2. SOLUBLE GROUPS

§ 2.1. Conjugates and Commutators

I'll begin by reminding you of some basic facts. Let $x, y \in$ G. The **conjugate** of x by y is $x^y = y^{-1}xy$. The map $x \to x^g$, for a fixed g, is an automorphism of G. We denote it by $\Theta(g)$.

The map $g \to \Theta(g)$ is a homomorphism from G to the automorphism group Aut(G) of G and the image is denoted by Inn(G). The $\Theta(g)$ are called **inner automorphisms**. Any other automorphisms are called **outer automorphisms**.

The kernel of the homomorphism Θ is clearly the centre Z(G) and so, by the First Isomorphism Theorem, $G/Z(G) \cong \mathrm{Inn}(G)$.

We also conjugate subgroups. If $H \le G$ and $g \in G$ then $H^g = g^{-1}Hg = \{g^{-1}hg \mid h \in H\}$. $H^g \le G$ for all $g \in G$ and $H \trianglelefteq G$ if and only if $H^g = H$ for all $g \in G$.

Closely related to conjugates are commutators. The **commutator** of x and y is $x^{-1}x^y$, which we can write out in full as $x^{-1}y^{-1}xy$. We denote it by $[x, y]$.

The name derives from the fact that $[x, y] = 1$ if and only if x commutes with y. The number of commutators is a crude measure of how far the group departs from being abelian.

Two identities that hold for commutators are:

(1) $[x, yz] = [x, z]\,[x, y]^z$ and
(2) $[xy, z] = [x, z]^y\,[y, z]$.
These can be proved by simply writing both sides of each equation in full.

Extended commutators are defined inductively by:

$$[x_1, x_2, \ldots, x_n, x_{n+1}] = [[x_1, x_2, \ldots, x_n], x_{n+1}].$$

An interesting identity involving commutators of length 3 is:

$$[x, y^{-1}, z]^y\,[y, z^{-1}, x]^z\,[z, x^{-1}, y]^x = 1.$$

Again one can simply write out the left-hand side of this identity and cancel it down to 1. But it's a lot of work. The proof can be made easier by putting

$$u = xzx^{-1}yx,\ v = yxy^{-1}zy \text{ and } w = zyz^{-1}xz.$$

Then the identity becomes $(u^{-1}v)(v^{-1}w)(w^{-1}u) = 1$.

§ 2.2. The Derived Series

Unfortunately the set of commutators is not a subgroup, although it does satisfy two of the three criteria for a subset to be a subgroup. It contains the identity and it is closed under inverses, because $[y, x] = [x, y]^{-1}$. However, in general, it isn't always closed under products.

The simplest example is the free group on 4 generators ⟨A, B, C, D | ⟩. Clearly the product of the two commutators [A, B] and [C, D] isn't a commutator.

It would be nice to give a small finite example of such a group, but the smallest such examples are two groups of order 96.

So we're forced to define the **derived subgroup** of a group G to be **G′** = the group *generated* by all the commutators.

Clearly **(G × H)′ = G′ × H′** for all groups G, H. If H is a normal subgroup of G, what is (G/H)′? Is it G′/H′? No, because any subgroup of G/H has to have the form K/H for some subgroup K of G. Is it G′/H? No, because a subgroup of G/H has to have the form K/H where H ≤ G. In fact **(G/H)′ = G′H/H**.

In Volume 1 we proved that the derived subgroup of G is the largest normal subgroup for which the quotient group is abelian. This is usually the quickest way of finding it. We can continue the process, giving a whole series of subgroups.

We define G′′ to be (G′)′ and G′′′ = (G′′)′ etc. We denote the ***n*-th derived subgroup** (the result of *n* such steps) by $G^{(n)}$ so G′′′ can be written as $G^{(3)}$.

