https://AlexBrodbelt.github.io/ClassificationOfFiniteSubgroupsOfPGL https://github.com/AlexBrodbelt/
https://AlexBrodbelt.github.io/ClassificationOfFiniteSubgroupsOfPGL/docs

Classification of finite subgroups of PGL

AlexBrodbelt

March 9, 2025

Chapter 1

Abstract and Summary

1.1 Acknowledgements

I would to thank my supervisor Prof. David Jordan for his invaluable support and guidance throughout the project; Christopher Butler for providing the TeX code so I could easily set up the blueprint, and hopefully, improve and add to his amazing exposition of **Dickson's Classification Theorem**.

I would also like to thank Prof. Kevin Buzzard for his support, patience and guidance throughout the project. His advice and comments on how I should go about formalising mathematics have been of utmost value.

Finally, I would like to thank the many members of the Lean Zulip community who have provided insightful ideas and comments that have helped me progress much faster than otherwise, this also includes assistance with technical issues with setting up the blueprint and so forth. I am grateful to:

- Artie Khovanov
- David Loeffler
- Mitchell Lee
- Yakov Pechersky
- Edward van de Meent
- Ruben Van de Velde
- Andrew Yang
- Patrick Massot
- Johan Commelin
- Scott Carnahan
- Damiano Testa

- Aron Liu

I apologise if I have forgotten to include any names.

1.2 Summary

The primary aim of this project is to present the ongoing formalisation of the classification of finite subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$ in the Lean proof assistant. This result fits into to the much larger and more ambitious project of formalising Fermat's Last Theorem FLT in Lean, an effort being led by Prof. Kevin Buzzard at Imperial College London. In fact, this theorem corresponds to theorem 12.7 in Appendix. Furthermore, another goal of this project is to serve as a Rosetta stone for how informal mathematics corresponds to formal mathematics; the hope is that the blueprint will serve as an example of how late undergraduate mathematics is formalised using `mathlib`, the mathematics library of Lean. A pleasant outcome of presenting both the informal and formal mathematics alongside into one cohesive website is that it allows to new ways of presenting mathematics, where the informal and formal mathematics complement each other.

1.3 How to read this blueprint

1.3.1 Navigating the blueprint

The main distinctions are due to the interactive side of this blueprint:

- In the bottom right corner there should a subset of the following buttons:
    1. Eye-minus $\boxdot^-$: Will toggle the blueprint to display less text.
    2. Eye-plus $\boxdot^+$: Will toggle the blueprint to display more text.
    3. Arrow-left $\Leftarrow$: Will navigate the page to the previous chapter
    4. Arrow-up $\Uparrow$: Will navigate the page to the index.
    5. Arrow-right $\Rightarrow$: Will navigate to the next chapter.

Important note
There are three states for toggling how much text, ordered from least to most text being displayed.

1. Displays only definitions and statements of theorems.
2. Displays definitions, statements, accompanying text and allows to toggle proofs being displayed or being hidden always
3. Displays defintions, statements, accompanying text and proofs.

1.3.2 Note on `remarks`

Any content that is within the `remark`, that is anything within a box like:

Remark 1.1 (A remark). Content of remark

environment will be dedicated towards explaining or illustrating how the mathematics formalised in Lean might differ to how the informal mathematics is often presented, may often omit implicit details, or how `mathlib` or myself have come up with particular abstractions which ease the process of formalisation.

The dependency graph

To the left of the website there should be an index which lists out the chapters of this blueprint which will eventually contain all proofs and intermediate formal statements necessary to prove the overarching claim. But, in addition to the index of chapters and bibliography there is an entry for the `Dependency graph`.

This will display a directed acyclic graph which demonstrates how all relevant definitions and statements feed into each to produce the final claim.

1.3.3 Distinguishing my work from Christopher Butler's work

Naturally, the largest bulk of my original work in this project consists of the formalisation of mathematics since Christopher Butler has kindly provided the TeX for his original master's thesis exposition on the classification of finite subgroups of $\mathrm{SL}_2(F)$. Bear in mind, the goal of the formalisation is this classification of finite subgroups of $\mathrm{PGL}_2(\bar{\mathbb{F}})$, it turns out the classifications problems are tightly related and this is why a lot of Christopher Butler's work is reused here.

Nonetheless, it may be surprising to understand that so far I having formalised around two thirds of the exposition alognside additional results relevant to concrete goal for formalising Fermat's Last Theorem. It turns out, that so far there is a rough correspondence for two lines of code/formal mathematics per one line of informal/pen-and-paper mathematics. That is to say, if 50 lines of code were displayed per page, all the code I have written would constitute a total of around 86 pages, since there are 4344 lines of Lean.

Moreover, on the basis of academic integrity I provide a rough overview of what constitutes my work and what constitutes Christopher Butler's work.

- My work:

  Chapter 2, Chapter 4, Chapter 6

- Christopher Butler's work:

  Aside from particular points where I have completely modified the approach to prove a particular statement, most proofs belong to Christopher Butler's exposition.

  Part of the intention of this is to highlight how the formal proof differs from the original informal proof;I have tried at every stage to follow the

argument within Christopher Butler's exposition. Therefore, it is my hope that comparing the informal and formal mathematics side by side should be interesting to the reader.

There are parts where I have had to stray from the original path:

- When classifying elements of $\mathrm{SL}_2(F)$ up to conjugacy.
- When formalising arguments using group homomorphisms and isomorphisms.
- When formalising arguments which hinge on the complete lattice structure of subgroups.
- When formalizing the maximal abelian subgroup class equation.

Often, I have broken up theorems into smaller lemmas to allow mapping Lean lemmas one-to-one with the corresponding lemma. This has often meant I have to define and prove intermediate definitions and theorems or prove particular statements more explicitly, and other terms, more generally.

1.4 Christopher Butler's acknowledgements and popular science summary

Considering this project hinges very heavily on the work of Christopher Butler, I feel obligated to include his own acknowledgements, abstract and popular science summary on **Dickson's Classification Theorem** for $\mathrm{SL}_2(F)$ over an algebraically closed field. I am very thankful for his work, it has been extremely useful for the process of formalisation.

1.4.1 Christopher Butler's Abstract

This paper is a reformulation of Leonard Dickson's complete classification of the finite subgroups of the two-dimensional special linear group over an arbitrary algebraically closed field, $\mathrm{SL}_2(F)$. The approach is to construct a class equation of the conjugacy classes of maximal abelian subgroups of an arbitrary finite subgroup of $\mathrm{SL}_2(F)$. In turn, this leads to only 10 possible classes of structures of this subgroup up to isomorphism.

1.4.2 Acknowledgements from Christopher Butler

I would like to take this opportunity to thank my advisor Arne Meurman. This paper would not have been possible without the guidance and insight he gave during our weekly discussions.

1.4.3 Christopher Butler's popular science summary

In order to explain what this paper is about, it is necessary to first define a few of the mathematical concepts which it concerns. A *group* is a set of objects, called *elements*, together with a rule, called an *operation*, which tells us how two elements combine with each other to make a third. Furthermore, to be considered a group it must also satisfy 4 conditions, called *axioms*. One of which is that the group must be *closed* under it's operation. This means that whenever any two elements in the group are combined, the resulting element is also part of the group. The remaining axioms require that the group must also be *associative*, have an *identity* element and each element must have an *inverse*. The way in which the elements in a group act with each other is called the group's *structure*. If 2 groups have the same number of elements and share the same structure, then they are regarded as being *isomorphic* to each other, which essentially means that they equivalent. Many everyday things can be regarded as groups, such as the symmetries of geometrical objects, or the number systems we use.

The set of 2 x 2 matrices whose *determinant* is equal to 1, together with the operation of ordinary matrix multiplication, forms a group called the *special linear group*. This is a group because the product of 2 matrices has a determinant equal to the product of the determinants of the 2 matrices, so since 1 x 1 = 1, this new element also belongs to the group, hence the axiom of being closed is satisfied. Furthermore, it is crucial that the entries in the matrices are taken from a specified *ring* or *field*. Rings and fields are, like groups, abstract mathematical objects, albeit they satisy even more axioms than groups do. Crucially, rings and fields have both an additive and a multiplicative identity.

This paper focuses on $\mathrm{SL}_2(F)$, which is the two-dimensional special linear group whose entries are taken from an *algebraically closed* field. Algebraically closed fields are infinite in size, which means that the resulting special linear group is also infinite. A *subgroup* of a group is simply a group with the added requirement that each of it's elements must also belong to the original group. Thus a finite subgroup of $\mathrm{SL}_2(F)$ is any finite set of elements belonging to this infinite group $\mathrm{SL}_2(F)$, which satisfy the 4 axioms of being a group.

This paper classifies all the possible structures which a finite subgroup of $\mathrm{SL}_2(F)$ could have. The result has implications within the study of finite *simple* groups. This classification was first done by American mathematician Leonard Eugene Dickson in 1901. The purpose of this reformulation is to make it accessible to a wider audience by providing a more detailed explanation at the various stages of the proof.

Chapter 2

Introduction

2.1 What is the formalisation of mathematics?

Formalisation of mathematics is the art of teaching a computer what a piece of mathematics means.

That is, it is the process of carefully writing down a mathematical statement typically in first order logic or higher order logic and then scrutinously justifying each step of the proof to a computer program that checks the validity of every step of the reasoning.

Typically one formalizes mathematics with the help of a proof assistant or interactive theorem prover, a piece of software which enables a human to write down mathematics and have the software verify the claims.

There exist many proof assistants, such examples are Lean, Isabelle, Coq, Metamath, etc.

For this project I have opted to use Lean due to its rapid growing mathematics library and its dependent type theory. I shall explain in more detail these last two reasons, but first I will comment on what Lean is.

What is Lean?

Lean is both a functional programming language and an interactive theorem prover (also known as a proof assistant) that is being developed at Microsoft research and AWS by Leonardo de Moura and his team. It has been designed for both use in cutting-edge mathematics and the verification of software which is often essential to safety critical systems such as medical or aviation software, where any error can have catastrophic consequences on people's lives or infrastructure.

Theorem provers like Lean harness the tight bond between proofs and programs. Often an algorithm, in fact serves as a proof for a mathematical statement

For example, such is the case for the following theorem:

Example 2.1 (Algorithm corresponds to a proof - Bézout's lemma). Let R be a ring with a euclidean function $\nu : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ which satisfies that for all $x, y \in R$ with $y \neq 0$, there exist $q, r \in \mathbb{R}$ such that $a = qb + r$ where either $r = 0$ or $\nu(r) < \nu(b)$; it is possible for any $r, s \in R$ to find a unique linear combination which is the greatest common divisor of r and s, that is, there exist coefficients $a, b \in R$ such that $ar + bs = \gcd(r, s)$.

Proof. We construct a and b by the extended euclidean algorithm, we sequentially divide in the following fashion:

$$r = q_0 s + r_1 \tag{2.1}$$
$$b = q_1 r_1 + r_2 \tag{2.2}$$
$$r_1 = q_2 r_2 + r_3 \tag{2.3}$$
$$\vdots \tag{2.4}$$
$$r_{i-1} = q_i r_i + r_{i+1} \tag{2.5}$$

by the definition of a euclidean domain, we have a strictly decreasing sequence $\nu(r_1) > \nu(r_2) > \ldots > \nu(r_k)$ that must eventually terminate in at most $\nu(r_1) + 1$ steps, and must have that $\nu(r_k) = 0$ for some $k \in \mathbb{N}$. It will then be that $r_{k-1} = \gcd(r, s)$, and by back substitution we can recover the values for the coefficients a and b. □

In `mathlib`, the extended euclidean algorithm is defined in the following way and is used to formalise Bézout's lemma

```
def xgcdAux (r s t r' s' t' : R) : R × R × R :=
if _hr : r = 0 then (r', s', t')
else
  let q := r' / r
  have _ := mod_lt r' _hr
  xgcdAux (r' % r) (s' - q * s) (t' - q * t) r s t
termination_by r
```

It is not always clear how a proof corresponds to a program, but this correspondence does exist nonetheless.

The correspondence is known as the **Curry-Howard correspondence** where formulas correspond to *types*, which correspond to the notion of a specification, proofs for formulas correspond to constructing a term of the corresponding type and so forth.

In fact it turns out that for every logic, such as classical or intuitionistic logic, there corresponds a corresponding type system which express the valid rules for programs.

For our purposes, we will not provide a deep overview of this fundamental correspondence, but rather we will illustrate the core principle with a suitable example.

Furthermore, within the block of Lean code above there was a lot of unfamiliar syntax which one is somehow meant to believe correspond to mathematics.

the following example hopes to illustrate a simpler example and give an overview of how to:

- Define the assumptions for a mathematical statement.
- Define the mathematical statement.
- Formalise the mathematical statement using Lean tactics.

Note that in the list Lean tactics are mentioned. Loosely speaking, a `tactic` is a Lean metaprogram that will write Lean programs, these (non-meta) programs can be the usual code one would write for an algorithm or it could be the program which corresponds to the proof term that one needs to construct to formalise a statement in Lean. Examples of tactics and how they are used will be illustrated in the following example.

Example 2.2 (Proving and formalising the sum of the first n odd integers). To understand how the nature of proof is preserved when passed into a theorem prover, we will compare side by side the informal and formal proofs for why the sum of the first n odd integers equals the n^{th} square. That is, we will prove and formalise:

$$\sum_{k=1}^{n} 2k - 1 = n^2 \tag{2.6}$$

There are many ways to prove this statement, other proofs can be found at [**?**]. The proof that is best suited to be formalise is the proof by induction which goes as the following:

Proof. We prove the claim holds for all $n \in \mathbb{N}$ by the principle of mathematical induction. Indeed,

- The claim holds true for $n = 1$ since the LHS is $\sum_{k=1}^{1} 2k - 1 = 1$ and the RHS is $1^2 = 1$ and indeed LHS = RHS. This proves the base case.
- Let $m \in \mathbb{N}$ be a natural number and suppose the statement (2.6) holds for $n = m$ then we will show that it then follows that it must hold for $n = m + 1$. Indeed,

  Consider the sum $\sum_{k=1}^{m+1} 2k - 1$, then we have that

$$\begin{aligned} \sum_{k=1}^{m+1} 2k - 1 &= \left(\sum_{k=1}^{m} 2k - 1 \right) + 2(m+1) - 1 \\ &\qquad \text{(by definition of the summation)} \\ &= n^2 + 2n + 1 \qquad \text{(by the induction hypothesis)} \\ &= (n+1)^2 \end{aligned} \tag{2.7}$$

  This proves the induction step, and therefore by the principle of mathematical induction. The claim holds true for all $n \in \mathbb{N}$.

□

To define this statement in Lean we first must define what we mean by $\sum_{k=1}^{n} 2k-1$, to define this sum in Lean we use the recursive definition for the summation where

$$\sum_{k=1}^{n+1} f(k) = \sum_{k=1}^{n} f(k) + f(n+1) \qquad \text{(for } n \geq 0\text{)}$$

and

$$\sum_{k=1}^{0} f(k) = 0$$

where in Lean that naturals numbers include zero.

```
def sum_of_n_odd :  →
     | 0 => 0
     | n + 1 => sum_of_n_odd n + (2*n + 1)
```

This definition of summing the odd numbers is equivalent up to reindexing to the definition above. The reason we do not use subtraction is because the natural numbers are a commutative semiring, in particular, it does not always make sense to subtract one from a natural number, the predecessor of zero is not defined. We only need understand that a natural number is either zero or a successor of a natural number. In essence, when defining a function from the natural, we only need to think about where to send zero and where to send the successor of a natural number, such functions are defined inductively/recursively. This pattern of thought is continually used throughout Lean.

Given the code definition above is a program one can indeed compute using the function, this might be how one would first conjecture that such a theorem about the sums of the first odd natural numbers is true in the first place!

To state the theorem in Lean, we use the keyword `thorem` or `lemma`; followed by the name we would like to give the theorem, in this case it is, `closed_eq_sum_of_first_n_odd_nat`; then followed by a list of arguments which will either be the objects and assumptions on the objects, in this case we only specify that `n` is a natural number; then after a colon `:`, we specify the mathematical statement, in this case that `sum_of_first_n_odd_nat n = n * n`. We will walk through the formal proof after providing the Lean code

```
theorem closed_eq_sum_of_first_n_odd_nat (n :  ) : sum_of_first_n_odd_nat n = n * n := by
    induction n
    -- Prove the base case.
    case zero =>
        rw [mul_zero, sum_of_first_n_odd_nat]
    -- Prove the induction step.
    case succ m hm =>
        rewrite [sum_of_first_n_odd_nat]
```

```
 -- Apply the induction hypothesis
rewrite [hm]
-- Multiply out the square of sum
rewrite [add_mul_self_eq]
-- We finish it off by hand
rewrite [mul_one, mul_one, add_assoc]
rfl
done
```

After the `:=` Lean expects a proof term of the type `sum_of_first_n_odd_nat n = n * n`, it is possible to define the corresponding program which constructs the term, but often it is more intuitive to enter what is known as *tactic mode*.

As outlined above, tactics are metaprograms, i. e: programs that write programs, which in this case allow the simulation of typical pen-and-paper mathematics in Lean; to enter tactic mode one must begin the proof with the `by` tactic. Furthermore, using tactic mode allows access to an extremely useful interactive *infoview* which displays the objects at play in the proof, the assumptions on the objects, the state of the proof

Once in tactic mode, we have access to other tactics accessible throught the keywords `induction`, `case`, `rw`, `rw`, `ring`, `simp` and so on. Given the natural number are defined inductively in Lean, Lean understands that to prove that a property P holds true for all natural numbers it is sufficient to provide a proof term for $P(0)$ and supposing $P(n)$ holds we can show that then $P(n+1)$ holds, in Lean terminology, the natural numbers have their own induction principle. In fact this will be automatically true for any inductive datatype, but we will not go into this.

To access this fact, we must invoke the `induction` tactic which splits the original goal of `sum_of_first_n_odd_nat n = n * n` into two smaller goals

1. The base case: `sum_of_first_n_odd_nat 0 = 0 * 0`.
2. The induction step: `sum_of_first_n_odd_nat (m + 1) = (m + 1) * (m + 1)`

The `case` tactic allows us to focus in on one of the tactics, at first we focus on the goal with the label *zero* to prove the base case; then we focus in on the induction step by typing `case succ m hm` which also introduces two new objects into the proof context, the natural number m and the assumption on `m` which says that m satisfies the induction hypothesis, `sum_of_first_n_odd_nat m = m * m`. We then proceed to use the rewrite tactic, `rewrite`, which allows to replace equal or logically equivalent terms, so if you have the theorem `h : a = b`, then `rw [h]` will replace every ocurrence of `a` in the goal for a `b`, in the new modified goal.

Finally, `rfl` proves any goal that is true by reflexivity of the given relation; in this case, we finish proving the goal by reflecivity of the equality relation. Typically, one uses the `rw` tactic which is a combination of `rewrite` followed by `rfl`.

Theorems and lemmas in Lean are given an identifier by which to access through, for example, the theorem `add_mul_self_eq` states that for all $a, b \in S$ where S is a semiring we have that `(a + b) * (a + b) = a * a + 2 * a * b + b * b`.

