example H is solvable. Also $|G/K| = 5 \cdot 2^{k-m}$ thus by step 2, G/K is solvable. Finally from our tool theorem G is solvable.

□

If you check our colored map in the end we will find out that there is not so much proving for me to do[14]. We only need to consider the few Sporadic Cases as I will call them[15] which are 56,72,84,90.

4. Sporadic Cases

Case 56!. *Every group of order* 56 *is solvable.*

Proof. From Sylow's theorems we know that N_7 is either 1 or 8. If it is 1 by now I am sure you know how to prove that G is solvable. So let it be 8. Again count all the elements in those groups that are not the identity. We get $8 \cdot 6 = 48$ elements. But again by the Sylow theorems we get that there exists at least one 2-Sylow subgroup of order 8. If you add them up you get $48 + 8 = 56$ elements which leaves no room for another 2-Sylow subgroup. Thus G is again solvable by the standard method! □

Case 84!. *Every group of order* 84 *is solvable.*

Proof. Obviously $|G| = 84 = 7 \cdot 3 \cdot 2^2$. Consider the number of the 7-sylow subgroups of G, N_7. Then $N_7 = 1 \text{mod} 7$ and N_7 divides 84 thus $(N_7, 7) = 1$ so N_7 can be only 1. Lets call this normal 7-sylow subgroup P. Then P is normal, cyclic of order 7, abelian and solvable. Also $|\frac{G}{P}| = 12$ which is solvable by lemma 2. So by our tool-theorem G is solvable. □

Case 72!. *Every group of order* 72 *is solvable.*

Proof. Let G be a group with $|G| = 2^3 \cdot 3^2$. First of all we can use Burnside's theorem but there is another way more easy but still not so ... numerical. Unfortunately it is the only one that I can think of thus I will write it down.

• Consider the number of the 3-sylow subgroups in G. Then easily we can see that $N_3 = 1$ or $N_3 = 4$.

i) If $N_3 = 1$ we have that there exists only one 3-sylow subgroup lets call it P of order 9 which is a 3-group thus it is solvable. Also $|\frac{G}{P}| = 2^3$ thus $\frac{G}{P}$ is a 2-group thus it is solvable and by the theorem tool G is solvable.

ii) If $N_3 = 4$ by the theorem I named 4th sylow theorem we get that there exists a homomorphism $\phi : G \to S_4$. Also 4 divides $|Im\phi|$. And $Im\phi \leq S_4$. Thus

[14] Which was the purpose for this whole thing!

[15] Obviously sporadic is a Greek word meaning something like random. Sporades is a complex of Greek islands that definitely illustrates this randomness !!

the possible cases for $|Im\phi|$ are $4, 8, 12, 24$. But we know from the 1st theorem of homomorphisms that $\frac{G}{Ker\phi} \simeq Im\phi$. Thus if we use Lagrange's theorem we get $\frac{|G|}{|Ker\phi|} = |Im\phi|$ so the possible numbers for the order of $ker\phi$ are $18, 9, 6, 3$. Thus $Ker\phi$ is a nontrivial normal subgroup of G. By checking our colored map in the end we can see that in all cases our $Ker\phi$ is going to be a solvable group. Also the numbers for $G/Ker\phi$ are $4, 8, 12, 24$ so $G/Ker\phi$ is also going to be solvable in every case.(check the colored table in the end again). Thus by our tool theorem G is solvable. □

Case 90!. *Every group of order* 90 *is solvable.*

Proof. Let G be a group of order $90 = 2 \cdot 3^2 \cdot 5$

- The number of Sylow 5-groups is 1 or 6.

i) If it is one lets call P the unique cyclic, abelian, solvable 5-sylow subgroup of G. Then G/P has order 18 and it is solvable by theorem 1. So by our tool theorem G is solvable.
ii) If there are 6 5-Sylow subgroups in G. This gives us $6 \cdot 4 = 24$ elements of order 5 living inside the 6 different 5-Sylow subgroups.

- The number of 3-Sylow subgroups is 1 or 10.

a) If it is 1 lets call Q the unique 3-Sylow subgroup of G. Then Q is a 3-group thus it is solvable. Also G/Q has order 10 and it is solvable by theorem 1. Thus by the tool theorem G is solvable.
b) If we have 10, 3-Sylow subgroups, of order 9.

- We cannot have that all 3-Sylow subgroups intersect in $\{e\}$, for then we would have 8*10 = 80 elements of order a divisor of 9 in the 3-Sylow subgroups, leaving too little room for the 24 elements of order 5 $(80 + 24 > 90)$.

- So there are P, Q, 3-Sylow subgroups that intersect non-trivially. Obviously $|P \bigcap Q| = 3$. Let $T = P \bigcap Q$ and S the normalizer of T. Then it is obvious that P and Q are subgroups of S, since P and Q are abelian and T is a subset of them. So $|S| > 3 + 6 + 6 = 15$. Also $|S|$ divides 90. Thus $|S|$ can be 18 or 45 or 90.
- If $|S| = 90$ that means exactly that $S = G$ which means that T is normal, cyclic, abelian of order 3 thus solvable. Also G/T has order 30 and thus it is solvable (check our table). By our tool theorem G is solvable.
- If $|S| = 45$, it would be a subgroup of index 2 in G and hence normal, and by our table solvable. Also G/S is of order 2 thus solvable. By our tool theorem G is also solvable.
- If $|S| = 18$ then S has index 5. But then $|G| = 90$ does not divide $5! = 120$ thus by our lemma S contains a non-trivial normal subgroup of G. The possible orders for this subgroup which we will call N are 2,3,6,9,18. In all cases if we check our table N is solvable. The possible order for G/N are respectively 45,30,15,10,5. Thus again by our table in the end we get that G/N is solvable in any case. So by our tool theorem G is again solvable in all cases. DONE!
- This proof uses all the basic tools and the numerical approach. I wouldn't dream

of presenting it in a seminar but I believe it is a very beautiful result and it is this that motivated me in the first place[16]. □

5. Thanks

I would like to send a special thank you to the 42 teem for their invitation which was the original motivation to write this talk. Keep the ideas running guys. A big thank you to Prof. P.Tiep who underwent the troublesome procedure of reading and correcting this paper. Finally a special thanks to prof. G.Tapper for technical (and general) support. Once more I would like to thank all of you back home who were patient enough to attend this weird lecture. I would also like to thank the people that came in this hall to see me. I would like to thank also pr E.Raptis for first introducing me to this subject[17], and professor A.Turrul for inviting me to this seminar.

References

1. J.Fraleigh *Introduction to the Theory of Groups*
2. D.Robinson *A Cource In The Theory of Groups*
3. M.Lang *Theory of Groups*
4. I.Herstein *Topics In Algebra*

Mathematics Department, University of Florida, Gainesville , USA
E-mail address: thanos@plaza.ufl.edu

[16] I couldn't find the proof when I first tried!

[17] I finally understand now!