In other words we define $G^{(n)}$ inductively by:

$$G^{(0)} = G;\ G^{(n+1)} = G^{(n)\prime} \text{ for all } n.$$

This results in a chain of subgroups:

$$G \geq G' \geq G'' \geq G^{(3)} \geq G^{(4)} \geq .....$$

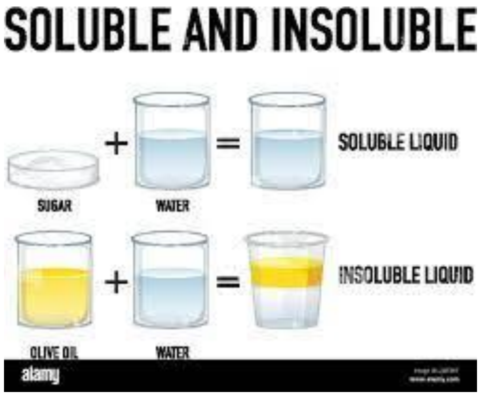
Each subgroup is normal in the one before and the quotients of successive terms are abelian. Such a series is called the **derived series** for G.

Example 1: $\mathbf{S}_4' = \mathbf{A}_4$, $\mathbf{S}_4'' = \mathbf{V}_4$ and $\mathbf{S}_4''' = \mathbf{S}_4^{(3)} = 1$.
Here $\mathbf{V}_4$ = {I, (12)(34), (13), (24), (14)(23)} is the normal subgroup of order 4. Because $\mathbf{A}_4/\mathbf{V}_4$ has order 12/4 = 3, it is cyclic, and hence abelian, so $\mathbf{S}_4'' = \mathbf{A}_4' \le \mathbf{V}_4$. Thus $\mathbf{S}_4''$ has order 1, 2 or 4. It's not 1 because $\mathbf{A}_4$ is not abelian. It's not of order 2 because then $\mathbf{A}_4/\mathbf{A}_4'$ would have to be cyclic of order 6, yet $\mathbf{A}_4$ has no elements of order 6.
This leaves $\mathbf{S}_4'' = \mathbf{A}_4' = \mathbf{V}_4$. Finally, since $\mathbf{V}_4$ is abelian $\mathbf{S}_4''' = \mathbf{V}_4' = 1$.

§ 2.3. Soluble Groups

The class of **soluble groups** is $\mathfrak{S} = \mathfrak{A}^\infty$. Thus a group G is soluble if and only if, for some *n*, there is a subnormal series from **1** to G, with each quotient being abelian.

The smallest possible value of *n* is called the **soluble length** of G. We denote the class of soluble groups of length at most *n* by $\mathbb{S}_n$. Clearly $\mathbb{S}_0$ = I and $\mathbb{S}_1 = \mathfrak{A}$. The groups in $\mathbb{S}_2$ are called **metabelian** groups.



Theorem 1:
(1) Subgroups of soluble groups are soluble.
(2) Quotients of soluble groups are soluble.
(3) If G/H is soluble and H is soluble then G is soluble.
Proof: These follow immediately from Theorem 2 of Chapter 1 and the fact that A is both subgroup and quotient closed. ✋☺

Clearly a group G is soluble if and only if $G^{(n)} = 1$ for some *n*. Moreover the value of the smallest such *n* will be the soluble length of G, as we now show.

Theorem 2: If *n* is the smallest integer such that $G^{(n)} = 1$ then the soluble length of G is *n*.
Proof: Let *n* be the soluble length of G.
Then there exists a subnormal series

$$1 = G_0 < G_1 < \ldots < G_n = G$$

such that each G_{i+1}/G_i is abelian and *n* is the smallest such value. Suppose that $G^{(m)} = 1$ and *m* is the smallest such value.

Since the derived series has abelian quotients we have $n \leq m$. But $G_{i+1}' \leq G_i$ for all *i* and so $G^{(n)} \leq G_0 = 1$. Hence $m \leq n$. Thus $m = n$. ✋☺

The soluble length of a subgroup or quotient group cannot exceed that of the group itself, but it may be less.

There are two ways that a group can fail to be soluble. The derived series might continue to descend indefinitely.

$$G > G' > G'' > G^{(3)} > G^{(4)} > \ldots..$$

Of course this can only occur for an infinite group. But a group, even a finite one, can fail to be soluble by virtue of its derived series getting 'stuck' at some point, that is, where it reaches a subgroup that is not the identity but which, like the identity subgroup, is equal to its own derived subgroup. One very special way this can happen is for a non-abelian group to have no normal subgroups other than itself and the identity.

§ 2.4. Simple Groups

A group G that has no normal subgroups, apart from G itself and 1, is called a **simple** group. Such groups are 'simple' so far as their lattice of normal subgroups goes. But in other respects most of them are far from simple, in the normal sense of the word. But let's get the really simple simple groups out of the way.