2.2 Fermat's Last Theorem

Problem statement and its history

Fermat's Last Theorem, before it was proved that is, A conjecture about the *Fermat equation* which is defined to be

Definition 2.3 (Fermat Equation)**.** The equation $a^n + b^n = c^n$ is Fermat's Equation

When a, b, c and n in this equation are restricted to positive integers, we are defining a particular family of what are called *Diophantine equation.* Diophantus, an ancient greek mathematician was interested in positive integers which satisfy this equation. For instance, a particular set of numbers which satisfy this equation are the *Pythagorean triples*, such triples have been known since Babylonian times. For example, when we substitute the Pythagorean triple $(a, b, c) = (3, 4, 5)$ and set $n = 2$ we find that indeed Fermat's equation holds for this choice of numbers since:

$$3^2 + 4^2 = 5^2$$

In fact, much is known about the case when $n = 2$; it is known that all Pythagorean triples are of the form:

Theorem 2.4 (Pythagorean triples)**.** *All pythagorean triples are of the form:*

$$a = r \cdot (s^2 - t^2), \qquad b = r \cdot (2st), \qquad c = r \cdot (s^2 + t^2)$$

The natural question to ask from such an extremely satisfying theorem is whether the same can be said for when $n \geq 2$. Initially, mathematicians set out to to find solutions $n = 3$. However, it seemed only the "trivial" triple satsfied Fermat's equation for when $n = 2$

$$0^3 + 1^3 = 1^3$$

Among these mathematicians was Pierre de Fermat, who suspected it was not possible to find a nontrivial triple for the exponent $n = 3$ and what is more he believed it was not possible to find any nontrivial triple for any exponent $n > 2$. In fact, Pierre de Fermat wrote in the margin of his copy of *Arithmetic* written by Diophantus: " It is impossible... for any number which is a power greater than the second to be written as the sum of two like powers

$$x^n + y^n = z^n \text{ for } n > 2.$$

I have a truly marvelous demonstration of this proposition which this margin is too narrow to contain. ”

This copy and many of Pierre de Fermat's belongings were searched in the hope of finding such a proof. Nonetheless, to this date no proof has been found.

It took Euler to provide a (flawed) proof for the nonexistence of nontrivial solutions to Fermat's equation for the exponent $n = 3$, so far so good, Fermat's conjecture held true for $n = 3$. The case where $n = 4$ was also proved by Euler; soon enough particular cases where n was some fixed natural number where being shown, which indeed seemed to suggest Fermat's conjecture was true. However, no approach seemed to generalise to prove the general case...

TODO - link paragraphs and clean up

The proof of Fermat's Last Theorem is the culmination of the effort of mathematicians spanning generations.

From Diophantus, the first known person to systematically study what we now call *Diophantine equations*, to Fermat developing the elementary theory of number theory and then due to the invaluable work of countless mathematicians around the world which built upon each other's work a list of such mathematicians contains the names of: Gauss, Galois, Euler, Abel, Dedekind, Noether, Euler, Kummer, Mazur, Kronecker, etc.

2.3 Formalizing Fermat's Last Theorem

Following the sequence of success stories ranging from the Liquid Tensor Experiment to the formalisation of the Polynomial Freiman-Rusza conjecture.

Prof. Kevin Buzzard from Imperial College London has received a five-year grant that will allow him to lead the formalisation of Fermat's Last Theorem. This grant kicked in in October of 2024.

At the time of writing, since October of 2024, a digital blueprint has been set up to manage the project.

Alongside other infrastructure like the project dashboard, mathematicians around the world can claim tasks that are set by Prof. Kevin Buzzard and if in return a task is returned with a ”sorry” free proof then one can claim the glory of having completed the task.

The first target of the formalisation of Fermat's Last Theorem

The goal of the ongoing efforts of the formalisation is to reduce the proof of Fermat's Last Theorem to results that were known in the 1980s such as Mazur's Theorem.

However, it should be mentioned that the proof being formalised is not the proof Andrew Wiles and Richard Taylor initially came up with during 1994, but a more modernised approach that has been refined over the last 20 years.

At the time of writing, the first target set by Prof. Kevin Buzzard is to formalise the **Modularity Lifting Theorem**

After all, the ultimate goal is to formalise all of mathematics and so far the library relevant to Algebraic Number Theory, Algebraic Geometry and Arithmetic Geometry is not developed enough to be even able to state the propositions and let alone formalise their corresponding proofs.

Morally, the goal of the formalisation of Fermat's Last Theorem is to formalise much of Algebraic Number Theory, Algebraic Geometry, Arithmetic Geometry and so forth so that one day the mathematics library of Lean `mathlib`, contains all mathematics known to human kind.

2.4 Classification of finite subgroups of the $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ within Fermat's Last Theorem

The primary concern of this project is to formalise Theorem 2.47 of [**?**] which states:

1. If H is finite subgroup of $\mathrm{PGL}_2(\mathbb{C})$ then H is isomorphic to one of the following groups: the cyclic group C_n of order n ($n \in \mathbb{Z}_{>0}$), the dihedral group D_{2n} of order $2n$ ($n \in \mathbb{Z}_{>1}$), A_4, S_4 or A_5.
2. If H is a finite subgroup of $\mathrm{PGL}_2(\bar{\mathbb{F}}_\ell)$ then one of the following holds:
   (a) H is conjugate to a subgroup of the upper triangular matrices;
   (b) H is conjugate to $\mathrm{PGL}_2(\mathbb{F}_{\ell^r})$ and $\mathrm{PSL}_2(\mathbb{F}_{\ell^r})$ for some $r \in \mathbb{Z}_{>0}$;
   (c) H is isomorphic to A_4, S_4, A_5 or the dihedral group D_{2r} of order $2r$ for some $r \in \mathbb{Z}_{>1}$ not divisible by ℓ

   Where ℓ is assumed to be an odd prime.

Recall that the Projective General Linear Group is defined to be:

Definition 2.5 (Projective general linear group)**.** The projective general linear group is the quotient group

$$\mathrm{PGL}_n(F) = \mathrm{GL}_n(F)/(Z(\mathrm{GL}_n(F))) = \mathrm{GL}_n(F)/(F^\times I)$$

Similarly, the Projective Special Linear Group is defined to be:

Definition 2.6 (Projective special linear group)**.**

$$\mathrm{PSL}_n(F) = \mathrm{SL}_n(F)/(Z(\mathrm{SL}_n(F))) = \mathrm{SL}_n(F)/(\langle -I \rangle)$$

At first glance, neither the statement or the definitions seem to indicate how the classification of finite subgroups of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ play a role in the proof of Fermat's Last Theorem, after all, Fermat's Last Theorem is a statement regarding natural numbers.

Upon inspection of the proof it turns out that Theorem 2.47 of [**?**] is required is for Theorem 2.49, Remark 2.47 and Lemma 4.11. Where in particular, Theorem 2.49 is a key component in Theorem 3.42 which states that:

Theorem 2.7 (Theorem 3.42)**.** *For all finite sets $\Sigma \subset \Sigma_{\bar{\rho}}$, the map $\phi_\Sigma : R_\Sigma \to \mathbb{T}_\Sigma$ is an isomorphism and these rings are complete intersections,*

There is of course a lot of notation to hidden within these statement, yet unpacking and understanding in detail the following two theorems is not at all the concern for this project. Naturally, the reference [**?**] would be the indicated source to truly understand what these statements claim and how they fit together in the big picture of proving Fermat's Last Theorem; but for completeness, very loosely the key idea is that the two key players:

1. The local ring R_Σ which is called the universal deformation ring for representations of type Σ.
2. The ring $\mathbb{T}_\Sigma$ is a Hecke algebra, defined as a subalgebra of the linear endomorphisms of a certain space of automorphic forms.

Where $\Sigma_{\bar{\rho}}$ is the set of primes p satisfying

- $p = \ell$ and $\bar{\rho}|_{G_\ell}$ is good and ordinary; or
- $p \neq \ell$ and $\bar{\rho}$ is unramified at p.

TODO - explain why this isomorphism is crucial.
Moreover, the statement of Theorem 2.49 is the following:

Theorem 2.8 (Theorem 2.49)**.** *Suppose $L = \mathbb{Q}(\sqrt{(-1)^{\ell-1}/2}\ell)$ then $\bar{\rho}$ is absolutely irreducible. Then there exists a non-negative integer r such that for any $n \in \mathbb{Z}_{>0}$ we can find a finite set of primes Q_n with the following properties.*

1. *If $q \in Q_n$ then $q \equiv 1 \mod n$.*
2. *If $q \in Q_n$ then $\bar{\rho}$ is unramified at q and $\rho(Frobq)$ has distinct eigenvalues.*
3. *$\#Q_n = r$.*

The place where the theorem 2.47 is of interest, the theorem that this project aims to be a blueprint for, is because proving proving the claim above requires showing that the cohomology group $H^1(\mathrm{Gal}(F_n/F_0), \mathrm{ad}^0\bar{\rho}(1))^G_{\mathbb{Q}}$ is trivial, which in turn reduces to showing that ℓ, an odd prime, does not divide the Galois group $\mathrm{Gal}(F_0/\mathbb{Q})$ which is isomorphic to a finite subgroup $\mathrm{PGL}_2(\bar{\mathbb{F}}_\ell)$ and has $\mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})$ as a quotient.

Provided the classification of finite subgroups of $\mathrm{PGL}_2(\bar{\mathbb{F}}_\ell)$, it suffices to prove that the cohomology group is trivial for the case where $\ell = 3$.

This explains in a very vauge fashion why the classification of finite subgroups of $\mathrm{PGL}_2(\bar{\mathbb{F}})$ is relevant to proving Fermat's Last Theorem.

2.5 Overview and reduction to the classification problem

Returning to the domain of the problem of interest, classifying finite subgroups of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$.

Observing that $\bar{\mathbb{F}}_p$ is by construction an algebraically closed field, since it is the algebraic closure of $\mathbb{F}_p$; it turns out that for any $n \in \mathbb{N}$, we can show that $\mathrm{PGL}_n(F)$ is isomorphic to $\mathrm{PSL}_n(F)$ and thus we only need consider finite subgroups of $\mathrm{PSL}_2(\bar{\mathbb{F}})$.

Furthermore, on the back of the isomorphism defined between $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ and $\mathrm{PSL}_2(\bar{\mathbb{F}}_p)$, and determining that the center $Z(\mathrm{SL}_2(\bar{\mathbb{F}}_p)) = \langle -I \rangle$, we can in fact focus on the much more tractable problem of classifying the finite subgroups of $SL_2(\bar{\mathbb{F}}_p)$ to eventually classify the finite subgroups of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$. Moreover, since the more general problem of classifying the finite subgroups of $\mathrm{SL}_2(F)$ where F is an arbitrary algebraically closed field yields a statement very close to the desired statement and Christopher Butler has a in-depth exposition of this result, the formalisation of slightly more general result was chosen.

Considering proving the existence of such an isomorphism $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ and $\mathrm{PSL}_2(\bar{\mathbb{F}}_p)$ is no more difficult in the general case, the goal of the next chapter will be to formalise the definition of a suitable homomorphism between $\mathrm{PGL}_n(F)$ and $\mathrm{PSL}_n(F)$, where F is an algebraically closed field, and formally prove in the Lean proof assistant that this homomorphism actually defines an isomorphism.

Chapter 3

Preliminaries

This section briefly outlines some standard group theory results which perhaps may not have been covered in a first course in Group Theory. Since they are not the main focus of this paper, most of the proofs have been omitted. A more advanced reader may choose to skip this first chapter, using it only for reference purposes as and when the results are subsequently cited.

3.1 Some Elementary Theorems

The following theorems are all well-known fundamental results in group theory. If the reader is interested in the proofs, they can be found in Hungerford [**?**].

Theorem 3.1 (Lagrange's theorem)**.** *Let G be a finite group. Then the order of any subgroup of G divides the order of G.*

Theorem 3.2 (First isomorphism theorem)**.** *Let $\phi : G \to G'$ be a homomorphism of groups. Then,*

$$G/\ker\ \phi \cong Im\ \phi.$$

Hence, in particular, if ϕ is surjective then,

$$G/\ker\ \phi \cong G'.$$

Theorem 3.3 (Second isomorphism theorem)**.** *Let H and N be subgroups of G, and $N \lhd G$. Then, $H/H \cap N \cong HN/N$.*

Theorem 3.4 (Third isomorphism theorem)**.** *Let H and K be normal subgroups of G and $K \subset H$. Then H/K is a normal subgroup of G/K and,*

$$(G/K)/(H/K) \cong G/H.$$

Theorem 3.5 (Cauchy's theorem)**.** *If the order of a finite group G is divisible by a prime number p, then G has an element of order p.*

3.2 Sylow Theory

In 1872, Norweigian mathematician Peter Ludwig Sylow published his theorems regarding the number of subgroups of a fixed order that a given finite group contains. Today these are collectively known as the Sylow Theorems and play a vital role in determining the structure of finite groups. I will use the results of these theorems several times throughout this paper and I state them here without proof. If the reader would like to read further, the proofs can be found in most introductory texts on group theory, such as Bhattacharya [**?**], except Corollary **??** which can be found in Alperin and Bell [**?**, p.64] .

Definition 3.6 (Sylow p-subgroup)**.** Let G be a finite group and p a prime, a **Sylow *p*-subgroup** of G is a subgroup of order p^r, where p^{r+1} does not divide the order of G.

Let p be a prime. A group G is called a ***p*-group** if the order of each of it's elements is a power of p. Similarly, a subgroup H of G is called a ***p*-subgroup** if the order of each of it's elements is a power of p.

Remark 3.7 (Sylow p-subgroup in Lean). TODO

In each of the following results, G is a finite group of order $p^r m$, where p is a prime which does not divide m.

Theorem 3.8 (Sylow's first theorem)**.** *If p^k divides $|G|$, then G has a subgroup of order p^k.*

Theorem 3.9 (Sylow's second theorem)**.** *All Sylow p-subgroups of G are conjugate.*

Theorem 3.10 (Sylow's third theorem)**.** *The number of Sylow p-subgroups n_p divides m and satisfies $n_p \equiv 1 (mod\ p)$.*

Corollary 3.11 (Sylow's fourth theorem)**.** *A Sylow p-subgroup of G is unique if and only if it is normal.*

Corollary 3.12 (Sylow's fifth theorem)**.** *Any p-subgroup of G is contained in a Sylow p-subgroup.*

3.3 Group Action

Definition 3.13. Let G be a group and X be a set. Then G is said to **act** on X if there is a map $\phi : G \times X \to X$, with $\phi(a, x)$ denoted by a^*x, such that for

$a, b \in G$ and $x \in X$, the following 2 properties hold:

$$(i) \quad a^*(b^*x) = (ab)^*x,$$
$$(ii) \quad {I_G}^*x = x.$$

The map ϕ is called the **group action** of G on X.

Definition 3.14. Let G be a group acting on a set X and let $x \in X$. Then the set,

$$Stab(x) = \{g \in G : gx = x\},$$

is called the **stabiliser** of x in G. Each g in $S_G(x)$ is said to **fix** x, whilst x is said to be a **fixed point** of each g in $S_G(x)$. Also, the set,

$$\text{Orb}(x) = \{gx : g \in G\},$$

is called the **orbit** of x in G.

The orbit and the stabiliser of an element are closely related. The following theorem is a consequence of this relationship and it will be useful throughout this paper.

Theorem 3.15 (Orbit-Stabilizer theorem)**.** *Let G be a finite group acting on a set X. Then for each $x \in X$,*

$$|G| = |Orb(x)||Stab(x)|.$$

The following standard theorem will all play a vital roll later on.

Theorem 3.16. *Let G be a group and H a subgroup of G of finite index n. Then there is a homomorphism $\phi : G \longrightarrow S_n$ such that,*

$$\ker(\phi) = \bigcap_{x \in G} xHx^{-1}.$$

Proof. See [**?**, p.110] for proof. □

3.4 Conjugation

Definition 3.17 (Conjugate elements)**.** Let G be a group and a an element of G. An element $b \in G$ is said to be **conjugate** to a if $b = xax^{-1}$ for some $x \in G$.

Remark 3.18. In Lean, to state that two elements $g, h \in G$ where G is a group, we use the slightly more general definition of conjugacy over monoids.

That is to say, given $g, h \in G$ where G is a group (or more generally monoid) and impose that g and h are conjugate, instead of writing the equality which has type `Prop`:

We use the following statement of type `Prop` that has been defined in Mathlib under the name of `IsConj`.

The reason we would choose this over the naive statement is because Mathlib will contain a lot of very useful lemmas attached to this definition.

Saying two elements are conjugate is writing something like the following:

Assuming the terms `g : G` and `h : G` of the type `G` (which has the `Group` typeclass instance) are in scope.

Definition 3.19 (Conjugate subgroups). Let H_1 be a proper subgroup of G and fix $x \in G \setminus H_1$. The set $H_2 = \{g \in G : g = xh_1x^{-1}, \forall h_1 \in H_1\}$ is said to be a **conjugate subgroup** of H_1. We write $H_2 = xH_1x^{-1}$. It is trivial to show that H_2 is a subgroup of G.

Remark 3.20. In Lean, to state that two subgroups H, K of a group G are conjugate subgroups similar to how is done in 3.18 we can open the `MulAut` namespace to make use of the custom syntax:

This notation and API is useful because conjugation by a particular element is defined to be an element in the automorphism group of G, $\mathrm{Aut}(G)$.

This becomes particularly crucial when formalizing the interactions of subgroups with the complete lattice structure on the set of subgroups of a group.

These interactions and more discussion about this lattice structure will happen later on.

Conjugation plays an important roll thoughout the paper, particularly, the following properties about conjugate elements and subgroups.

Proposition 3.21. *Let a, b be conjugate elements of a group G and A, B be conjugate subgroups of G. If either a or b has finite order, then both a and b have the same order.*

Proof. Since a and b are conjugate elements in G, $b = xax^{-1}$ for some $x \in G$. Suppose that b has finite order and $b^k = I_G$ for some $k \in \mathbb{Z}^+$,

$$I_G = b^k = (xax^{-1})^k = xa^kx^{-1} \Rightarrow a^k = I_G.$$

Alternatively suppose that a has finite order and $a^k = I_G$ for some $k \in \mathbb{Z}^+$,

$$a^k = I_G \Rightarrow I_G = xa^kx^{-1} = (xax^{-1})^k = b^k.$$

Thus $a^k = I_G \iff b^k = I_G$. Thus a and b have the same order.

□

Proposition 3.22. *Let A and B be conjugate subgroups of G. Then $A \cong B$.*

Proof. Since A and B are conjugate, there exists some $x \in G$ such that $B = xAx^{-1}$. Define the map ϕ by,

$$\begin{aligned} \phi : A &\longrightarrow xAx^{-1}, \\ a_1 &\longmapsto xa_1x^{-1}. \qquad (\forall\ a_1 \in A) \end{aligned}$$

We show that ϕ is a homomorphism between A and $B = xAx^{-1}$.

$$\phi(a_1a_2) = xa_1a_2x^{-1} = (xa_1x^{-1})(xa_2x^{-1}) = \phi(a_1)\phi(a_2).$$

Now consider an arbitrary $k \in \ker(\phi)$.

$$k \in \ker(\phi) \iff \phi(k) = I_G \iff xkx^{-1} = I_G \iff k = I_G.$$

So $\ker(\phi) = \{I_G\}$ which means ϕ is injective. Now let $b_1 \in B = xAx^{-1}$. Thus $b_1 = xa_1x^{-1}$ for some $a_1 \in A$. Since $a_1 \in A$, $\phi(a_1) = xa_1x^{-1} = b_1$ and so ϕ is surjective. Thus ϕ is an isomorphism and A and B are isomorphic.

□

The final part of this proposition is an important result which shows that since conjugate subgroups are isomorphic, conjugation preserves group structure and properties. In particular, conjugate subgroups have the same cardinality and if one is abelian or cyclic, then so is the other.

3.5 Automorphism

Definition 3.23. An **automorphism** of a group G is a isomorphism from G onto itself. The set of all automorphisms of G forms a group under composition and is denoted by $Aut(G)$.

An **inner automorphism** is an automorphism whereby G acts on itself by conjugation. That is, each $g \in G$ induces a map, $i_g : G \to G$, where $i_g(x) = gxg^{-1}$ for each $x \in G$. The set of all inner automorphisms is denoted by $Inn(G)$ and is a normal subgroup of $Aut(G)$ (For proof of this see [**?**, p.104].

3.6 Direct Product

Definition 3.24. If $G_1, G_2, ..., G_n$ are groups, we define a coordinate operation on the Cartesian product $G_1 \times G_2 \times ... \times G_n$ as follows:

$$(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) = (a_1b_1, a_2b_2, ..., a_nb_n),$$

where $a_i, b_i \in G_i$. It is easy to verify that $G_1 \times G_2 \times ... \times G_n$ is a group under this operation. This group is called the **direct product** of $G_1, G_2, ..., G_n$.

Lemma 3.25. *SpecialSubgroups.prod$_m$ulEquiv$_j$oin$_o$f$_d$isjoint$_o$f$_n$ormalLetAandBbenormalsubgroupsofGwithA* $\cap B = \{I_G\}$. *Then* $AB \cong A \times B$.

Proof. First note that the elements of A commute with the elements of B, since $\forall\ a \in A$ and $b \in B$,

$$\begin{aligned} aba^{-1}b^{-1} &= a(ba^{-1}b^{-1}) \in A, && \text{(since } A \lhd G\text{)} \\ aba^{-1}b^{-1} &= (aba^{-1})b^{-1} \in B. && \text{(since } B \lhd G\text{)} \end{aligned}$$

Therefore $aba^{-1}b^{-1} \in A \cap B = \{I_G\}$, and $ab = ba$.

Define the operation $*$ on $A \times B$ by $(a_1, b_1) * (a_2, b_2) = (a_1a_2, b_1b_2)$. Now define the map ϕ by,

$$\begin{aligned} \phi : A \times B &\longrightarrow AB, \\ (a, b) &\longmapsto ab. && (\forall\ a \in A,\ b \in B) \end{aligned}$$

We show that ϕ is a homomorphism between $A \times B$ and AB.

$$\begin{aligned} \phi((a_1, b_1) * (a_2, b_2)) &= \phi(a_1a_2, b_1b_2) \\ &= a_1a_2b_1b_2 \\ &= a_1b_1a_2b_2 \\ &= \phi(a_1, b_1)\phi(a_2, b_2). \end{aligned}$$

Thus ϕ is a homomorphism and clearly surjective. It remains to show that it is injective.

$$\begin{aligned} \phi(a_1, b_1) &= \phi(a_2, b_2), \\ a_1b_1 &= a_2b_2, \\ a_1b_1b_2^{-1} &= a_2, \\ b_1b_2^{-1} &= a_1^{-1}a_2 \in A \cap B. \end{aligned}$$

Since $A \cap B = \{I_G\}$, we have $b_1b_2^{-1} = I_G = a_1^{-1}a_2$ and so $b_1 = b_2$, $a_1 = a_2$ and ϕ is injective. So ϕ is an isomorphism and $AB \cong A \times B$.

□

Remark 3.26 (Internal direct product of subgroups). Given the product of subgroups is not necessarily a subgroup. It does not make sense to define the product of two subgroups as having the type of a subgroup.

To be clear, it is be possible to define this type provided the appropriate assumptions such as for example disjointness and normality of the subgroups, but what turns out to be much more sensible in the bigger picture is to again harness the complete lattice structure on subgroups. It is often the case subgroups do not statisfy the appropriate conditions for the pointwise product of sets to be a subgroup, but still one wants to define the smallest subgroup which contains both subgroups, whether it turns out to be the pointwise product of the subgrops or something larger.

This notion corresponds to taking the supremum or join of two subgroups `H : Subgroup G` and `K : Subgroup G` which denoted by

Naturally, as expected $H \leq H \sqcup K$ and $K \leq H \sqcup K$. Furthermore, if we now supply the appropriate assumptions, when peeking at the different facets of the supremum we will be able to recover the properties we desire.

For instance, the theorem `Subgroup.mul_normal`.

only requires one of the subgroups to be normal for us to conclude that the underlying set of the supremum is the pointwise product of sets!

Bringing the lattice of subgroups to the forefront turns out to be extremely useful for formalising arguments, and more generally, makes the arguments much more transparent.

Lemma 3.27. *Let A and B be subgroups of G. If $A \cap B = \{I_G\}$ and $ab = ba$ $\forall a \in A$, $b \in B$. Then $AB \cong A \times B$.*

Proof. Since A and B commute, the argument outlined in Lemma 3.25 also holds here. □

Chapter 4

Reduction of classification of finite subgroups of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ to classification of finite subgroups of $\mathrm{PSL}_2(\bar{\mathbb{F}}_p)$

4.1 Over an algebraically closed field $\mathrm{PSL}_n(F)$ is isomorphic to the projective $\mathrm{PGL}_n(F)$

When F is algebraically closed and $\mathrm{char}(F) \neq 2$ we can construct an isomorphism between the projective special linear group and the projective general linear group.

Definition 4.1. $\mathrm{SL}_m onoid Hom_P GL Let \varphi : \mathrm{SL}_n(R) \to \mathrm{PGL}_n(R)$ be the injection of $\mathrm{PSL}_n(R)$ into $\mathrm{PGL}_n(R)$ defined by

$$S \mapsto i(S)\ (R^\times I)$$

where $i : \mathrm{SL}_n(F) \hookrightarrow \mathrm{GL}_n(F)$ is the natural injection of the special linear group into the general linear group.

```
def SL_monoidHom_GL  (n : Type*) [Fintype n] [DecidableEq n] (R : Type*) [CommRing R] :
    SL n R →* GL n R := SpecialLinearGroup.toGL
```

We prove a useful fact about elements that belong to the center of $\mathrm{GL}_n(R)$:

Lemma 4.2. $General Linear Group.mem_c enter_g eneral_l inear_g roup_i f f Let R be a commutative ring, then G \in GL_n(F)$ *belongs to center of* $\mathrm{GL}_n(R)$, $Z(\mathrm{GL}_n(R))$ *if and only if* $G = r \cdot I$ *where* $r \in R^\times$.

Proof.

- Suppose $G \in GL_n(F)$ belongs to $Z(\mathrm{GL}_n(F))$ then for all $H \in \mathrm{GL}_n(F)$ we have that $GH = HG$. We will find it sufficient to only consider the case where H is a transvection matrices. Let $1 \leq i < j \leq n$, then the transvection matrices are of the form $T_{ij} = I + E_{ij}$ where E_{ij} is the standard basis matrix given by

$$E_{ij_{kl}} = \begin{cases} 1 & \text{if } i = k \text{ and } l = j \\ 0 & \text{otherwise} \end{cases}$$

  Given $T_{ij}G = (I + E_{ij})G = GT_{ij}(I + E_{ij})$, and addition is commutative we can use the cancellation law to yield that

$$E_{ij}G = GE_{ij}$$

  But G only commutes with E_{ij} for all $i \neq j$ if $G = r \cdot I$ for some $r \in R^\times$.

- Suppose $G = r \cdot I$ for some $r \in R^\times$ then it is clear that for all $H \in \mathrm{GL}_n(F)$ that $r \cdot IH = r \cdot H = H \cdot r = H(r \cdot I)$

□

```
theorem mem_center_general_linear_group_iff {n : Type u} [DecidableEq n]
    [Fintype n] {R : Type*} [CommRing R] {M : GL n R} :
    M  center (GL n R)  ( r : R , (r • 1) = M) := by
    rw [mem_center_iff]
    refine ?mp, ?mpr
    case mp =>
      intro hM
      -- If M commutes with every matrix then it must commute with the transvection matrices
      have h :  (t : TransvectionStruct n R), Commute (t.toGL) M := fun t => hM t.toGL
      /-
      If M commutes with the transvection matrices,
      then M  Set.range (Matrix.scalar n) where Set.range is R
      -/
      simp_rw [← Commute.units_val_iff] at h
      have h : (M : Matrix n n R)  Set.range (Matrix.scalar n) :=
        mem_range_scalar_of_commute_transvectionStruct h
      obtain r, rfl :=
        mem_range_unit_scalar_of_mem_range_scalar_and_mem_general_linear_group h
      use r
    case mpr =>
      intro hM N
      obtain r, rfl := hM
      ext i j
      simp [GeneralLinearGroup.coe_mul, GeneralLinearGroup.coe_mul,
        ← coe_scalar_matrix, scalar_commute]
```

Lemma 4.3. *$SL_monoidHom_PGLcenter_SL_le_kerLetRbeanon-trivialcommutativering, thenZ($*$\mathrm{SL}_n(R)) \subseteq \ker(\varphi)$.

Proof. GeneralLinearGroup.mem$_c$*enter$_g$eneral$_l$inear$_g$roup$_i$ff If* S $\in Z(\mathrm{SL}_n(R)) \leq \mathrm{SL}_n(F)$ then $S = \omega I$ where ω is a primitive root of unity.

Because $\varphi = \pi_{Z(\mathrm{GL}_n(F))} \circ i$, the kernel of φ is $i^{-1}(Z(\mathrm{GL}_n(F)))$, where we recall that $i : \mathrm{SL}_n(R) \hookrightarrow \mathrm{GL}_n(F)$ is the injection of $SL_n(F)$ into $\mathrm{GL}_n(F)$.

But given $i(S) = i(\omega \cdot I) = \omega \cdot I$ is of the form $r \cdot I$ where $r \in R^\times$ by 4.2 it follows that $S \in \ker \varphi$, as desired. □

```
lemma center_SL_le_ker (n : Type*) [Fintype n] [DecidableEq n]
    (R : Type*) [CommRing R]:
    center (SpecialLinearGroup n R)  (SL_monoidHom_PGL n R).ker := by
    cases hn : isEmpty_or_nonempty n
    · exact le_of_subsingleton
    · intro x x_mem_center
      rw [SpecialLinearGroup.mem_center_iff] at x_mem_center
      obtain  , h , h  := x_mem_center
      simp [MonoidHom.mem_ker, SL_monoidHom_PGL, GL_monoidHom_PGL, SL_monoidHom_GL]
      rw [GeneralLinearGroup.mem_center_general_linear_group_iff]
      have IsUnit_ : IsUnit  := IsUnit.of_pow_eq_one h  Fintype.card_ne_zero
      use IsUnit_ .unit
      ext
      simp only [coe, ← h, scalar_eq_smul_one]
      rfl
```

Definition 4.4. $\mathrm{SL}_m onoid Hom_P GLPSL_m onoid Hom_P GLGiven \mathrm{Z}(\mathrm{SL}_n(F)) \leq \ker \varphi$ as shown in 4.3, by the universal property there exists a unique homomorphism $\bar{\varphi} : \mathrm{PSL}_n(F) \to \mathrm{PGL}_n(F)$ which is the lift of φ. Where $\varphi = \bar{\varphi} \circ \pi_{Z(\mathrm{SL}_n(F))}$ and $\pi_{Z(\mathrm{SL}_n(F))} : \mathrm{SL}_n(F) \to \mathrm{PSL}_n(F)$ is the canonical homomorphism from the group into its quotient.

```
def PSL_monoidHom_PGL (n R : Type*) [Fintype n] [DecidableEq n] [CommRing R] :
    PSL n R →* PGL n R :=
    @QuotientGroup.lift (SL n R) _ (center (SL n R)) (center_is_normal n R) (PGL n R)
      (PGL_is_monoid n R) (SL_monoidHom_PGL n R) (center_SL_le_ker n R)
```

Lemma 4.5. $Injective_P SL_m onoid Hom_P GLPSL_m onoid Hom_P GLThehomomorphismisinjective.$

```
theorem Injective_PSL_monoidHom_PGL  (n F : Type*) [hn  : Fintype n] [DecidableEq n]
    [Field F] [IsAlgClosed F] :  Injective (PSL_monoidHom_PGL n F) := by
    rw [← MonoidHom.ker_eq_bot_iff, eq_bot_iff]
    intro psl psl_in_ker
    obtain  S, hS  := Quotient.exists_rep psl
    rw [← hS] at psl_in_ker
    simp only [PSL_monoidHom_PGL, SL_monoidHom_PGL, GL_monoidHom_PGL, SL_monoidHom_GL,
      MonoidHom.mem_ker, QuotientGroup.lift_mk, MonoidHom.coe_comp, QuotientGroup.coe_mk',
      Function.comp_apply, QuotientGroup.eq_one_iff] at psl_in_ker
    rw [GeneralLinearGroup.mem_center_general_linear_group_iff] at psl_in_ker
    obtain  , h  := psl_in_ker
    have  _eq_root_of_unity : det S.val = 1 := SpecialLinearGroup.det_coe S
    simp [GeneralLinearGroup.ext_iff, SpecialLinearGroup.toGL] at h
    have S_eq_omega_smul_one : (S : Matrix n n F) =   • 1 := Eq.symm (Matrix.ext h )
    simp [S_eq_omega_smul_one] at  _eq_root_of_unity
    simp [← hS]
    refine SpecialLinearGroup.mem_center_iff.mpr ?_
    use
    refine  ? _is_root_of_unity, ?S_is_scalar_matrix
    case  _is_root_of_unity => exact (eq_one_iff_eq_one_of_mul_eq_one  _eq_root_of_unity).mpr rfl
    case S_is_scalar_matrix => rw [S_eq_omega_smul_one]; exact scalar_eq_smul_one n F ↑
```

Remark 4.6 (Quotients and universal properties in Lean). When formalising results on quotient groups or for that matter as will be seen later on in the blueprint, any type of quotient. It is valuable to appreciate which model `mathlib` uses for quotients. At undergraduate level mathematics, when thinking of the elements of a quotient group one typically thinks of cosets as being the elements

However, in Lean the way quotient groups are constructed is much more abstract, and there is a good reason for this; the terms of quotient groups are objects where the only thing we care about this objects is how the map into another group or how a group maps into them, and it is typically the case that this is closely related to the original group previous to taking the quotient.

The key property that is of interest when proving mathematics is the universal property.

Proof. GeneralLinearGroup.mem$_c enter_g eneral_l inear_g roup_i f f$

To show $\bar{\varphi}$ is injective we must show that $\ker \bar{\varphi} \leq \bot_{\mathrm{PSL}_n(F)}$ where $\bot_{\mathrm{PSL}_n(F)}$ is the trivial subgroup of $\mathrm{PSL}_n(F)$.

Let $[S] \in \mathrm{PSL}_n(F)$ and suppose $[S] \in \ker \bar{\varphi}$. If $[S] \in \ker \bar{\varphi}$ then $\bar{\varphi}([S]) = [1]_{\mathrm{PGL}_n(F)}$. But on the other hand, $\bar{\varphi}([S]) = \varphi(s)$ and so $\varphi(S) = 1_{\mathrm{PGL}_n(F)}$

and thus $S \in Z(\mathrm{GL}_n(F))$, from 4.2 it follows that $s = r \cdot I$ for some $r \in R^\times$. But given the restriction of $S \in \mathrm{SL}_n(F)$ we know that

$$\det(S) = \det(r \cdot I) = r^n = 1 \implies r \text{ is a } n^{\text{ th}} \text{ root of unity}$$

Therefore, given elements of $Z(\mathrm{SL}_n(F))$ are those matrices of the form $\omega \cdot I$ where ω is a n^{th} root of unity, we can conclude that $[S] = [1]_{\mathrm{PSL}_n(F)}$ and thus $\ker \bar{\varphi} \leq \bot_{\mathrm{PSL}_n(F)}$ as required.

Which shows that the homomorphism $\bar{\varphi}$ is injective. □

Before we can show that $\bar{\varphi}$ is surjective we need the following lemma which allows us to find a suitable representative for an arbitrary element of $\mathrm{PGL}_n(F)$.

Lemma 4.7. *exists$_S$ L$_e$q$_s$caled$_G$ L$_o$f$_I$sAlgClosedIfFisanalgebraicallyclosedfieldthenforevery* $G \in \mathrm{GL}_n(F)$ *there exists a nonzero constant* $\alpha \in F^\times$ *and an element* $S \in \mathrm{SL}_n(F)$ *such that*

$$G = \alpha \cdot S$$

Proof. Let $G \in \mathrm{GL}_n(R)$ then define

$$P(X) := X^n - \det(G)$$

By assumption F is algebraically closed and $\det(G) \in F^\times$ thus there exists a root $\alpha \in F^\times$ such that

$$\alpha^n - \det(G) = 0 \iff \alpha = \sqrt[n]{\det(G)}$$

Let $S = \frac{1}{\alpha} \cdot G$, by construction $S \in \mathrm{SL}_n(F)$ as

$$\det(S) = \left(\frac{1}{\alpha}\right) \cdot \det(G) = \frac{1}{\det(G)} \det(G) = 1$$

□

Lemma 4.8. $PSL_m onoid Hom_P GL Surjective_P SL_m onoid Hom_P GL The map is surjective.$

Proof. $\text{exists}_S L_e q_s caled_G L_o f_I s Alg Closed Let \mathrm{G} \quad (\mathrm{F}^\times I) = [G] \in \mathrm{PGL}_n(F)$, then $G \in \mathrm{GL}_n(F)$ we can find a representative of $[G']$, that lies within the special linear group. Given elements of the special linear group are matrices with determinant equal to one, we must scale G to a suitable factor to yield a representative which lies within $\mathrm{SL}_n(F)$. Suppose $\det(G) \neq 1$ and let

$$P(X) := X^n - \det(G) \in F[X]$$

By assumption, F is algebraically closed so there exists a root $\alpha \neq 0 \in F$ such that

$$\alpha^n - \det(G) = 0 \iff \alpha^n = \det(G)$$

We can define

$$G' := \frac{1}{\alpha} \cdot G \quad \text{where} \quad \det(G') = \frac{1}{\alpha^n} \det(G) = 1.$$

Thus $G' \in \mathrm{SL}_n(F) \leq \mathrm{GL}_n(F)$ and given $G' = \frac{1}{\alpha} G$ we have that $G'\ (F^\times I) = G\ (F^\times I)$.