Groups of prime order (necessarily cyclic) are simple groups. This is a direct consequence of Lagrange's Theorem. These groups, together with the trivial group 1, are in fact the only abelian simple groups. (Why?).

So the only simple groups of real interest are the non-abelian ones. Among these the finite non-abelian simple groups have attracted an enormous amount of interest over the last hundred years. A classification of the finite simple groups has now been finished. But has been an enormous task.

The Guinness Book of Records, in an earlier edition, mentioned only two theorems of mathematics. Pythagoras' Theorem holds the record for the largest number of different proofs (about 350) and of course everybody has heard of Pythagoras' Theorem, even if they can't recall even one of these many proofs. But very few people have heard of the Classification Theorem for Finite Simple Groups. Its claim to fame is the sheer size of its proof. Nowhere does the proof appear in its entirety, and probably it will never appear complete in one publication. It is a mosaic of thousands of mathematical papers by hundreds of group theorists, all building on one another. If all the papers necessary for a complete proof were ever assembled in one place it is estimated that they would occupy about 15,000 pages (the equivalent of a large, multi-volume encyclopaedia)!

The theorem states that every finite simple group is either in one of 19 families or they are one of 15 **sporadic** or one-off examples.

Among the infinite families of finite simple groups are:

- $\mathbf{C}_p$ for prime p (these, and $\mathbf{1}$, are the only finite abelian simple groups).
- $\mathbf{A}_n$ for $n \geq 5$, the alternating groups

- **PSL**(n, p^m) for a prime p and integers m and n where $n \geq 3$ or $n = 2$ and $q \geq 4$, which I'll now define.

PSL(n, p^n) is SL(n, p^m)/Z where SL(n, p^m) is the group of all $n \times n$ matrices, with determinant 1, over the field GF(p^m) of size p^m, and Z is its centre, the set of all $n \times n$ scalar matrices λI where λ is an n'th root of unity.

In addition to the above three families, and a few more, there are 15 **sporadic finite simple groups**. These don't belong to any one of the infinite families.

The smallest is the **Mathieu group** $\mathbf{M}_{11}$, of order 7920. The largest sporadic groups is called the **Monster**, with order greater than 8×10^{54}.
Another is the so-called **Baby Monster** which only has order about 4×10^{33}.

We now turn our attention to showing that $\mathbf{A}_n$ is simple for $n \geq 5$. This fact is central to the proof of the insolubility of the quintic. Polynomials of degree 5 or more cannot be solved by radicals simply because $\mathbf{A}_n$ is simple for $n \geq 5$.

§ 2.5. The Simplicity of $\mathbf{A}_n$

Lemma: $\mathbf{A}_n$ is generated by cycles of length 3.

Proof: Every even permutation is a product of an even number of transpositions. We show that any product of two transpositions $g = (x_1\ x_2)(x_3\ x_4)$ is a product of cycles of length 3.

Case I the transpositions are disjoint:
Then $g = (x_1\ x_2\ x_3)(x_1\ x_4\ x_3)$.

Case II: the transpositions have one symbol in common: say $x_4 = x_1$: Then $g = (x_1\ x_2\ x_3)$. ✋☺

Theorem 3: If $n \geq 5$, all cycles of length 3 are conjugate in $\mathbf{A}_n$.

Proof: Of course any two 3-cycles are conjugate in $\mathbf{S}_n$. But are they conjugate in $\mathbf{A}_n$? As often happens it might be that the 3-cycles split into two conjugacy classes when we restrict ourselves to $\mathbf{A}_n$.

Let $g = (x_1\ x_2\ x_3)$, $h = (y_1\ y_2\ y_3)$ be any two cycles of length 3. Then $g = k^{-1}hk$ for any permutation k that maps x_1 to y_1, x_2 to y_2 and x_3 to y_3. With at least two more symbols to complete the definition it's possible to arrange for k to be even (just add a disjoint 2-cycle if necessary).

For $n < 3$ there are no cycles of length 3. For $n = 3$ or 4 there are two conjugacy classes of cycles of length 3 in $\mathbf{A}_n$. ✋☺

Theorem 4: $\mathbf{A}_n$ is simple for $n \geq 5$.
Proof: Suppose that $n \geq 5$ and suppose that H is a proper non-trivial normal subgroup of $\mathbf{A}_n$.
If $h \in$ H and $g \in \mathbf{A}_n$ then, since H is normal in $\mathbf{A}_n$,
$[g, h] = (g^{-1}h^{-1}g)h \in$ H.

We'll show that H contains a cycle of length 3. Since all cycles of length 3 are conjugate to one another in $\mathbf{A}_n$ this would mean that H must contain every cycle of length 3 and so must contain every even permutation, contradicting the fact that H < $\mathbf{A}_n$.
Choose $1 \neq h \in$ H.

Case 1 *h* = (××××…)…: Without loss of generality we may let $h = (1234\ldots)\ldots$
Let $g = (123)$. Then $[g, h] = (132)(234) = (142)$.

Case 2 *h* = (×××)(×××) …:
Without loss of generality let $h = (123)(456)\ldots$
Let $g = (145)$.
Then $[g, h] = (154)(256) = (16254)$. Go to case 1.

Case 3 *h* = (×××)(××)(××) …: Then $h^2 = (\times\times\times)$.

Case 4 *h* = (××)(××)(××) … : Without loss of generality let $h = (12)(34)(56)\ldots$ and let $g = (12345)$.
Then $[g, h] = (15432)(21436) = (153)(246)$.
Go to case 2.

Case 5 h = (××)(××): Without loss of generality let $h = (12)(34)$ and let $g = (12345)$.
Then $[g, h] = (15432)(21435) = (12453)$. Go to case 1. ✋☺

In fact $\mathbf{A}_n$ is simple for *all* values of *n except* $n = 4$. For $n \le 2$, $\mathbf{A}_n$ is trivial. For $n = 3$ it is cyclic of order 3. And $\mathbf{A}_4$ isn't simple because it contains the proper, non-trivial, subgroup

$$\mathbf{V}_4 = \{I, (12)(34), (13)(24), (14)(23)\}.$$

Since $\mathbf{A}_5$ is the smallest non-abelian simple group it is the smallest group that is not soluble.

§ 2.6. Small Groups are Soluble

All small finite groups are soluble. What do I mean by small? You'll see.

Groups of prime order are cyclic, and hence soluble. Groups of order $2p$ are cyclic or dihedral and so are soluble. Since the centre of a non-trivial p-group is non-trivial we can see that all p-groups are soluble. The theory of Sylow subgroups is a powerful tool in dealing with other cases.

Lemma: Suppose that $|G| = p^n m$ for some m, n and prime p which doesn't divide m. Suppose that $|G| > p$.
Suppose that for every integer of the form $h = 1 + kp$ that divides m, either $h = 1$ or $h! < |G|$.
Then G is not simple.

Proof: Let The number of Sylow *p*-subgroups be *h*.
Then $h = 1 + kp$ and divides *m*.
Hence $h = 1$ or $h! < |G|$.
Case I: *h* = 1: Then G has a unique Sylow *p*-subgroup, P, which must be normal. If P = G then G is a *p*-group and so is not simple.
Case II: *h*! < |G|:
G permutes the Sylow *p*-subgroups by conjugation. Hence there is a homomorphism $\Phi: G \to \mathbf{S}_h$. Since $|G| > |\mathbf{S}_h|$ $K = \ker \Phi > 1$. If K = G then every Sylow *p*-subgroup is normal in G (and hence there is only one of them.) So K is a proper non-trivial normal subgroup and so is not simple.✋☺

Theorem 5: All group of order up to 59 are soluble.
Proof: Let $|G| = n < 60$.
If $n = 1$, G is soluble of length 0.
The following table lists values of n up to 59, together with the values of *p*, *n* and *m* in cases where the above lemma shows that groups of order *m* are soluble.

|G|	*p*	*n*	*m*	|G|	*p*	*n*	*m*	|G|	*p*	*n*	*m*
2	2	1	1	21	7	1	3	41	41	1	1
3	3	1	1	22	11	1	2	42	7	1	6
4	2	2	1	23	23	1	1	43	43	1	1
5	5	1	1	24	2	3	3	44	11	1	4
6	3	1	2	25	5	2	1	45	5	1	9
7	7	1	1	26	13	1	2	46	23	1	2
8	2	3	1	27	3	3	1	47	47	1	1