Therefore, $\varphi(G') = i(G')(F^\times I) = G'(F^\times I) = G(F^\times I)$. □

Lemma 4.9. $PSL_m onoid Hom_P GL Bijective_P SL_m onoid Hom_P GL The map is bijective$

Proof. $\text{Injective}_P SL_m onoid Hom_P GL, Surjective_P SL_m onoid Hom_P GL We have shown that is injective in 4.5 an$ to $\mathrm{PGL}_n(F)$. □

Theorem 4.10. $PSL_m onoid Hom_P GL PGL_i so_P SLI f F is an algebraically closed field, then the map$ *:* $\mathrm{PSL}_n(F) \to \mathrm{PGL}_n(F)$ *defines a group isomorphism between* $\mathrm{PSL}_n(F)$ *and* $\mathrm{PGL}_n(F)$.

Proof. $\text{Bijective}_P SL_m onoid Hom_P GL The map was shown to be a bijection in 4.9 and given is mulitplicative as it was$ we can conclude that $\bar{\varphi}$ defines a group isomorphism between $\mathrm{PSL}_n(F)$ and $PGL_n(F)$ □

This isomorphism will be essential to the classification of finite subgroups of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$, as we only need understand a the classification of subgroups of $\mathrm{PSL}_2(F)$ structure to reach our desired result.

4.2 Christopher Butler's exposition

Following from the isomorphism defined in the previous section, we can now proceed to classify the finite subgroups of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ by classifying the finite subgroups of $\mathrm{PSL}_2(\bar{\mathbb{F}}_p)$. In turn, one can begin classifying the finite subgroups of $\mathrm{PSL}_2(\bar{\mathbb{F}}_p)$ by classifying the finite subgroups of $\mathrm{SL}_2(\bar{\mathbb{F}}_p)$ and then considering what happens after quotienting by the center, $Z(\mathrm{SL}_2(F)) = \langle -I \rangle$.

We now turn our attention to the more general setting when F is an arbitrary field that is algebraically closed, as this will turn out to be sufficient for our purposes.

Given $|\langle -I \rangle| = 2$ when $\mathrm{char}F \neq 2$ and $\langle -I \rangle = \perp$ when $\mathrm{char}F = 2$. When a finite subgroup of $\mathrm{SL}_2(F)$ is sent through the canonical mapping $\pi_{Z(\mathrm{SL}_2(F))} : \mathrm{SL}_2(F) \to \mathrm{PSL}_2(F)$ the resulting subgroup will at most shrink by a factor of two or remain intact should the center not be contained within the subgroup.

We now proceed to classify all finite subgroups of $\mathrm{SL}_2(F)$ when F is algebraically closed field. From now on, we follow Christopher Butler's exposition of Dickson's classification of finite subgroups of $\mathrm{SL}_2(F)$ over an algebraically closed field F.

Christopher has been kind enough to provide the TeX code so I could prepare this blueprint which crucially hinges on the result which his exposition covers.

Chapter 5

Properties of the two dimensional $\mathrm{SL}_2(F)$

5.1 General Notation

Throughout this paper, F will denote an arbitrary algebraically closed field. The letter p will be used to denote the characteristic of F. Recall that the definition of the characteristic of a field is:

Definition 5.1 (Characteristic of a field). Let F be a field, the characteristic of a field, denoted by $\mathrm{char}(F) \in \mathbb{N}$, is the smallest natural number $p \in \mathbb{N}_0$ such that

$$\underbrace{1 + \ldots + 1}_{p} = 0$$

where in the case there is no such number then $p = 0$.

Example 5.2. $\mathbb{Z}/p\mathbb{Z}$ is a field of characteristic $\mathrm{char}(\mathbb{Z}/p\mathbb{Z}) = p$ as $p \cdot 1 = 0$.

Example 5.3. The field $\mathbb{Q}$ is a field with $\mathrm{char}(\mathbb{Q}) = 0$ as $n \cdot 1 \neq 0$ for all $n \in \mathbb{N} \subset \mathbb{Q}$.

Remark 5.4 (The characteristic is either prime or zero). The characteristic of a field is either a prime number or zero.

Unless otherwise stated, the letters $\alpha, \beta, \gamma, \delta$ and σ will denote elements of F; whereas δ and ρ will denote elements of $F^\times$, where $F^\times$ are the invertible, or equivalently, non-zero elements of F.

5.2 Subsets of $\mathrm{SL}_2(F)$

In this chapter we make some useful observations about specific elements and subgroups of $\mathrm{SL}_2(F)$.

First, we define the following elements of $\mathrm{SL}_2(F)$.

Special matrices of $\mathrm{SL}_2(F)$

Definition 5.5 (The diagonal matrix of $SL_2(F)$). SpecialMatrices.d Given an element $\delta \in F^\times$ we define the diagonal matrix:

$$d_\delta = \begin{bmatrix} \delta & 0 \\ 0 & \delta^{-1} \end{bmatrix}$$

Definition 5.6 (The shear matrix of $SL_2(F)$). SpecialMatrices.s Given an element $\delta \in F$ we define the shear matrix:

$$s_\sigma = \begin{bmatrix} 1 & 0 \\ \sigma & 1 \end{bmatrix}$$

We record the nice property of s_σ

Definition 5.7 (Rotation by $\pi/2$ radians matrix). SpecialMatrices.w We denote the matrix which corresponds to a rotation by $\pi/2$ radians to be:

$$w = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

The matrices d, s and w satisfy the following relations:

Lemma 5.8 (Closure of D under multiplication). *SpecialMatrices.d SpecialMatrices.*$d_m ul_{de} q_{dm} ul Forany \delta, \rho \in F^\times$ *we have that*

$$d_\delta d_\rho = d_{\delta\rho}$$

Proof. We verify by matrix multiplication that indeed:

$$d_\delta d_\rho = \begin{bmatrix} \delta & 0 \\ 0 & \delta^{-1} \end{bmatrix} \begin{bmatrix} \rho & 0 \\ 0 & \rho^{-1} \end{bmatrix} = \begin{bmatrix} \delta\rho & 0 \\ 0 & \delta^{-1}\rho^{-1} \end{bmatrix} = d_{\delta\rho}.$$

□

Lemma 5.9 (Closure of S under multiplication). *SpecialMatrices.s SpecialMatrices.*$s_m ul_{se} q_{sa} dd Forany \sigma, \gamma \in F$ *we have that*

$$s_\sigma s_\gamma = s_{\sigma+\gamma}.$$

Proof. We verify by matrix multiplication that indeed:

$$s_\sigma s_\gamma = \begin{bmatrix} 1 & 0 \\ \sigma & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \gamma & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \sigma+\gamma & 1 \end{bmatrix} = s_{\sigma+\gamma}.$$

□

Lemma 5.10. *SpecialMatrices.s SpecialMatrices.*$s_p ow_e q_{sm} ul Forany \sigma \in F$ *and for any* $n \in \mathbb{N}$*, we have that* $s_\sigma^n = s_{n\cdot\sigma}$

Proof. SpecialMatrices.s$_m$u$l_{se}q_{sa}$ddWeprovethisbyinduction, $indeedfor$n= 0$theidentityholdstrivially.$
Suppose $s_\sigma^n = \begin{bmatrix} 1 & 0 \\ n \cdot \sigma & 0 \end{bmatrix}$ then consider $s_\sigma^(n+1)$. Since

$$s_\sigma^(n+1) = s_\sigma^n s_\sigma = s_{n\cdot\sigma} s_\sigma = s_{(n+1)\sigma}$$

□

Lemma 5.11 (Order of nontrivial s_σ). *SpecialMatrices.s SpecialMatrices.order$_s e q_c$harTheorderofs_σ for any $\sigma \neq 0$ is char(F)*

Proof. SpecialMatrices.s$_p$ow$_e q_{sm}$ulLetpdenotethecharacteristicofthefield, $andlet\sigma \in F$, by 5.10 we know that for any $s_\sigma^p = s_{p\cdot\sigma}$. Since p is the characteristic of the field $p \cdot \sigma = 0$, we have that $s_{p\cdot\sigma} = s_0 = I$ □

Lemma 5.12. *SpecialMatrices.d, SpecialMatrices.s SpecialMatrices.d$_m$ul$_{sm}$ul$_{di}$nv$_e q_s$Wehavethatforall$\delta \in F^\times$ and $\sigma \in F$*

$$d_\delta s_\sigma d_\delta^{-1} = s_{\sigma\delta^{-2}}.$$

Proof. We verify by matrix multiplication that indeed:

$$d_\delta s_\sigma d_\delta^{-1} = \begin{bmatrix} \delta & 0 \\ 0 & \delta^{-1} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \sigma & 1 \end{bmatrix} \begin{bmatrix} \delta^{-1} & 0 \\ 0 & \delta \end{bmatrix} = \begin{bmatrix} \delta & 0 \\ 0 & \delta^{-1} \end{bmatrix} \begin{bmatrix} \delta^{-1} & 0 \\ \sigma\delta^{-1} & \delta \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \sigma\delta^{-2} & 1 \end{bmatrix} = s_{\sigma\delta^{-2}}.$$

□

Lemma 5.13. *SpecialMatrices.d, SpecialMatrices.w SpecialMatrices.w$_m$ul$_{de}q_{di}$nv$_w$Foranyδ ∈ $F^\times$ we have:*

$$wd_\delta w^{-1} = d_\delta^{-1}.$$

Proof. We verify by matrix multiplication that indeed

$$\begin{aligned} wd_\delta w^{-1} &= \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} \delta & 0 \\ 0 & \delta^{-1} \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -\delta \\ \delta^{-1} & 0 \end{bmatrix} \\ &= \begin{bmatrix} \delta^{-1} & 0 \\ 0 & \delta \end{bmatrix} = d_\delta^{-1}. \end{aligned}$$

□

We can now express familiar kinds of matrices of $\mathrm{SL}_2(F)$ in terms of these three matrices:

First we note a straightforward observation:

Corollary 5.14. *det$_e q_m$ul$_d$iag$_o f_l$ower$_t$riangularThedeterminantofa2 ×2 lower triangular matrix, M, is the product of the diagonal entries* $\det(M) = M_{11}M_{22}$.

Proof. We use the 2×2 determinant formula. □

Corollary 5.15. *$det_e q_m ul_d iag_o f_l ower_t riangular Special Linear Group.fin_t wo_d iagonal_i ff A2$ $\times 2$ matrix of* $\mathrm{SL}_2(F)$*, x is a diagonal matrix if and only if $x = d_\delta$ for some $\delta \in F^\times$.*

Proof. Since x is diagonal and belongs to the special linear group, the determinant is $x_{11}x_{22} = 1$ which shows $x_{11} = x_{22}^{-1}$, as required. □

Corollary 5.16. *SpecialMatrices.s, $det_e q_m ul_d iag_o f_l ower_t riangular Special Linear Group.fin_t wo_s hear_i ff Amatr$ x is a shear matrix, that is of the form* $\begin{bmatrix} \alpha & 0 \\ \sigma & \alpha \end{bmatrix}$ *if and only if either $x = s_\sigma$ or $x = -s_\sigma$ for some $\sigma \in F$.*

Proof. Again using the formula for the determinant of a 2×2 matrix to show that indeed if x is a shear matrix in the special linear group then $x_{11}^2 = x_{22}^2 = 1$ then $\alpha = \pm 1$, as required. □

Corollary 5.17. *SpecialLinearGroup.$fin_t wo_a ntidiagonal_i ff A matrix A \in \mathrm{SL}_2(F)$ is anti-diagonal, that is of the from* $\begin{bmatrix} 0 & \beta \\ \gamma & 0 \end{bmatrix}$ *if and only if $A = d_\delta w$*

Proof. This is shown by direct computation, we observe that w flips the rows and changes the sign of one the flipped rows to account for the determinant needing to be equal to one. □

From these relations we can now single out the following subgroups of $\mathrm{SL}_2(F)$.

Special subgroups of $\mathrm{SL}_2(F)$

Definition 5.18 (The subgroup of diagonal matrices). SpecialSubgroups.D The set of diagonal matrices with matrix multiplication is a subgroup of $\mathrm{SL}_2(F)$:

$$D = \{d_\delta \mid \delta \in F^\times\} = \left\{ \begin{bmatrix} \delta & 0 \\ 0 & \delta^{-1} \end{bmatrix} \mid \delta \in F^\times \right\}$$

Definition 5.19 (The subgroup of shear matrices). SpecialSubgroups.S The set of shear matrices with matrix multiplication is a subgroup of $\mathrm{SL}_2(F)$:

$$S = \{s_\sigma \mid \sigma \in F\} = \left\{ \begin{bmatrix} 1 & 0 \\ \sigma & 1 \end{bmatrix} \mid \sigma \in F \right\}$$

Definition 5.20 (The subgroup of lower triangular matrices). SpecialSubgroups.L The set of lower triangular matrices (see below) with matrix multiplication is a subgroup of $\mathrm{SL}_2(F)$

$$L = DS$$

where $DS = \{d_\delta s_\sigma \mid \delta \in F^\times \text{ and } \sigma \in F\}$ is the pointwise product of D and S.

Definition 5.21 (The subgroup of containing diagonal and antidigonal matrices). SpecialSubgroups.DW The set of all diagonal and anti-diagonal matrices with matrix multiplication is a subgroup of $\mathrm{SL}_2(F)$

$$DW = \langle D, w \rangle = \{d_\delta\} \cup \{d_\delta w\} \tag{5.1}$$

Remark 5.22. It is possible to have specify the subgroup DW in 5.21 as the subgroup closure of $D \sqcup \langle w \rangle$ but then it would require some additional work to show that the underlying set is indeed $D \cup Dw$.

Corollary 5.23. *SpecialMatrices.d, SpecialMatrices.s* $mem_{L}if\,f_{l}ower_{t}riangularThesubgroupL \leq \mathrm{SL}_2(F)$ *is the subgroup of* 2×2 *lower triangular matrices with determinant one,* $L = \left\{ \begin{bmatrix} \alpha & 0 \\ \gamma & \delta \end{bmatrix} \mid \alpha, \gamma, \delta \in F \text{ and } \alpha\delta = 1 \right\}$.

Proof. Observe that for every $l \in L$ there is some $\delta \in F^\times$ and $\sigma \in F$ such that $l = d_\delta s_\sigma = \begin{bmatrix} \delta & 0 \\ \sigma * \delta^{-1} & \delta^{-1} \end{bmatrix}$ which is lower triangular.

Furthermore, for every lower triangular matrix $L = \begin{bmatrix} \alpha & 0 \\ \gamma & \delta \end{bmatrix}$

Setting $\delta = \alpha \in F^\times$ as $\alpha\delta = 1$ and setting $\sigma = \gamma\alpha$ indeed yields the equality

$$d_\delta s_\sigma = \begin{bmatrix} \alpha & 0 \\ \gamma & \delta \end{bmatrix}$$

Thus $L = DS$ is the set of lower triangular matrices. □

Remark 5.24. To define the subgroups D, S and L in Lean.

One has to:

1. Specify what the underlying set is, what is called the `carrier`.
2. Prove that the set is closed under multiplication, that is, provide a proof term to the field `mul_mem'`.
3. Prove that the set contains the identity element of the group, that is, provide a proof term to the field `one_mem'`.
4. Show that the group is closed under the inversion operator $(-)^{-1}$, `inv_mem'`.

Once these four fields have been filled in, one has succesfully defined a subgroup in Lean.

Remark 5.25. Despite the definition of L as being DS, some work has to be shown that indeed $DS = D \sqcup S$.

If either D or S were normal in $\mathrm{SL}_2(F)$, this fact would be immediate as we would be able to use `mul_normal` or `normal_mul`:

However, given neither D or S are normal in $\mathrm{SL}_2(F)$ slightly more work is needed to show this.

It is interesting how Lean really forces either increased understanding or increased frustration.

These elements and subgroups are fundamental to this paper and this notation will be used throughout.

Definition 5.26 ($(D,\cdot) \cong (F^\times,\cdot)$). SpecialSubgroups.D, SpecialMatrices.d$_m ul_{de} q_{dm} ul Special Subgroups. D_i so_u n$ $F^\times \xrightarrow{\sim} D$ defined by $\delta \mapsto d_\delta$ defines a group isomorphism.

Proof. The function $\psi : F^\times \to D$ defined by $\psi(\delta) = d_\delta$ is a homomorphism between the group $F^\times$ under normal multiplication and D under normal matrix multiplication:

$$\psi(\delta\rho) = d_{\delta\rho} = d_\delta d_\rho = \psi(\delta)\psi(\rho). \qquad \text{(by Lemma ??)}$$

Observe that ψ is trivially injective and surjective and thus an isomorphism. So $D \cong F^\times$ and D is a subgroup of L.

□

Definition 5.27 ($(S,\cdot) \cong (F,+)$). SpecialSubgroups.S SpecialSubgroups.S$_i so_F Themap \phi$: $F \xrightarrow{\sim} S$ defined by $\sigma \mapsto s_\sigma$ defines a group isomorphism.

Proof. The function $\phi : F \to T$ defined by $\phi(\sigma) = s_\sigma$ is a homomorphism between the group F under addition and S under normal matrix multiplication:

$$\phi(\sigma+\gamma) = s_{\sigma+\gamma} = s_\sigma s_\gamma = \phi(\sigma)\phi(\gamma). \qquad \text{(by Lemma ??)}$$

It is clear that ϕ is injective and surjective and thus an isomorphism. So $S \cong F$ and S is a subgroup of L.

□

Lemma 5.28. *SpecialSubgroups.normal$_S$ubgroupOf$_L$Sisanormalsubgroupof$L$*

Proof. Let s_γ and $d_\delta s_\sigma$ be arbitrary elements of T and H respectively. Conjugating s_γ by $d_\delta s_\sigma$ gives,

$$\begin{aligned}
(d_\delta s_\sigma) s_\gamma (d_\delta s_\sigma)^{-1} &= (d_\delta s_\sigma) s_\gamma (t_\sigma^{-1} d_\delta^{-1}) \\
&= d_\delta (s_\sigma s_\gamma t_{-\sigma}) d_\delta^{-1} && \text{(since } t_\sigma^{-1} = t_{-\sigma}\text{)} \\
&= d_\delta s_\gamma d_\delta^{-1} && \text{(by Lemma ??)} \\
&= s_{\gamma\delta^{-2}} \in S. && \text{(by Lemma ??)}
\end{aligned}$$

Since s_γ was chosen arbitrarily from $\mathrm{SL}_2(F)$we have $(d_\delta s_\sigma) S (d_\delta s_\sigma)^{-1} = S$ and since $d_\delta s_\sigma$ was chosen arbitrarily from L, we have that $S \lhd L$.

□

Remark 5.29 (Subgroups of subgroups in Lean). In Lean, for this particular scenario, S is considered to be a subgroup of $\mathrm{SL}_2(F)$.

It is fairly easy to see that $S \not\lhd \mathrm{SL}_2(F)$. When we say that $S \lhd L$, we are implicitly restricting S to be a subset of L and thus we are actually thinking

about the subgroup $S \cap L$, but in fact this does not change anything because $S = S \sqcap L$ as $S \leq \mathrm{SL}_2(F)$.

Informally we do not think twice about this, but when formalizing this we do need to be clear which is the ambient group for S to be normal and in this case it should be a subgroup of L, rather than $\mathrm{SL}_2(F)$.

So this is why the informal statement corresponds to the formal statement:

```
Normal (S F).subgroupOf (L F)
```

This example highligths how as useful as it is that Lean keeps track of what the ambient groups are, it is often the case that we look at the same object under a different lense such as in this case, where we restrict it to be a subgroup of another group that contains it. It turns out that there is learning curve to becoming comfortable with these transitions.

On the positive side, the automation leans offers, that is, the tactics and the unification algorithm (the algorithm which allows you to subsitute equal terms when say you use the `rw` tactic) is continually being refined, and it is increasingly able to do a lot of coercions on its own.

Lemma 5.30. *SpecialSubgroups.D, SpecialSubgroups.S SpecialSubgroups.*$D_j oin_{Sq} uot_{Ss} ubgroupOf_{D} j oin_{Sm} ulEqu$
$/ S \cong D$.

Proof. SpecialSubgroups.normal$_{Ss} ubgroupOf_{L} The function \pi : L \to D$ defined by $\pi(d_\delta s_\sigma) = d_\delta$ is a homomorphism between L under normal matrix multiplication and D under normal matrix multiplication:

$$\begin{aligned} \pi(d_\delta s_\sigma d_\rho s_\gamma) &= \pi(d_\delta d_\rho s_\sigma s_\gamma) && \text{(where } \sigma = \sigma\rho^2 \text{ by Lemma } \mathbf{??}\text{)} \\ &= d_\delta d_\rho \\ &= \pi(d_\delta s_\sigma)\pi(d_\rho s_\gamma). \end{aligned}$$

We see that π is trivially surjective and has kernel

$$\ker(\pi) = \{d_\delta s_\sigma \in L : \pi(d_\delta s_\sigma) = I_{\mathrm{SL}_2(F)}\} = S.$$

Thus by the First Isomorphism Theorem,

$$\begin{aligned} L/\ker(\pi) &\cong \mathrm{Im}(\pi), \\ L/ &\cong D. \end{aligned}$$

□

Remark 5.31. Interestingly, this proof was quite hard to formalise for reasons I will expand on below, but first let me introduce some ideas.

There are two complete lattice structures at play here: one where the top element is $\top = \mathrm{SL}_2(F)$ and another lattice which is the corresponding sublattice where $\top = D \sqcup S$. The second sublattice is crucial because we need S to be normal in an ambient group, and clearly $S \not\lhd \mathrm{SL}_2(F)$; therefore when restricting

S to begin a subgroup of $D \sqcup S = L$. Given S is a subgroup of $D \sqcup S = L$ as $S \leq S \sqcup D = L$, considered as a subgroup of $D \sqcup S = L$ we as shown in 5.28 it is normal S a subgroup of L.

This eventually entails to using the theorem called `QuotientGroup.quotientInfEquivProdNormalQuotient` which corresponds to the statment

```
H  N.subgroupOf H * (H  N)  N.subgroupOf (H  N)
```

Which is in fact the second isomorphism theorem, not the first isomorphism theorem! Which contrasts to how the statement was proved informally.

where in for this particular theorem, `H` is specialized to:

```
H := (D F).subgroupOf (D F  S F)
```

and `N` is specialized to:

```
N := (S F).subgroupOf (D F  S F)
```

recall that within Lean, `F` denotes the base field for $\mathrm{SL}_2(F)$, D and S.

Written informally, it corresponds to

$$D \cong \frac{D}{\bot} = \frac{D}{S \sqcap D} \cong \frac{D \sqcup S}{S} = \frac{L}{S}$$

5.3 The Center of $\mathrm{SL}_2(F)$

Definition 5.32. The **centre** $Z(G)$ of a group G is the set of elements of G that commute with every element of G.

$$Z(G) = \{z \in G : \forall g \in G, \ \ gz = zg\}.$$

It is an immediate observation that $Z(G)$ is a normal subgroup of G, since for each $z \in Z$, $gzg^{-1} = gg^{-1}z = z$, $\forall g \in G$. It's also clear that a group is abelian if and only if $Z(G) = G$.

Definition 5.33. SpecialSubgroups.Z Let R be a commutative ring and define Z to be the subgroup generated by $-I \in \mathrm{SL}_2(R)$

Remark 5.34. Observer that the subgroup generated by an element $g \in G$, $\langle g \rangle$, can be thought of more generally within any lattice as the closure of a singleton set g. Therefore, the subgroup generated by $-I$ is equal to

$$\langle -I \rangle = \overline{\{-1\}} = \inf\{K \leq G \mid \{-1\} \subseteq K\}.$$

When taking the closure of a singleton, when the ambient lattice is the subgroup lattice; and the closure corresponds to taking the powers of the element in the singleton $\{g\}$, which is what is typically understood as the subgroup generated by g.

The way Z is defined in Lean is thus:

```
def Z (R : Type*) [CommRing R] : Subgroup SL(2,R) :=
    closure {(-1 : SL(2,R))}
```

Corollary 5.35. *SpecialSubgroups.closure*$_n$*eg*$_o$*ne*$_e$*qThesubgroupclosureofthesingleton{-I}, orequivalently, thesubgroupgeneratedby-Iequals*$\overline{\{-I\}} = \{I, -I\}$

Proof. Since $-1^2 = 1$, we have that $-I^2 = I$ and thus the result follows. □

Lemma 5.36. *SpecialSubgroups.ZSpecialSubgroups.center*$_S$*L2*$_e$*q*$_Z$*Z(*$\mathrm{SL}_2(F)) = \langle -I_{\mathrm{SL}_2(F)} \rangle = Z$.

Proof. Take an arbitrary element $x = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \mathrm{SL}_2(F)$and an arbitrary element $z = \begin{bmatrix} z_1 & z_2 \\ z_3 & z_4 \end{bmatrix} \in Z$ and consider their product:

$$zx = \begin{bmatrix} z_1 & z_2 \\ z_3 & z_4 \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} z_1 & z_2 \\ z_3 & z_4 \end{bmatrix} = xz,$$

$$\begin{bmatrix} z_1\alpha + z_2\gamma & z_1\beta + z_2\delta \\ z_3\alpha + z_4\gamma & z_3\beta + z_4\delta \end{bmatrix} = \begin{bmatrix} z_1\alpha + z_3\beta & z_2\alpha + z_4\beta \\ z_1\gamma + z_3\delta & z_2\gamma + z_4\delta \end{bmatrix}. \tag{5.2}$$

Equating either the top left or bottom right entries, we see that $z_2\gamma = z_3\beta$. Since β and γ can take any values in F, for equality to always hold we must have $z_2 = 0 = z_3$. Hence equation (5.2) simplifies to

$$\begin{bmatrix} z_1\alpha & z_1\beta \\ z_4\gamma & z_4\delta \end{bmatrix} = \begin{bmatrix} z_1\alpha & z_4\beta \\ z_1\gamma & z_4\delta \end{bmatrix}.$$

Thus

$$z_1 = z_4 \qquad \text{and} \qquad z = \begin{bmatrix} z_1 & 0 \\ 0 & z_1 \end{bmatrix}.$$

Since we are working in the special linear group, $\det(z) = 1$, thus $z_1 = \pm 1$ and $Z = \langle -I_{\mathrm{SL}_2(F)} \rangle$ as required. Observe that this is a cyclic group of order 2 except in the case of $p = 2$ where $-I_{\mathrm{SL}_2(F)} = I_{\mathrm{SL}_2(F)}$.

□

Following this result, for ease of notation, $Z(\mathrm{SL}_2(F))$ will be denoted simply by Z throughout the rest of this paper.

Lemma 5.37. *SpecialSubgroups.exists*$_u$*nique*$_o$*rderOf*$_e$*q*$_t$*woIfp*$\neq$ *2, then* $\mathrm{SL}_2(F)$ *contains a unique element of order 2.*

Proof. Consider an arbitrary element $x \in \mathrm{SL}_2(F)$with order 2. That is $x^2 = I_{\mathrm{SL}_2(F)}$, $x \neq I_{\mathrm{SL}_2(F)}$and thus $x = x^{-1}$.

$$x = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}^{-1} = \begin{bmatrix} \delta & -\beta \\ -\gamma & \alpha \end{bmatrix}.$$

Thus $\alpha = \delta$, $\beta = -\beta \Rightarrow 2\beta = 0$ and $\gamma = -\gamma \Rightarrow 2\gamma = 0$. In the case of $p \neq 2$ this gives $\beta = 0 = \gamma$. So

$$x = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}.$$

Also $\alpha^2 = 1$ since $x \in \mathrm{SL}_2(F)$, so $\alpha = \pm 1$. For x to have order 2, we must have $\alpha = -1$. Hence there is a unique element of order 2, namely $-I_{\mathrm{SL}_2(F)}$.

□

Lemma 5.38. *SpecialSubgroups.card*$_{Z}$*eq*$_{t}$*wo*$_{o}$*f*$_{t}$*wo*$_{n}$*e*$_{z}$*eroIfthecharacteristicchar(F)* $\neq 2$ *then* $|Z| = 2$.

Proof. If $\mathrm{char}(F) \neq 2$ then $1 \neq -1$ as $2 \neq 0$ therefore, $I \neq -I$ which shows that $Z = \{I, -I\}$ contains two distinct elements. □

Lemma 5.39. *SpecialSubgroups.card*$_{Z}$*eq*$_{o}$*ne*$_{o}$*f*$_{t}$*wo*$_{e}$*q*$_{z}$*eroIfthecharacteristicchar(F)* = 2*then*$|Z| = 1$.

Proof. If $\mathrm{char}(F) = 2$ then $1 = -1$ as $2 = 0$ therefore, $I = -I$ which shows that $Z = \{I, -I\} = \{I\}$ only contains one element. □

Lemma 5.40 (Z is cyclic). *SpecialSubgroups.IsCyclic*$_{Z}$

Proof. By construction, $Z = \overline{\{-I\}} = \{-I^k \mid k \in \mathbb{Z}\} = \langle -I \rangle$, therefore Z is generated by a single element and is thus cyclic. □

In the next chapter it will be useful to record the interactions between S and Z for instance

Definition 5.41. SpecialSubgroups.S, SpecialSubgroups.Z, SpecialMatrices.s$_{m}$*ul*$_{se}$*q*$_{sa}$*ddSpecialSubgroups.SZW* $\cup -S$, or equivalently the pointwise product SZ.

Corollary 5.42. *SpecialSubgroups.SZ SpecialSubgroups.S*$_{m}$*ul*$_{Z}$ *s*$_{u}$*bset*$_{S}$*ZSZ* $= S \cup -S$

Proof. by construction an element of SZ is either of the form $s_\sigma I = s_\sigma \in S$ or $s_\sigma - I = -s_\sigma \in -S$. The reverse subset inclusion is very similar. □

Lemma 5.43. *SpecialSubgroups.Z, SpecialSubgroups.S, SpecialSubgroups.SZ SpecialSubgroups.S*$_{j}$*oin*$_{Z}$*e*$_{q}$*S*$_{Z}$*Thejo* $\sqcup Z = SZ$

Proof. SpecialSubgroups.closure$_{n}$*eg*$_{o}$*ne*$_{e}$*q*, *SpecialSubgroups.S*$_{m}$*ul*$_{Z}$ *s*$_{u}$*bset*$_{S}$*ZWeshowthat*S $\sqcup Z = SZ$ by antisymetry, that is, we show both that

- $S \sqcup Z \subseteq SZ$

  Let $x \in S \sqcup Z$, then if x is in the subgroup closure then if K is a subgroup whose underlying set contains SZ then x is in K, but since SZ was shown to be a subgroup in 5.41 we can conclude that $x \in SZ$ and thus $x = s_\sigma z$ for some σinF.

- $SZ \subseteq S \sqcup Z$

  Let $s_\sigma z \in SZ$ then we must show that $s_\sigma z$ is the subgroup closure of S and Z but since the subgroup closure must at least contain the pointwise product whose underlying set is equal to the union $S \cup -S$, we are done.

□

5.4 Conjugacy of the Elements of $\mathrm{SL}_2(F)$

Classification of elements of $\mathrm{SL}_2(F)$ up to conjugation

Lemma 5.44 (Upper triangularizability criteria). *$isConj_upper_triagnular_iff A matrix M \in Mat_2(F)$ is triangularizable if and only if there exists an invertible matrix $C \in \mathrm{GL}_2(F)$ such that the bottom left entry $CMC_{21}^{-1} = 0$.*

Proof. Given a matrix U is in upper triangular form if and only if

$$U = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$$

that is, the bottom left entry is zero. It then follows that

M is triangularizable if and only there exists a $C \in \mathrm{GL}_2(F)$ such that is in upper triangular form CMC^{-1}, that is, the bottom left entry of CMC^{-1} is zero. □

Lemma 5.45 (Upper triangularizability of a 2×2 matrix over an algebraically closed field). *$isTriangularizable_of_algClosedWhenFisanalgebraicallyclosedfield, foranyM \in Mat_2(F)$ there exists an invertible matrix $C \in \mathrm{SL}_2(F) \leq \mathrm{GL}_2(F)$ such that $CMC^{-1} = U$ where*

$$U = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$$

for some $a, b, d \in F$.

Proof. $\mathrm{isConj}_upper_triangular_iff We prove this by direct computation.$

Let

$$M = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \mathrm{Mat}_2(F)$$

By lemma 5.44, we only need to show that we can find a matrix $C \in \mathrm{SL}_2(F)$ such that when it acts on M by conjugation, the bottom left entry is annihilated.

- Suppose on the one hand that $\beta \neq 0$

  Observe that

$$s_\sigma M s_\sigma^{-1} = \left(\begin{bmatrix} -\beta\sigma + \alpha & \beta \\ -\beta\sigma^2 + \alpha\sigma - \delta\sigma + \gamma & \beta\sigma + \delta \end{bmatrix} \right) \tag{5.3}$$

Given F is algebraically closed we can set $\sigma \in F$ to be a root of the polynomial

$$P(X) := -\beta X^2 + \alpha X - \delta X + \gamma$$

setting $C := s_\sigma$ yields the desired element which triangularizes M.

- Suppose on the other hand that $\beta = 0$

  Given the top right entry is zero we only need find a matrix in $\mathrm{SL}_2(F)$ which flips the antidiagonal entries (modulo modifying the signs) it is thus sufficient to use

  $$w = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{as indeed} \quad wMw^{-1} = \begin{bmatrix} \delta & -\gamma \\ 0 & \alpha \end{bmatrix} \text{ is in triangular form}$$

□

Corollary 5.46 (Upper triangular matrices are conjugate to lower triangular matrices). *SpecialMatrices.w lower$_t$riangular$_i$sConj$_u$pper$_t$riangularForevery $U \in Mat_2(F)$ that is upper triangular the matrix wUw^{-1} is a lower triangular matrix*

Proof. Direct computation shows this result, see the Lean code! □

Lemma 5.47. *upper$_t$riangular$_i$sConj$_d$iagonal$_o$f$_n$onzero$_d$etAnuppertriangularmatrix $U = \begin{bmatrix} \alpha & \beta \\ 0 & \delta \end{bmatrix}$ isconjugatetoadiagonalmatrixif $\alpha - \delta \neq 0$*

Proof. We show this by direct computation.
Conjugation of M by the matrix

$$C := \begin{bmatrix} 1 & \frac{\beta}{\alpha - \delta} \\ 0 & 1 \end{bmatrix}$$

yields a diagonal matrix (see the Lean code for the computation!). □

Proposition 5.48. *SpecialMatrices.s, SpecialMatrices.d SL2$_I$sConj$_{do}$r$_I$sConj$_{so}$r$_I$sConj$_n$eg$_{so}$f$_A$lgClosedEachel is conjugate to either d_δ for some $\delta \in F^\times$, or to $\pm s_\sigma$ for some $\sigma \in F$.*

Proof. isTriangularizable$_o$f$_a$lgClosed, lower$_t$riangular$_i$sConj$_u$pper$_t$riangular, upper$_t$riangular$_i$sConj$_d$iagona $\in \mathrm{SL}_2(F)$can be regarded as a linear transformation in the 2 dimensional vector space over F, with the eigenvalues π_1 and π_2.

If π_1 and π_2 are distinct, then x is thus diagonalisable. That is, there exists an invertible matrix $a \in GL(2, F)$ such that $y = axa^{-1}$ is a diagonal matrix. Furthermore, we can multiply a by a suitable scalar to find an element in $\mathrm{SL}_2(F)$which conjugates x and y:

$$\text{Set } b = \frac{a}{\sqrt{\det(a)}}, \quad \text{thus } \; bxb^{-1} = \frac{a}{\sqrt{\det(a)}}\, x\, (\sqrt{\det(a)}\,)\, a^{-1} = axa^{-1} = y.$$

Observe that $\det(b) = 1$, hence x and y are conjugate in L. Furthermore, since y is a diagonal matrix it must belong to the set D, showing that x is conjugate to d_δ for some $\delta \in F^\times$.

If $\pi_1 = \pi_2$ then x has just one repeated eigenvalue. Suppose that x is diagonalisable. Then there exists an element $c \in GL(2, F)$ and a diagonal matrix $\pi_1 I_G$ such that $x = c(\pi_1 I_G)c^{-1} = \pi_1 I_G$. Thus $x = \pm I_G$, which trivially belongs to both D and $\times Z$.

Now assume that x is not diagonalisable. Chapter 7 of [**?**] shows that there exists an element $d \in GL(2, F)$, such that $x = djd^{-1}$, where,

$$j = \begin{bmatrix} \pi_1 & 1 \\ 0 & \pi_1 \end{bmatrix}$$

is the Jordan Normal Form of x. By the method described above, we can multiply d by a suitable scalar to show that x is conjugate to j in L. Now we conjugate j by an element of $\mathrm{SL}_2(F)$whose top left entry is 0.

$$\begin{bmatrix} 0 & -\gamma^{-1} \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} \pi_1 & 1 \\ 0 & \pi_1 \end{bmatrix} \begin{bmatrix} \delta & \gamma^{-1} \\ -\gamma & 0 \end{bmatrix} = \begin{bmatrix} 0 & -\gamma^{-1} \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} \pi_1\delta - \gamma & \pi_1\gamma^{-1} \\ -\pi_1\gamma & 0 \end{bmatrix} = \begin{bmatrix} \pi_1 & 0 \\ -\gamma^2 & \pi_1 \end{bmatrix}$$

Now clearly the determinant of x is equal to the determinant of j, namely 1, which means that $\pi_1 = \pm 1$. This shows that j is conjugate in $\mathrm{SL}_2(F)$to some element in $\times Z$ as well as x. Furthermore, since conjugation is transitive, x is conjugate to $\pm s_\sigma$ for some $\sigma \in F$.

□

Remark 5.49. Formalizing the classification of elements of $\mathrm{SL}_2(F)$ up to conjugation in Lean was surprisingly difficult.

Given the (informal) proof presented of propostion 5.48 extracted from Christopher Butler's exposition uses the Jordan Normal Form theorem.

Furthermore, since at the time of writing, the Jordan Normal form theorem is still not yet in Mathlib this theorem turned out to be quite difficult to formalise.

The original approach to formalise the Jordan Normal Form theorem for 2×2 matrices involved studying the eigenspace and generalized eigenspaces of the endomorphism associated to a 2×2 matrix. This is one the standard approached taught in an undergraduate curriculum, yet surprisingly, to formalise the 2×2 case with this approach untractable.

The reason this approach and often standard techniques might not integrate well with `mathlib` often ocurrs for the following reasons I will now outline.

The crux of formalising a mathematical result always lies at finding the right abstraction, as illustrated in 5.29, understanding the lattice structure on the set of subgroups becomes an indispensable tool for formalising results regarding subgroups and their properties. In this particular case, the right abstraction is not entirely clear.