9	3	2	1
10	5	1	2
11	11	1	1
12	2	2	3
13	13	1	1
14	7	1	2
15	5	1	3
16	2	4	1
17	17	1	1
18	3	2	2
19	19	1	1
20	5	1	4

28	7	1	4
29	29	1	1
30	**5**	**1**	**6**
31	31	1	1
32	2	5	1
33	11	1	3
34	17	1	2
35	7	1	5
36	3	2	4
37	37	1	1
38	19	1	2
39	13	1	3
40	5	1	8

48	2	4	3
49	7	2	1
50	5	1	10
51	17	1	3
52	13	1	4
53	53	1	1
54	3	3	2
55	11	1	5
56	**7**	**1**	**8**
57	19	1	3
58	29	1	2
59	59	1	1

The two values that are in bold don't fit the lemma and we need to work a bit harder.

|G| = 30: If a group of order 30 is not soluble it must have 10 Sylow 3-subgroups and 6 Sylow 5-subgroups.
Each Sylow 3-subgroup is a $\mathbf{C}_3$ and has 2 elements of order 3. Each Sylow 5-subgroup is a $\mathbf{C}_5$ and has 4 elements of order 5. Moreover all these subgroups must be disjoint (only having the identity in common). This gives 20 elements of order 3 and 24 elements of order 5. But this is already more than |G|, a contradiction.

|G| = 56: If G is not soluble we'd need to have 7 Sylow 2-subgroups and 8 Sylow 7-subgroups. The Sylow 2-subgroups have order 8. Thus there are 48 elements of order 7, leaving just 8 elements of all other orders. Just one Sylow 2-subgroup would use up all of these and so there can't possibly be 7 Sylow 2-subgroups. ✋☺

So all groups of order less than 60 are soluble and $\mathbf{A}_4$, of order 60 is not soluble, so it is therefore the smallest non-soluble group.

In my notes on *Representation Theory* I show that all groups of order $p^a q^b$, where p, q are distinct primes, are soluble. This would have greatly simplified the above analysis. However that theorem requires a considerable amount of representation theory and number theory to prove.

EXERCISES FOR CHAPTER 2

Exercise 1: For each of the following statements determine whether it is true or false.

(1) The derived subgroup is the set of all commutators.
(2) The inverse of a commutator is a commutator.
(3) A conjugate of a commutator is a commutator.
(4) The product of two commutators is a commutator.
(5) G/G' is always abelian.
(6) $\mathbf{S}_n$ is a simple group for all n.
(7) If G is a non-abelian simple group $G' = G$.
(8) $\mathbf{A}_n$ is simple for all n.
(9) $(G/H)' = G'/H$.
(10) All groups whose order is less than 60 are soluble.

Exercise 2: Prove that the following identities hold for commutators:

(a) $[y^{-1}, x]^y = [x, y]$;
(b) $(xy)^2 = x^2y^2[y, x][y, x, y]$;
(c) $[x, y, y^z].[y, z, x^{-1}] = 1$.

Exercise 3: If $n \geq 1$, find $\mathbf{D}_{2n}'$.

Exercise 4: Show if $60 < |G| < 90$ then G is soluble.

SOLUTIONS FOR CHAPTER 2

Exercise 1: (1) FALSE (it is the subgroup generated by all the commutators);
(2) TRUE;
(3) TRUE;
(4) FALSE;
(5) TRUE;
(6) FALSE ($\mathbf{A}_n$ is a normal subgroup);
(7) TRUE;
(8) FALSE ($\mathbf{A}_4$ has $\mathbf{V}_4$ as a proper, non-trivial normal subgroup);
(9) FALSE;
(10) TRUE.

Exercise 2:

(a) $[y^{-1}, x]^y = y^{-1}[y^{-1}, x]y = y^{-1}(yx^{-1}y^{-1}x)y = x^{-1}y^{-1}xy.$

(b)
$$\begin{aligned}
x^2y^2[y, x][y, x, y] &= x^2y^2\,y^{-1}x^{-1}yx\,[y, x]^{-1}y^{-1}[y, x]y \\
&= x^2y^2\,y^{-1}x^{-1}yx\,[x, y]y^{-1}[y, x]y \\
&= x^2y^2\,y^{-1}x^{-1}yx\,x^{-1}y^{-1}xyy^{-1}y^{-1}x^{-1}yxy \\
&= x^2yx^{-1}\,(y\,xx^{-1}y^{-1})\,x\,(yy^{-1})\,y^{-1}x^{-1}yxy \\
&= x^2y\,x^{-1}xy^{-1}x^{-1}yxy \\
&= x^2\,(yx^{-1}xy^{-1})\,x^{-1}yxy \\
&= x^2x^{-1}yxy \\
&= xyxy = (xy)^2.
\end{aligned}$$