Is it best to prove the theorem for matrices or for endomoprhisms? Which will be the easiest approach? Which approach is most general? Which approach yields the most amount of useful lemmas?

The reason why the Jordan Normal Form theorem is not yet in Mathlib is because it hinges on the following two results which have not been formalised yet:

1. The classification of nilpotent endomorphisms.
2. The classification of semisimple endomorphisms.

Such formalisation would be an amazing project to undertake. Bear in mind, the theorem formalized is the more general Jordan-Chevallier theorem.

To the authors understanding, the general theorem will be formalised by studying the eigenspace and general eigenspace. This approach turned out to be essentially equivalent in difficuly to formalising the special case of 2×2 matrices over an algebraically closed field with the same approach, since the argument is inductive in some sense.

Therefore, after discussions with Prof. Kevin Buzzard's it turned out to be much more effective to classify matrices of the special linear group up to conjugation by splitting on a few different cases of what a 2×2 matrix might look like and finding the suitable matrices bywhich to conjugate to put them in either the form of d_δ or $\pm s_\sigma$.

5.5 Centralizers & Normalizers

Both the centraliser and normalizer of a subset H are subgroups of G. Note also that the centraliser is a stronger condition than the normalizer and any element in the centraliser of H is also in its normalizer. If H is a singleton then it's clear that its centraliser and normalizer are equal.

Normalizers

Definition 5.50. The **normalizer** $N_G(H)$ of a subset H of a group G is the set of elements of G which stabilise H under conjugation.

$$N_G(H) = \{g \in G : gHg^{-1} = H\}.$$

Corollary 5.51. $lower_triangular_iff_top_right_entry_eq_zero A matrix M \in Mat(2; F)$ *is lower triangular if and only if the* $M_{12} = 0$.

Proof. It is easy to see the top right entry must be zero for a matrix to be lower triangular. □

Proposition 5.52 (Normalizer of subgroups of S are contained in L). *SpecialSubgroups.S, SpecialSubgroups.L* $normalizer_subgroup_Sl e_L For any subgroup S_0 \leq S$ *with order greater than 1, we have that the normalizer* $N_{\mathrm{SL}_2(F)}(S_0) \subset L$.

Proof. $\mathrm{mem}_{Lif}f_{lower_triangular, lower_triangular_if}f_{top_right_entry_eq_zeroLets_\sigma}$ be an arbitary element of S_0 with $\sigma \neq 0$. To determine the normalizer of S_0 in $\mathrm{SL}_2(F)$we consider which $x \in \mathrm{SL}_2(F)$ satisfy $xs_\sigma x^{-1} \in S_0$.

$$\begin{aligned} xs_\sigma x^{-1} &= \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \sigma & 1 \end{bmatrix} \begin{bmatrix} \delta & -\beta \\ -\gamma & \alpha \end{bmatrix} \\ &= \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} \delta & -\beta \\ \delta\sigma - \gamma & \alpha - \beta\sigma \end{bmatrix} \\ &= \begin{bmatrix} \alpha\delta - \beta\gamma + \beta\delta\sigma & -\beta^2\sigma \\ \delta^2\sigma & \alpha\delta - \beta\gamma - \beta\delta\sigma \end{bmatrix}. \end{aligned}$$

Since $xs_\sigma x^{-1} \in S_0$ we have $-\beta^2\sigma = 0$ and since $\sigma \neq 0$, we have $\beta = 0$. Since s_σ was chosen arbitrarily, any element which normalises S_0 is a lower diagonal matrix and is therefore in H by (**??**). Thus $N_{\mathrm{SL}_2(F)}(S_0) \subset H$ as required.

□

Lemma 5.53. *$ex_of_card_{Dg}t_twoIfthecardinalityoffinitesubgroupof D_0 \leq D$ is greater than* 2 *then there exists an element $x \in D_0$ which does not belong to the center Z, that is, $x \neq d_1 = I$ and $x \neq d_{-1} = -I$.*

Proof. Suppose for a contradiction that if $\delta \neq \pm 1$ then $d_\delta \notin D_0$. We show that $D_0 \leq Z$ and therefore, $|D_0| \leq 2$ our contradiction.

Let $d_\delta \in D_0 \leq D$ then given $d_\delta \notin D_0$ if $\delta \neq \pm 1$ and $Z = \langle -I \rangle = \{I, -I\}$. It immediately follows that $D_0 \leq Z$.

□

Proposition 5.54 (Normalizers of subgroups of D are contained in L). *Special-Subgroups.D, SpecialSubgroups.DW $normalizer_subgroup_{De}q_D W N_{\mathrm{SL}_2(F)}(D_0) = \langle D, w \rangle$, where D_0 is any subgroup of D with order greater than 2.*

Proof. SpecialLinearGroup.$\mathrm{fin}_t wo_diagonal_i ff, SpecialLinearGroup.fin_t wo_antidiagonal_i ff, ex_of_card_{Dg}t_twoS$ 3, we can choose a $d_\delta \in D_0 \backslash Z$, that is where $\delta \neq 1$. To determine the normalizer of D_0 in $\mathrm{SL}_2(F)$we consider which $x \in \mathrm{SL}_2(F)$satisfy $xd_\delta x^{-1} \in D_0$.

$$\begin{aligned} xd_\delta x^{-1} &= \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} \delta & 0 \\ 0 & \delta^{-1} \end{bmatrix} \begin{bmatrix} \delta & -\beta \\ -\gamma & \alpha \end{bmatrix} \\ &= \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} \delta\delta & -\beta\delta \\ -\gamma\delta^{-1} & \alpha\delta^{-1} \end{bmatrix} \\ &= \begin{bmatrix} \alpha\delta\delta - \beta\gamma\delta^{-1} & \alpha\beta(\delta^{-1} - \delta) \\ \gamma\delta(\delta - \delta^{-1}) & \alpha\delta\delta^{-1} - \beta\gamma\delta \end{bmatrix} \in D_0. \end{aligned} \tag{5.4}$$

Since (5.4) is in D_0, the top right and bottom left entries must be 0. Since $\delta \neq \pm 1$, we have $\delta \neq \delta^{-1}$ and so $\alpha\beta = 0 = \gamma\delta$.

If $\alpha = 0$, then β and γ are non-zero since $\det(x) = 1$, thus $\delta = 0$. So $\det(x) = -\gamma\beta = 1$ and $-\gamma = \beta^{-1}$. (5.4) becomes

$$\begin{bmatrix} \delta^{-1} & 0 \\ 0 & \delta \end{bmatrix} = d_\delta^{-1}.$$

Since D_0 is a group, it contains the inverse of each of it's elements, so $d_\delta^{-1} \in D_0$ as required. In this case we have $x \in wD$.

If $\alpha \neq 0$, then similarly $\beta = 0$, $\delta = \alpha^{-1}$ and $\gamma = 0$. (5.4) now becomes

$$\begin{bmatrix} \delta & 0 \\ 0 & \delta^{-1} \end{bmatrix} = d_\delta \in D_0.$$

This time we have $x \in D$. So $x \in D \cup wD = \langle D, w\rangle$ and any element which normalises D_0 is in $\langle D, w\rangle$, thus $N_{\mathrm{SL}_2(F)}(D_0) \subset \langle D, w\rangle$.

Now take an arbitrary $y \in \langle D, w\rangle = D \cup wD$. If $y \in D$ then $y = d_{\rho 1}$, for some $\rho 1 \in F^\times$.

$$d_{\rho 1} d_\delta d_{\rho 1}^{-1} = d_\delta \in D_0. \qquad \text{(by Lemma ??)}$$

If $y \in wD$ then $y = wd_{\rho 2}$, for some $d_{\rho 2} \in F^\times$.

$$\begin{aligned} (wd_{\rho 2}) d_\delta (wd_{\rho 2})^{-1} &= wd_{\rho 2} d_\delta d_{\rho 2}^{-1} w^{-1} \\ &= wd_\delta w^{-1} \\ &= d_\delta^{-1} \in D_0. \qquad \text{(by Lemma ??)} \end{aligned}$$

Thus y indeed who whole of $\langle D, w\rangle$ is contained in $N_{\mathrm{SL}_2(F)}(D_0)$. This inclusion gives the desired result, $N_{\mathrm{SL}_2(F)}(D_0) = \langle D, w\rangle$.

□

Centralisers

Definition 5.55 (Centralizer). The **centraliser** $C_G(H)$ of a subset H of a group G is the set of elements of G which commute with each element of H.

$$C_G(H) = \{g \in G : gh = hg, \quad \forall h \in L\}.$$

Corollary 5.56. *centralizer$_n$eg$_e$q$_c$entralizerLet$x \in \mathrm{SL}_2(F)$ then the centralizer of the negative equals $C_{SL_2(F)}(x) = C_{SL_2(F)}(-x)$.*

Proof. An element $y \in \mathrm{SL}_2(F)$ belongs to $C_{SL_2(F)}$ if and only if $1 = xyx^{-1}y^{-1} = (-x)y(-x^{-1})y^{-1}$ if and only if y belongs to $C_{\mathrm{SL}_2(F)}(-x)$. □

Proposition 5.57 (Centralizer of noncenter s_σ). *SpecialSubgroups.S, SpecialSubgroups.Z, SpecialMatrices.s centralizer$_{se}$q$_S$ZThecentralizer$C_{\mathrm{SL}_2(F)}(\pm s_\sigma) = S \times Z$ where $\sigma \neq 0$.*

Proof. SpecialLinearGroup.fin$_t$wo$_s$hear$_i$ff, *centralizer*$_n$eg$_e$q$_c$entralizerTodeterminethecentraliserofs$_\sigma$ in L, we consider which $y \in \mathrm{SL}_2(F)$satisfy $ys_\sigma = s_\sigma y$ for an arbitrarily chosen s_σ, with $\sigma \neq 0$.

$$
\begin{aligned}
ys_\sigma &= s_\sigma y, \\
\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \sigma & 1 \end{bmatrix} &= \begin{bmatrix} 1 & 0 \\ \sigma & 1 \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}, \\
\begin{bmatrix} \alpha + \beta\sigma & \beta \\ \gamma + \delta\sigma & \delta \end{bmatrix} &= \begin{bmatrix} \alpha & \beta \\ \gamma + \alpha\sigma & \delta + \beta\sigma \end{bmatrix}. \qquad (5.5)
\end{aligned}
$$

Equating the top left entries of (5.5) gives $\alpha + \beta\sigma = \alpha$ which means $\beta = 0$ since $\sigma \neq 0$ by assumption. Equating the bottom left entries gives that $\alpha = \delta$. Finally, since $\det(y) = 1$, we have $\alpha\delta = 1$ so $\alpha = \pm 1$. Thus a $y \in C_{\mathrm{SL}_2(F)}(s_\sigma)$ is

$$
y = \begin{bmatrix} \alpha & 0 \\ \gamma & \alpha \end{bmatrix}. \qquad \text{(where } \alpha = \pm 1\text{)}
$$

So $y = \pm s_\sigma$ for some $\sigma \in F$, and $SZ = \{\pm s_\sigma\} \subset C_{\mathrm{SL}_2(F)}(s_\sigma)$. Now take an arbitrary $s_\gamma z \in SZ$.

$$
\begin{aligned}
(s_\gamma z)s_\sigma &= s_\sigma(s_\gamma z), \\
s_\gamma s_\sigma z &= s_\sigma s_\gamma z, \qquad && \text{(since } z \in Z\text{)} \\
t_{\gamma+\sigma} &= t_{\gamma+\sigma}.
\end{aligned}
$$

Thus $s_\gamma z$ and indeed the whole of SZ is contained in $C_{\mathrm{SL}_2(F)}(s_\sigma)$, so $C_{\mathrm{SL}_2(F)}(s_\sigma) = SZ$.

Since S commutes elementwise with Z and $\cap Z = \{I_G\}$, we can apply Corollary 3.27 and assert that $C_{\mathrm{SL}_2(F)}(s_\sigma) = SZ \cong S \times Z$ as required. The centraliser of $-s_\sigma$ is also $\times Z$, since an element x commutes with $-s_\sigma$ if and only if it commutes with s_σ:

$$
xs_\sigma = s_\sigma x \iff -(xs_\sigma) = -(s_\sigma x) \iff x(-s_\sigma) = (-s_\sigma)x.
$$

Note that in case of $\sigma = 0$, $\pm s_\sigma \in Z$ and thus it's centraliser is the whole of L.

□

Proposition 5.58 (Centralizer of noncenter d_δ). *SpecialMatrices.d, SpecialSubgroups.D centralizer*$_{de}$q$_D$*Thecentralizer* $C_{\mathrm{SL}_2(F)}(d_\delta) = D$ *for* $\delta \neq \pm 1$.

Proof. SpecialLinearGroup.fin$_t$wo$_d$iagonal$_i$ff$Nowweconsiderwhich$y $\in \mathrm{SL}_2(F)$satisfy $yd_\delta = d_\delta y$ for an arbitrarily chosen d_δ, with $\delta \neq \pm 1$.

$$yd_\delta = d_\sigma y,$$

$$\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix}\begin{bmatrix}\delta & 0\\ 0 & \delta^{-1}\end{bmatrix} = \begin{bmatrix}\delta & 0\\ 0 & \delta^{-1}\end{bmatrix}\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix},$$

$$\begin{bmatrix}\alpha\delta & \beta\delta^{-1}\\ \gamma\delta & \delta\delta^{-1}\end{bmatrix} = \begin{bmatrix}\alpha\delta & \beta\delta\\ \gamma\delta^{-1} & \delta\delta^{-1}\end{bmatrix}. \tag{5.6}$$

Equating the top right and bottom left entries of (5.6) gives that $\beta = 0 = \gamma$ since Since $\delta \neq \delta^{-1}$. Thus $\delta = \alpha^{-1}$ and

$$x = \begin{bmatrix}\alpha & 0\\ 0 & \alpha^{-1}\end{bmatrix} \in D.$$

Thus x and indeed the whole of $C_{\mathrm{SL}_2(F)}(d_\delta)$ is contained in D. Now take an arbitrary $d_\rho \in D$.

$$d_\rho d_\delta = d_{\rho\delta} = d_\delta d_\rho.$$

So clearly $D \subset C_{\mathrm{SL}_2(F)}(d_\delta)$ and thus $C_{\mathrm{SL}_2(F)}(d_\delta) = D$ as required. □

Proposition 5.59 (Centralizers of conjugate elements). *conjugate$_c$entralizers$_o$f$_I$sConjLetaandbbeconjugateeler*
G such that $xC_G(a)x^{-1} = C_G(b)$.

Proof. This proposition essentially claims that conjugate elements have conjugate centralisers. Since a and b are conjugate there exists an $x \in G$ such that $b = xax^{-1}$. Let g be an arbitrary element of $C_G(a)$. Then,

$$\begin{aligned}(xgx^{-1})(xax^{-1}) &= xgax^{-1}\\ &= xagx^{-1} && \text{(since } g \in C_G(a)\text{)}\\ &= (xax^{-1})(xgx^{-1}).\end{aligned}$$

Thus $xgx^{-1} \in C_G(xax^{-1})$. Since g was chosen arbitrarily,

$$xC_G(a)x^{-1} \subset C_G(xax^{-1}) = C_G(b).$$

Conversely, let h be an arbitary element of $C_G(xax^{-1})$. Then,

$$\begin{aligned}(x^{-1}hx)a &= x^{-1}h(xax^{-1})x\\ &= x^{-1}(xax^{-1})hx && \text{(since } h \in C_G(xax^{-1})\text{)}\\ &= a(x^{-1}hx).\end{aligned}$$

So $x^{-1}hx \in C_G(a)$ and since h was arbitrarily chosen from $C_G(xax^{-1})$, $x^{-1}C_G(xax^{-1})x \subset C_G(a)$. Multiplication on the left by x and on the right by x^{-1} gives $C_G(b) = C_G(xax^{-1}) \subset xC_G(a)x^{-1}$. Since we have shown that each set contains the other, $xC_G(a)x^{-1} = C_G(b)$ as required.

□

Corollary 5.60 (Centralizer of non-central element is commutative). $IsCommutative_centralizer_of_not_mem_center$ *is abelian unless x belongs to the centre of L.*

Proof. $SL2_IsConj_do r_IsConj_so r_IsConj_n eg_so f_A lgClosed, conjugate_centralizers_of_IsConj, centralizer_se q_S Z, c$ which does not lie in the centre of $\mathrm{SL}_2(F)$ has centraliser $S \times Z$, whilst a non-central element of the form d_δ has centraliser D. Both S and D are abelian since they are isomoprhic to F and $F^\times$ respectively. Let $s_\sigma z_1$ and $s_\gamma z_2$ be arbitrary elements of $\times Z$.

$$\begin{aligned}(s_\sigma z_1)(s_\gamma z_2) &= s_\sigma s_\gamma z_2 z_1 && \text{(since } z_1 \in Z\text{)}\\ &= s_\gamma s_\sigma z_2 z_1 && \text{(since } T \text{ is abelian)}\\ &= (s_\gamma z_2)(s_\sigma z_1). && \text{(since } z_2 \in Z\text{)}\end{aligned}$$

Thus $S \times Z$ is also abelian. Since every element of $\mathrm{SL}_2(F)$ is conjugate to d_δ or $\pm s_\sigma$ by Proposition 5.48 and conjugate elements have conjugate centralisers by Proposition 5.59, the centraliser of each $x \in \mathrm{SL}_2(F) \setminus Z$ is conjugate to either $\times Z$ or D. Proposition **??**(iii) shows that conjugate subgroups are isomorphic and therefore have the same structure, thus since both $S \times Z$ and D are abelian, $C_{\mathrm{SL}_2(F)}(x)$ is also abelian. Note that in general this does hold for $x \in Z$, since its centraliser is the whole of $\mathrm{SL}_2(F)$which is not abelian unless $\mathrm{SL}_2(F) = Z$.

□

5.6 The Projective Line & Triple Transitivity

It is convenient to sometimes take a geometric viewpoint and regard the elements of $\mathrm{SL}_2(F)$as pairs of vectors in the 2-dimensional vector space over F, which we will denote V. An element of $\mathrm{SL}_2(F)$is thus a linear transformation of V.

Definition 5.61. Let L be the set of all 1-dimensional subspaces of V. A subset S of L is called a **subspace** of L if there is a subspace U of V such that S is the set of all 1-dimensional spaces of U. We have $\dim U = \dim S + 1$. The set L on which this concept of subspaces is defined is called the **projective line** on V and an element of L is a 0-dimensional subspace of L and consequently called a **point**. The projective line can be considered as a straight line in the field, plus a point at infinity.

Any 1-dimensional subspace of V is a set of vectors of the form ηu, where u is a non-zero vector of V and $\eta \in F^\times$. Thus the points of L are equivalence

classes with the following relation defined on the set of vectors of V.

$$u = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \sim \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = v \iff u = \eta v, \qquad (\text{for } \eta \in F^\times).$$

Notice that u and v are equivalent if and only if $u_1 v_2 = v_1 u_2$. Importantly each point P_i of L can be represented by a corresponding equivalence class of vectors of V, that is, P corresponds to u if $P = u_1/u_2$. In the case when $u_2 = 0$, this corresponds to the point at infinity.