(c) $[x, y, z^x] = [[x, y], z^x] = [x, y]^{-1}(z^x)^{-1}[x, y]z^x$

$= [y, x]\, x^{-1}z^{-1}x\, x^{-1}y^{-1}xy\, x^{-1}zx$

$= y^{-1}x^{-1}yx\, x^{-1}z^{-1}x\, x^{-1}y^{-1}xy\, x^{-1}zx$

$= y^{-1}x^{-1}yz^{-1}y^{-1}xyx^{-1}zx$

By making the changes x→z, y→x, z→y twice we get:

$[z, x, y^z] = x^{-1}z^{-1}xy^{-1}x^{-1}zxz^{-1}yz$ and

$[y, z, x^y] = z^{-1}y^{-1}zx^{-1}z^{-1}yzy^{-1}xy$

Combining we get:

$[x, y, z^x].[z, x, y^z].[y, z, x^y]$

$= y^{-1}x^{-1}yz^{-1}y^{-1}xyx^{-1}zx.\, x^{-1}z^{-1}xy^{-1}x^{-1}zxz^{-1}yz$

$.\, z^{-1}y^{-1}zx^{-1}z^{-1}yzy^{-1}xy$

$= y^{-1}x^{-1}yz^{-1}y^{-1}xyx^{-1}\,(zx.\, x^{-1}z^{-1})\, xy^{-1}x^{-1}zxz^{-1}(yz$

$.\, z^{-1}y^{-1})\, zx^{-1}z^{-1}yzy^{-1}xy$

$= y^{-1}x^{-1}yz^{-1}y^{-1}xyx^{-1}\; xy^{-1}x^{-1}zxz^{-1}\, zx^{-1}z^{-1}yzy^{-1}xy$

$= y^{-1}x^{-1}yz^{-1}y^{-1}x\,(yx^{-1}\; xy^{-1})\, x^{-1}z\,(xz^{-1}\, zx^{-1})\, z^{-1}yzy^{-1}xy$

$= y^{-1}x^{-1}yz^{-1}y^{-1}(xx^{-1}zz^{-1})\, yzy^{-1}xy$

$= y^{-1}x^{-1}y\,(z^{-1}y^{-1}yz)\, y^{-1}xy$

$= y^{-1}x^{-1}yy^{-1}xy$

$= 1.$

Exercise 3: $D_{2n} = \langle A, B \mid A^n, B^2, BA = A^{-1}B\rangle$.

$D_2 \cong C_2$ and so $D_2' = 1$.

$D_4 \cong C_2 \times C_2$ and so $D_4' = 1$.

Suppose that $n \geq 3$.

Case I: *n* is odd: Then $\mathbf{D}_{2n}' = \langle A\rangle$.

Case II: n is even: Then $\mathbf{D}_{2n}' = \langle A^{n/2}\rangle$.

Exercise 4: The following table expresses |G| as $p^n m$ where p is prime and is coprime to m. In all these cases we can show that G is soluble by the same methods that we used in Theorem 5.

|G|	***p***	***n***	***m***	**|G|**	***p***	***n***	***m***	**|G|**	***p***	***n***	***m***
61	61	1	1	70	5	1	14	80	**2**	**4**	**5**
62	31	1	2	71	71	1	1	81	3	4	1
63	7	1	9	72	3	2	8	82	41	1	2
64	2	6	1	73	73	1	1	83	83	1	1
65	13	1	5	74	37	1	2	84	7	1	12
66	11	1	6	75	5	2	3	85	17	1	5
67	67	1	1	76	19	1	4	86	43	1	2
68	17	1	4	77	11	1	7	87	29	1	3
69	23	1	3	78	13	1	6	88	11	1	8
70	7	1	10	79	79	1	1	89	89	1	1

In fact all groups G with 60 < |G| < 120 are soluble, making $\mathbf{S}_5$ the second smallest non-soluble group. However we need extra techniques to deal with |G| = 90 and |G| = 112.