Definition 5.62. Let S be a permutation group which acts on a set X and $\{x_1, x_2, x_3\}$ and $\{x_1', x_2', x_3'\}$ be two subsets of distinct elements of X. Then S is said be **triply transitive** on X if there is an element $\pi \in S$ such that,

$$x_i^\pi = x_i', \qquad (i = 1,2 \text{ or } 3).$$

Theorem 5.63. *Let L be the projective line over the field F. Then* $\mathrm{SL}_2(F)$*is triply transitive on the set of the points of L.*

Proof. Let P_1, P_2 and P_3 be distinct points of L and p_i be a vector in V corresponding to P_i. Since each P_i is distinct, p_1, p_2 and p_3 are thus pairwise linearly independent. Thus p_1 and p_2 form a basis for V and it's clear that there exist $\alpha, \beta \in F^\times$ such that,

$$p_3 = \alpha p_1 + \beta p_2.$$

Now, let Q_1, Q_2 and Q_3 be three more distinct points of L and q_i be a vector in V corresponding to Q_i. Similarly, by the above argument, there exist $\gamma, \delta \in F^\times$ such that,

$$q_3 = \gamma q_1 + \delta q_2.$$

Let $\pi \in GL(2, F)$ be the linear transformation which sends αp_1 to γq_1 and βp_2 to δq_2. Thus,

$$\pi(p_3) = \pi(\alpha p_1 + \beta p_2) = \pi(\alpha p_1) + \pi(\beta p_2) = \gamma q_1 + \delta q_2 = q_3$$

Hence we get $P_1^\pi = Q_1$, $P_2^\pi = Q_2$ and $P_3^\pi = Q_3$ and $GL(2, F)$ is triply transitive. Now set,

$$\eta = \sqrt{\frac{1}{\det \pi}}.$$

Consider the mapping θ which sends αp_1 to $\eta\gamma q_1$ and βp_2 to $\eta\delta q_2$. Observe that,

$$\det \theta = \eta^2 \det \pi = 1$$

So $\theta \in SL(2, F) = \mathrm{SL}_2(F)$and since $P_1^\theta = Q_1$, $P_2^\theta = Q_2$ and $P_3^\theta = Q_3$, we have that $\mathrm{SL}_2(F)$is also triply transitive.

□

The following proposition looks at what happens when the group $\mathrm{SL}_2(F)$acts on the projective line L.

Proposition 5.64. *(i) Each element of the form d_δ (with $\delta \neq \pm 1$), fixes the same two points on the projective line L and fix no other point.*

(ii) Each element of the form $\pm s_\sigma$ (with $\sigma \neq 0$), fixes the same point P on L and fix no other point. Furthermore, $\mathrm{Stab}(P) = H$.

(iii) All conjugate elements have the same number of fixed points on L.

(iv) Any noncentral element of $\mathrm{SL}_2(F)$*has at most 2 fixed points on L.*

Proof. (i) Let P be a fixed a point of an arbitrary $d_\delta \in D$, with $\delta \neq \pm 1$ and let u belong to the corresponding equivalence class of vectors of V to P.

$$d_\delta u = \begin{bmatrix} \delta & 0 \\ 0 & \delta^{-1} \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} u_1\delta \\ u_2\delta^{-1} \end{bmatrix} \sim \begin{bmatrix} u_1 \\ u_2 \end{bmatrix},$$

$$u_1u_2\delta = u_1u_2\delta^{-1}.$$

Since $\delta \neq \pm 1$, δ does not equal δ^{-1}, and so either $u_1 = 0$ or $u_2 = 0$. Thus u is equivalent to either the vector $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ or $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and these correspond to 2 distinct points of L which are fixed by d_δ.

(ii) Let P be a fixed a point of an arbitrary s_σ, with $\sigma \neq 0$, and let u be the corresponding element of V to P.

$$s_\sigma u = \begin{bmatrix} 1 & 0 \\ \sigma & 1 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} u_1 \\ u_1\sigma + u_2 \end{bmatrix} \sim \begin{bmatrix} u_1 \\ u_2 \end{bmatrix},$$

$$u_1u_2 = {u_1}^2\sigma + u_1u_2.$$

This gives ${u_1}^2\sigma = 0$ and since $\sigma \neq 0$ we have $u_1 = 0$. Thus s_σ has just one fixed point, P which corresponds to the equivalence class of $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ in V. We show also that P is also the only fixed point of $-s_\sigma$, with $\sigma \neq 0$.

$$-s_\sigma u = \begin{bmatrix} -1 & 0 \\ \sigma & -1 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} -u_1 \\ u_1\sigma - u_2 \end{bmatrix} \sim \begin{bmatrix} u_1 \\ u_2 \end{bmatrix},$$

$$-u_1u_2 = {u_1}^2\sigma - u_1u_2.$$

So again $u_1 = 0$ and $-s_\sigma$ fixes P and no other point. We now calculate the stabiliser of P in L, by considering which $x \in \mathrm{SL}_2(F)$fix P.

$$xu = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \beta \\ \delta \end{bmatrix} \sim \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Thus $\beta = 0$ and $x \in H$. Since x was chosen arbitrarily from $\mathrm{Stab}(P)$, we have $\mathrm{Stab}(P) \subset H$. Now let an arbitrarily chosen $y \in H$ act on P.

$$yu = \begin{bmatrix} \alpha & 0 \\ \gamma & \alpha^{-1} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ \alpha^{-1} \end{bmatrix} \sim \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Thus y and indeed H is contained in $\mathrm{Stab}(P)$, so $\mathrm{Stab}(P) = H$ as desired.

(iii) Let P_i $(i = 1, 2, ...)$ be the fixed points of $x \in \mathrm{SL}_2(F)$and let y be conjugate to x in L. That is, there exists a $g \in \mathrm{SL}_2(F)$such that $x = gyg^{-1}$.

$$\begin{aligned} xP_i &= P_i, \\ gyg^{-1}P_i &= P_i, \\ y(g^{-1}P_i) &= (g^{-1}P_i). \end{aligned}$$

This shows that P_i is a fixed point of x if and only if $g^{-1}P_i$ is a fixed point of y. Thus conjugate elements have the same number of fixed points.

(iv) By Proposition **??**(i), every element of $\mathrm{SL}_2(F)$is conjugate to either d_δ or $\pm s_\sigma$, so since conjugate elements have the same number of fixed points, every element of $\mathrm{SL}_2(F)\backslash Z$ has either the same number of fixed points as d_δ (with $\delta \neq \pm 1$), namely 2, or the same number as $\pm s_\sigma$, (with $\sigma \neq 0$), namely 1.

□

Chapter 6

The Maximal Abelian Subgroup Class Equation

6.1 A Finite Subgroup of $\mathrm{SL}_2(F)$

We now return to the realm of finite groups and consider G to be an arbitrary finite subgroup of $\mathrm{SL}_2(F)$. We will still continue to use Z to denote the centre of $\mathrm{SL}_2(F)$, and will use $Z(G)$ whenever we refer to the centre of G.

Observe that if Z is not contained in G, then Z must contain a non-identity element, thus $|Z| = 2$ and $p \neq 2$ by Lemma 5.38. Recall that $\mathrm{SL}_2(F)$ has a unique element of order 2 by Lemma 5.37, $-I_L$, which is not in G, therefore G has no element of order 2.

By Cauchy's Theorem, which says that if a prime p divides the order of a finite group, then the group contains an element of order p, we deduce that 2 does not divide the order of G.

This means that $|G|$ and $|Z|$ are relatively prime, so $G \cap Z = \{I_L\}$ and we can use Corollary 3.27 to show that $GZ \cong G \times Z$.

This shows that regardless of whether G contains Z or not, its structure is uniquely determined by GZ, so it suffices to only consider the case when $Z \subset G$.

6.2 Maximal Abelian Subgroups

Definition 6.1 (Maximal Abelian Subgroup). IsMaximalAbelian Let H and J be subgroups of a group G where H is abelian. H is called **maximal abelian** if J is not abelian whenever $H \subsetneq J$.

Remark 6.2. After the suggestion from Edward van de Meent, the definition in Lean was stated in positive form:

A subgroup H is said to be a maximal abelian subgroup of G if for every J subgroup of G satisfying $H \leq J$ we have that $J \leq H$. Which overall implies $H = J$ by antisymmetry of the preorder.

In Lean this statement looks like the following:

```
def IsMaximalAbelian {L : Type*} [Group L] (G : Subgroup L) : Prop := Maximal (IsCommutative) G
```

where the definition of `Maximal` in mathlib implicitly recognises the existence of a $\leq$ operator (a more primitive notion of a partial order) and is:

```
def Maximal (P :  → Prop) (x :  ) : Prop := P x     y , P y → x   y → y   x
```

Which informally means that an object M that satisfies a property is maximal if any other object K that also satisfies the property and is related to M by $M \leq K$ then in fact we must have the symmetric relation $K \leq M$.

When we define, $\leq := \subseteq$ then this is the natural notion of maximal.

Definition 6.3 (Elementary Abelian). IsElementaryAbelian A group G is said to be **elementary abelian** if it is abelian and every non-trivial element has order p, where p is prime.

Remark 6.4. In Lean we define the notion of a subgroup of H of G being elementary abelian the following way:

```
def IsElementaryAbelian {G : Type*} [Group G] (p :  ) (H : Subgroup G) : Prop :=
IsCommutative H    h : H, h   1 → orderOf h = p
```

Definition 6.5. IsMaximalAbelian MaximalAbelianSubgroupsOf Let $\mathfrak{M}$ denote the set of all maximal abelian subgroups of G.

Remark 6.6. When a set/object with some additional structure has been defined informally, when one wants to formalise results about the object it is often the case a decision has to be made about whether the set is defined in Lean as a set, whether it is defined as its own type or whether it should be a subtype of a more general type.

In this case, I have opted to define it as a set but later on when using quotients we shall see an example of how it is beneficial to define an object as a type/subtype in its own right.

Example 6.7. For example, in `mathlib` the set of $n \times n$ matrices, $\mathrm{Mat}(n; R)$ is defined as its own type. The General Linear Group is defined as the units of the $(n; R)^\times$ which is another type in itself. However, the Special Linear Group is defined as a subtype of (n, R). It is defined as:

```
def SpecialLinearGroup := { A : Matrix n n R // A.det = 1 }
```

Crucially, Lean does not understand subtypes to be definitionally equal to subsets!

Maximal abelian subgroups play an important role in determining the structure of G. In particular, every element in G must be contained in some maximal abelian subgroup, since every element commutes at least with itself and Z. This will allow us to decompose G into the conjugacy classes of these maximal abelian subgroups. Note also that unless $G = Z$, Z is not a maximal abelian subgroup, because for each $x \in G \backslash Z$, $\langle Z, x \rangle$ is clearly a larger abelian subgroup than Z.

We will shortly prove an important theorem regarding the maximal abelian subgroups of G, but in order to do so we require the following two lemmas.

Lemma 6.8. *IsElementaryAbelian.dvd$_c$ardIfGisafinitegroupoforderp^m where p is prime and $m > 0$, then p divides $|Z(G)|$.*

Proof. Let $C(x)$ be the set of elements of G which are conjugate in G to x, we call this the conjugacy class of x. Bhattacharya shows that the set of all conjugacy classes form a partition of G [**?**, p.112]. Now consider the following rearranged class equation of G, where S is a subset of G containing exactly one element from each conjugacy class not contained in $Z(G)$.

$$|G| - \sum_{x \in S} [G : N_G(x)] = |Z(G)|. \tag{6.1}$$

Since $|G| = p^m$, each subgroup of G is of order p^k for some $k \leq m$. In particular each $N_G(x)$ has order p^k and is strictly contained in G since $x \notin Z(G)$ by assumption. Thus each $[G : N_G(x)] > 1$, and are therefore divisible by p. Since p divides the left hand side of (6.1), it must also divide the right, thus p divides $|Z(G)|$.

□

Lemma 6.9. *order$_n$e$_c$harTheorderofanelementinthegroupofunitsofafield$F^\times$ cannot be equal to char(F).*

Proof. Suppose for a contradiction that there indeed exists an element $x \in F^\times$ of order p, where $x^p = \text{Frob}(x) = 1$. where Frob is the frobenius endomorphism.

Since $\text{Frob}(x) = textrmFrob(1) = 1 \iff \text{Frob}(x - 1) = 0 = \text{Frob}(0)$ and using the fact the frobenius endomorphism is injective we can conclude that $x - 1 = 0 \iff x = 1$ but this is a contradiciton as the order of $o(1) = 1$. Therefore, no such element can exist. □

Lemma 6.10 (Injection of a finite subgroup into the group of units of field). *coprime$_c$ard$_f$in$_s$ubgroup$_o$f$_i$nj$_h$om$_g$roup$_i$so$_u$nitsLetFbeafieldofcharacteristicp, letHbeafinitesubgroupofagr : $H \hookrightarrow F^\times$ then $|H|$ is coprime to p.*

Proof. order$_n$e$_c$hartheorderofthesubgroup|H|iscoprimetopifandonlyifp $\nmid |H|$. From 6.9 we know that for all $x \in F^\times$ we have that $o(x) \neq p$. Contraposing this statement, we now only need show that assuming $p \mid |H|$ we can deduce that there exists an element x of order p within F^x.

By Cauchy's theorem, we are guaranteed the existance of an element h in H that has oder p, but since f is a monomorphism, the order of $f(h)$ equals the order of h which is p. We have thus found witness and have proved the claim, which overall proves the original statement. □

Theorem 6.11. *MaximalAbelianSubgroupsOf MaximalAbelianSubgroup.centralizer$_m$eet$_{Gi}$n$_M$aximalAbelianSubg*
containing Z.
If $x \in G \backslash Z$ then we have $C_G(x) \in \mathfrak{M}$.

Proof. IsCommutative$_c$*entralizer$_o$f$_n$ot$_m$em$_c$enterLet*x*bechosenarbitrarily from*G
$\backslash Z$. Then by Corollary **??**, $C_{\mathrm{SL}_2(F)}(x)$ is abelian. By definition, $C_G(x) = C_{\mathrm{SL}_2(F)}(x) \cap G$, and using the elementary fact that the intersection of two subgroups is itself a subgroup, we have $C_G(x) < C_{\mathrm{SL}_2(F)}(x)$. Now since every subgroup of an abelian group is abelian, $C_G(x)$ is also abelian.

Now let J be a maximal abelian subgroup of G containing $C_G(x)$. Since J is abelian and $x \in C_G(x) \subset J$, we have $jx = xj$, $\forall j \in J$, thus $J \subset C_G(x)$. Therefore $J = C_G(x)$ and $C_G(x) \in \mathfrak{M}$.

□

Before we continue proving properties about Maximal Abelian Subgroups, we first need to understand how commutative subgroups interact with subgroups of $\mathrm{SL}_2(F)$. We now list a few results about commutative subgroups and their interaction with other subgroups:

Corollary 6.12. *IsCommutative$_o$f$_I$sCommutative$_s$ubgroupOf LetH, Kbetwosubgroupsof agroupGthenH $\sqcap$K = H $\cap$ K is commutative if H $\sqcap$ K regarded as a subgroup of K is commutative.*

Proof. Trivial □

Remark 6.13. The coroallary above 6.12 probably seems trivial, but Lean genuinely understands both objects as belonging to completely different types and this result is necessary to be able to jump between the corresponding contexts.

Lemma 6.14. *center$_m$ulLetHbeasubgroupof agroupGthenthepointwisesetproductZ(G) Hisasubgroupof G*

Proof.
1. `one_mem'`: Both $Z(G)$ and H are subgroups of G so they contain the identity element, thus $1 \cdot 1 \in Z(G)H$.
2. `mul_mem'`: Let $z_1h_1, z_2h_2 \in Z(G)H$ then $z_1h_1z_2h_2 = z_1z_2h_1h_2 \in Z(G)H$ as z_i is in the center.
3. `inv_mem'`: Let $zh \in Z(G)H$ then $z^{-1}h^{-1} \in Z(G)H$ and $zhz^{-1}h^{-1} = zz^{-1}hh^{-1} = 1$.

□

Lemma 6.15 (The join of a commutative subgroup with the center of a group is commutative). $IsComm_of_center_joi n_IsComm$

Let H be a commutative subgroup of G then the subgroup $Z(G) \sqcup H$ is a commutative subgroup of G.

Proof. center$_m$ul*Let*x, y $\in Z(G) \sqcup H$ recalling that the supremum can be thought of taking the closure we know that if x and y belong to the closure then since $Z(G)H$ is a subgroup of G and $Z(G) \sqcup H \subseteq Z(G)H$ we know that $x, y \in Z(G)H$ and thus there exist $z_1h_1 = x$ and $z_2h_2 = y$. Therefore, we can now show that x and y commute:

$$\begin{aligned} xy &= z_1h_1z_2h_2 \\ &= z_1z_2h_1h_2 && \text{(as } z_2 \text{ is in the center)} \\ &= z_2z_1h_2h_1 && \text{(as } H \text{ is a commutative subgroup)} \\ &= z_2h_2z_1h_1 && \text{(as } z_1 \text{ is in the center)} \end{aligned}$$

□

Lemma 6.16 (Z is contained within any Maximal Abelian Subgroup of a subgroup containing Z). *MaximalAbelianSubgroupsOf, SpecialSubgroups.Z MaximalAbelianSubgroup.center$_l$eLetH*
$\leq H$ then for any maximal abelian subgroup of H, A we have that $Z(G) \leq A$

Proof. IsCommutative$_o f_IsCommutative_subgroupOf, IsComm_of_center_joi n_IsComm$

Suppose for a contradiction that $Z(G) \not\leq A$, then there exists $z \in Z(G)$ which does not belong to A.

We construct the larger subgroup $A \sqcup Z(G)$ which is abelian by 6.15. Since A is a maximal abelian subgroup and $A \leq A \sqcup Z(G)$ we must have that $A \sqcup Z(G) \leq A$, but this is impossible because $z \in A \sqcup Z(G)$ but $z \notin A$, thus a contradiction. □

Lemma 6.17. *MaximalAbelianSubgroupsOf MaximalAbelianSubgroup.le$_c$entralizer$_o f_m$emLetHbeasubgroupof G*
$\in A$ then $A \leq C_G(x)$.

Proof. IsCommutative$_o f_IsCommutative_subgroupOf$LetHbeasubgroupofagroupGandletAbeamaximalabelian
$\in A$, because $x \in A$ and A is maximal abelian and thus abelian, we have that $ax = xa$. Therefore, $a \in C_G(x)$ as required □

Lemma 6.18. *MaximalAbelianSubgroupsOf MaximalAbelianSubgroup.not$_l$e$_o f_n$eLetHbeasubgroupofagroupGand*
$\neq B$ be maximal abelian subgroups of H then $B \not\leq A$.

Proof. Suppose for a contradiction that $B \leq A$, then by the maximality of B and because A is commutative as it is maximal abelian we must have that $A \leq B$. But this shows $A = B$ by antisymmetry, a contradiction. □

Lemma 6.19. *MaximalAbelianSubgroupsOf MaximalAbelianSubgroup.lt$_c$en$_m$eet$_G$LetHbeasubgroupof G, letA*
$\neq B$ be maximal abelian subgroups of H and let $x \in A \cap B$ then $A < C_G(x) \sqcap H$.

Proof. MaximalAbelianSubgroup.not$_l$e$_o$f$_n$e, $MaximalAbelianSubgroup.le_centralizer_of_memToshowtheinequa$

We show that the inequality holds by transitivity. Since $A < A \cup B$ because 6.18 guarantees $B \not\leq A$, furthermore, $A \cup B \leq C_G(x)$ by 6.17 where we use the fact that both $x \in A$ and $x \in B$; and $A \cup B \leq H$ since $A, B \leq H$. We can conclude that indeed, $A \cup B \leq C_G(x) \sqcap H$.

Overall, by transitivity we have that $A < C_G(x) \sqcap H$.

□

Theorem 6.20. *MaximalAbelianSubgroupsOf, SpecialSubgroups.Z MaximalAbelianSubgroup.center$_e$q$_m$eet$_o$f$_n$e$_M$a*

Proof. MaximalAbelianSubgroup.centralizer$_m$eet$_{Gi}$n$_M$aximal$AbelianSubgroups_of_n$oncentral, $MaximalAbeli$ $\in A \cap B$. Since both A and B are abelian, x commutes with each $a \in A$ and $b \in B$ and thus $C_G(x)$ contains both A and B. If $x \in G \setminus Z$, then $C_G(x) \in \mathfrak{M}$ by 6.11 and because A and B are distinct we have $A \subsetneq A \cup B \subset C_G(x)$. This contradicts the fact that A is maximum abelian and thus $x \in Z$. Finally, note that Z is contained in every maximal abelian subgroup, since otherwise we would have the contradiction that $\langle A, Z \rangle$ would generate a larger abelian subgroup than A. Hence $A \cap B = Z$.

□

Lemma 6.21. *MaximalAbelianSubgroupsOf, IsMaximalAbelian MaximalAbelianSubgroup.singleton$_o$f$_c$en$_e$q$_G$LetH* $= Z(G)$*thenthemaximalabeliansubgroupsareM* $= \{Z(G)\}$.

Proof. MaximalAbelianSubgroup.center$_l$e*WeshowthatA* $\in \mathfrak{M}$ if and only if $A = Z(G)$

- $\Rightarrow$ Suppose A is a maximal abelian subgroup of H, then by **??** $Z(G) \leq A$. Furthermore, $A \leq H = Z(G)$; which overall shows $A = Z(G)$ as required.
- $\Leftarrow$ Suppose $A = Z(G)$ we now show that A is a maximal abelian subgroup. On the one hand, $A = Z(G)$ so it follows that A is abelian. On the other hand, we need to show that $Z(G)$ is maximal. Let B be a subgroup of H that is commutative and such that $Z(G) \sqcap H \leq B$, we show that it follows that $B \leq Z(G) \sqcap H$. But this follows trivially as $B \leq H = Z(G) \sqcap H = \top$.

□

Lemma 6.22. *MaximalAbelianSubgroupsOf, SpecialSubgroups.Z MaximalAbelianSubgroup.IsCyclic$_a$nd$_c$ard$_C$opri* $= Z(G)$*thenanelementAofM, themaximalabeliansubgrupsof Gisacyclicgroupwhoseorderisrelativelyprimeto*

Proof. MaximalAbelianSubgroup.singleton$_o$f$_c$en$_e$q$_G$, $SpecialSubgroups.card_Ze$q$_t$wo$_o$f$_t$wo$_n$e$_z$ero, $SpecialSubgr$ $\neq 2$ then $|G| = 2$ and G is a cyclic group whose order is relatively prime to p. If $p = 2$ then $G = I_G$ which is trivially a S_p-subgroup.

□

Corollary 6.23. *mem$_c$entralizer$_s$elf LetGbeagroupthencentralizerofanelementx* $\in G$, $C_G(x)$ *contains* x.

Proof. An element always commutes with itself. □

```
lemma mem_centralizer_self {G : Type*} [Group G] (x : G) : x  centralizer {x} := by
  rintro y  rfl ; rfl
```

Lemma 6.24. *MaximalAbelianSubgroupsOf MaximalAbelianSubgroup.center*$_n$*ot*$_m$*emLetFbeanalgebraicallyclose*
where $G \neq Z(\mathrm{SL}_2(F))$ *then the center is not a maximal abelian subgroup of* G*,*
$Z \notin \mathfrak{M}$*.*

Proof. mem$_c$*entralizer*$_s$*elf*, *MaximalAbelianSubgroup.centralizer*$_m$*eet*$_{Gi}$*n*$_M$*aximalAbelianSubgroups*$_o$*f*$_n$*on*
$\leq G$ and $Z \not\leq G$.

- In the case where $Z \leq G$

  Since $Z \leq G$ and $Z \neq G$ it follows that $Z < G$, and so there must exist an x element in G which does not belong to Z. Therefore, since $x \in G \setminus Z$ by 6.11 $C_{\mathrm{SL}_2(F)}(x) \sqcap G \in \mathfrak{M}$, but since $x \notin Z$ yet $x \in C_{\mathrm{SL}_2(F)} \sqcap G$ by 6.23 it follows that $Z < C_{\mathrm{SL}_2(F)}(x) \sqcap G$, thus Z is not a maximal abelian subgroup.

- In the case where $Z \not\leq G$

  Suppose for a contradiction Z is maximal abelian subgroup of G, then it follows that $Z \leq G$; this contradicts the assumption that $Z \not\leq G$. Thus Z is not a maximal abelian subgroup of G in this case either.

□

```
lemma center_not_mem {F : Type*} [Field F] [IsAlgClosed F] [DecidableEq F] (G : Subgroup SL(2,F))
  (hG : center SL(2,F)  G) : center SL(2,F)  MaximalAbelianSubgroupsOf G := by
  intro h
  by_cases h' : center SL(2,F)  G
  · obtain  x, x_in_G, x_not_in_cen  := SetLike.exists_of_lt (lt_of_le_of_ne h' hG)
    have centra_ne_cen : centralizer {x}  G  center SL(2,F) := by
      apply ne_of_gt
      rw [SetLike.lt_iff_le_and_exists]
      split_ands
      · exact le_inf (Subgroup.center_le_centralizer ({x} : Set SL(2,F))) h'
      · exact  x,  mem_centralizer_self x, x_in_G , x_not_in_cen
    have centra_mem_MaxAbSub :=
      centralizer_meet_G_in_MaximalAbelianSubgroups_of_noncentral
        G x (Set.mem_diff_of_mem x_in_G x_not_in_cen)
    have cen_le_centra : center SL(2, F)  centralizer {x}  G :=
      le_inf (center_le_centralizer {x}) h'
    have cen_le_centra' : (center SL(2, F)).subgroupOf G  (centralizer {x}  G).subgroupOf G := by
      simp [← map_subtype_le_map_subtype]; rw [inf_of_le_left h']; exact center_le_centralizer {x}
    have centra_le_cen := h.left.right centra_mem_MaxAbSub.left.left cen_le_centra'
    simp [← map_subtype_le_map_subtype] at centra_le_cen
    absurd centra_ne_cen (le_antisymm centra_le_cen cen_le_centra)
    trivial
  · absurd h' h.right
    trivial
```

Lemma 6.25. *MaximalAbelianSubgroupsOf MaximalAbelianSubgroup.le*$_c$*entralizer*$_m$*eetLetHbeasubgroupofagro*
$\in A \subseteq G$ *then* $A \leq C_{\mathrm{SL}_2(F)} \sqcap H$*.*

Proof. MaximalAbelianSubgroup.le$_c entralizer_o f_m em$

Since $x \in A$ by 6.17 we have that $A \leq C_{\mathrm{SL}_2(F)}$ and considering A is a maximal abelian subgroup of G, it follows that $A \leq C_{\mathrm{SL}_2(F)} \sqcap G$. □

```
theorem le_centralizer_meet {G : Type*} [Group G] (A H : Subgroup G)
  (hA : A  MaximalAbelianSubgroupsOf H) (x : G) (x_in_A : x  A) :
  A  centralizer {x}  H := by
  apply le_inf
  exact le_centralizer_of_mem hA x_in_A
  apply hA.right
```

Lemma 6.26. *MaximalAbelianSubgroupsOf, SpecialSubgroups.Z MaximalAbelianSubgroup.eq$_c$entralizer$_m$eet$_o f_c$e where A is a maximal abelian subgroup of G and $Z(\mathrm{SL}_2(F)) < A$ then there exists an element $x \in G \setminus Z(SL(2)) \subseteq \mathrm{SL}_2(F)$ such that $A = C_{\mathrm{SL}_2(F)}(x) \sqcap G = C_G(x)$.*

Proof. MaximalAbelianSubgroup.centralizer$_m$eet$_{Gi}$n$_M$aximalAbelianSubgroups$_o f_n$oncentral, $MaximalAbeli$ < A, $thereexistsa$x $\in A \setminus Z$, this will be our desired witness. Since $x \in A \setminus Z \subseteq G \setminus Z$ as $A \leq G$, by 6.11 $C_{\mathrm{SL}_2(F)} \sqcap G \in \mathfrak{M}$. By 6.25 it follows that $A \leq C_{\mathrm{SL}_2(F)} \sqcap G$. Similarly, by the maximality of A we also have that $C_{\mathrm{SL}_2(F)} \sqcap G \leq A$. Therefore, $C_{\mathrm{SL}_2(F)} \sqcap G = A$. □

```
lemma eq_centralizer_meet_of_center_lt {F : Type*} [Field F] [IsAlgClosed F] [DecidableEq F]
  (A G : Subgroup SL(2,F)) (center_lt : center SL(2,F) < A) (hA : A  MaximalAbelianSubgroupsOf G) :
   x : SL(2,F), x  G.carrier \ center SL(2,F)  A = centralizer {x}  G := by
  rw [SetLike.lt_iff_le_and_exists] at center_lt
  obtain -, x, x_in_A, x_not_in_center := center_lt
  have hx : x  G.carrier \ center SL(2,F) := Set.mem_diff_of_mem (hA.right x_in_A) x_not_in_center
  obtain  centra_meet_G_IsComm, - , - :=
    centralizer_meet_G_in_MaximalAbelianSubgroups_of_noncentral G x hx
  -- We show centralizer {x}  G  A
  have A_le_centralizer_meet_G := (le_centralizer_meet A G hA x x_in_A)
  have A_le_centralizer_meet_G' : A.subgroupOf G  (centralizer {x}  G).subgroupOf G := by
    simp [← map_subtype_le_map_subtype]
    exact le_trans inf_le_left <| le_trans A_le_centralizer_meet_G inf_le_left
  -- by using the maximality of A and using the fact A  centralizer {x}  G
  have centralizer_meet_G_le_A := hA.left.right centra_meet_G_IsComm A_le_centralizer_meet_G'
  simp [← map_subtype_le_map_subtype] at centralizer_meet_G_le_A
  -- We show A = centralizer {x}  G
  exact  x, hx, le_antisymm A_le_centralizer_meet_G centralizer_meet_G_le_A
```

Theorem 6.27. *MaximalAbelianSubgroup.IsCyclic$_a$nd$_c$ard$_c$oprime$_C$har$P_o f_I$sConj$_d$LetFbeanalgebraicallyclose containing Z, let A be a subgroup of $\mathrm{SL}_2(F)$ which is a maximal abelian subgroup of G and furthermore suppose that $A = C_{\mathrm{SL}_2(F)}(x) \sqcap G$ where $x \in \mathrm{SL}_2(F) \setminus Z$ and that x is conjugate to d_δ for some $\delta \in F^\times$ then A is cyclic and the cardinality of A is coprime to p.*

Proof. SpecialSubgroups.center$_S L2_e q_Z$, $conjugate_c entralizers_o f_I sConj$, $centralizer_{de} q_D$, $SpecialMatrices.d$, $x = y d_\delta y^{-1} = d_\delta \in Z$.

Thus $\omega \neq \pm 1$. Let $A = C_G(x)$, since $C_G(x) \in \mathfrak{M}$ by part (i). Observe that

$$\begin{aligned} C_G(d_\delta) &< C_{\mathrm{SL}_2(F)}(d_\delta) && \text{(see proof of (i))} \\ &= D && \text{(by Lemma 5.58)} \\ &\cong F^\times. && \text{(by Lemma 5.26)} \end{aligned}$$

Since A is conjugate to $C_G(d_\delta)$ by Proposition 5.58, we have that A is isomorphic to a finite subgroup of $F^\times$, A is cyclic. By Lagrange's Theorem any finite subgroup of $F^\times$ has an order which divides $p^m - 1$ for some $m \in \mathbb{Z}^+$, and since $p \nmid (p^m - 1)$, $|A|$ is relatively prime to p.

□

```
theorem IsCyclic_and_card_coprime_CharP_of_IsConj_d {F : Type*} [Field F]
  [IsAlgClosed F] [DecidableEq F] {p :  } [hp' : Fact (Nat.Prime p)] [hC : CharP F p]
  (G : Subgroup SL(2,F)) [hG  : Finite G] (A : Subgroup SL(2,F)) (x : SL(2,F))
  (x_not_in_center : x   center SL(2,F)) (A_eq_centra : A = centralizer {x}   G )
  (  : F ) (x_IsConj_d : IsConj (d  ) x ) :
  (IsCyclic A   Nat.Coprime (Nat.card A) p) := by
  simp [center_SL2_eq_Z] at x_not_in_center
  have  _ne_one :    1 := by rintro rfl; simp_all
  have  _ne_neg_one :    -1 := by rintro rfl; simp_all
  obtain  c, c_smul_D_eq_centralizer  :=
      conjugate_centralizers_of_IsConj (SpecialMatrices.d  ) x x_IsConj_d
  rw [centralizer_d_eq_D   _ne_one  _ne_neg_one] at c_smul_D_eq_centralizer
  -- A = conj c • D   G   conj c • D F
  have A_le_conj_D :=
      le_trans (le_of_eq A_eq_centra) <|
      le_trans inf_le_left (le_of_eq c_smul_D_eq_centralizer.symm)
  -- to prove A has cardinality coprime to p we construct the following homomorphism
  -- compose the monoid homomorphisms of inclusions and isomorphisms
  let f  : A →* (conj c • D F:) := inclusion A_le_conj_D
  let f  : (conj c • D F:) →* D F := (MulEquiv.subgroupMap (conj c) (D F)).symm.toMonoidHom
  let f  : (D F) →* F  := (D_iso_units F).toMonoidHom
  let f : A →* F  := f .comp (f .comp f )
  -- f is injective
  have f_inj : Injective f := by
    dsimp [f]
    apply Injective.comp
    exact MulEquiv.injective (D_iso_units F)
    apply Injective.comp
    -- we construct the monoid homomorphism from the isomorphism
    exact MulEquiv.injective (MulEquiv.subgroupMap (conj c) (D F)).symm
    -- we construct the inclusion monoid homomorphism
    exact inclusion_injective A_le_conj_D
  -- to prove A is cyclic we construct the following homomorphism
  -- `F *← F  *← A`
  let f' : A →* F := (Units.coeHom F).comp f
  have f'_inj : Injective f' := by
    dsimp [f']
    apply Injective.comp
    exact Units.coeHom_injective
    exact f_inj
  let inst : Finite A := A_eq_centra   Set.Finite.subset hG  inf_le_right
  split_ands
    -- A is cyclic as it is finite and there exists a monoid monomorphism into F
```

```
· exact isCyclic_of_subgroup_isDomain f' f'_inj
  -- cardinality of A is coprime to p, the characteristic of F as F  has no element of order p
  -- after looking at the frobenius endomorphism
· exact coprime_card_fin_subgroup_of_inj_hom_group_iso_units A f f_inj
```

Remark 6.28 (Formalising properties preserved by isomorphisms in Lean). Formalising the argument above required fleshing out many more detail than the informal proof lead one to believe. In particular it was the following line of reasoning which required a lot of unpacking and making explicit isomorphisms and constructing explicit subgroups as the image of another subgroup pulled along the isomorphism:

$$\begin{aligned} C_G(d_\delta) &< C_{\mathrm{SL}_2(F)}(d_\delta) && \text{(see proof of (i))} \\ &= D && \text{(by Lemma 5.58)} \\ &\cong F^\times. && \text{(by Lemma 5.26)} \end{aligned}$$

Since A is conjugate to $C_G(d_\delta)$ by Proposition 5.58, we have that A is isomorphic to a finite subgroup of $F^\times$, A is cyclic.

This argument which has been left intact in the proof, had to be heavily modified and expanded upon. Since it was necessary to actually construct a group monomorphism of $f : A \hookrightarrow F^\times$ by composing the following maps

$$A \hookrightarrow cDc^{-1} \twoheadrightarrow D \hookrightarrow F^\times$$

From this monomorphism we then use the mathlib theorem `isCyclic_of_subgroup_isDomain` to prove A is cyclic; the theorem says:

If a finite subgroup has a monomorphism into the unit group of an integral domain, then the subgroup is cyclic.

This illustrates a typical issue one runs into when formalising mathematics:

Often the result you are looking for is a special case of a more general theorem.

Similarly, to prove the cardinality of A is coprime to p we use 6.10, which required proving some more intermediate results which involved the Frobenius endomorphism and other results from field theory.

To prove the statement when x is conjugate to s_σ for some $\sigma \in F$ we first need the following lemmas:

Lemma 6.29. *SpecialSubgroups.SZ, SpecialMatrices.s, MaximalAbelianSubgroupsOf, SpecialSubgroups.Z MaximalAbelianSubgroup.centralizer$_e$q$_c$onj$_S$Z$_o$f$_I$sConj$_{so}$r$_I$sConj$_n$eg$_s$*

Let F be an algebraically closed field, let G be a subgroup of $\mathrm{SL}_2(F)$, let $A \in \mathfrak{M}$, suppose $A = C_{\mathrm{SL}_2(F)} \sqcap G$ for some x in $G \setminus Z \subseteq \mathrm{SL}_2(F)$ which is conjugate to either s_σ or $-s_\sigma$ for $\sigma \neq 0$ then there exists a $c \in \mathrm{SL}_2(F)$ such that $cSZc^{-1} = C_{\mathrm{SL}_2(F)}(x)$

Proof. conjugate$_c$*entralizers$_o$f$_I$sConj, centralizer$_{se}$q$_S$Z, centralizer$_n$eg$_e$q$_c$entralizer, SpecialSubgroups.cent* $\notin Z$, x is not conjugate to either $s_0 = I \in Z$ or $-s_0 = -I \in Z$.

Given conjugate elements have conjugate centralizers by 5.59 it follows that

$$C_{\mathrm{SL}_2(F)}(x) = cC_{\mathrm{SL}_2(F)}(s_\sigma)c^{-1}$$

Where the last equality is a result of 5.57. □

```
lemma centralizer_eq_conj_SZ_of_IsConj_s_or_IsConj_neg_s {F : Type*} [Field F]
  [IsAlgClosed F] [DecidableEq F] (A G : Subgroup SL(2,F)) ( : F) (x : SL(2,F))
  (x_IsConj_s_or_neg_s : IsConj (s ) x  IsConj (- s ) x)
  (x_in_G : x  G.carrier) (x_not_in_center : x  center SL(2,F)) (hx : centralizer {x}  G = A) :
   c : SL(2,F), conj c • SZ F = centralizer {x} := by
  simp [center_SL2_eq_Z, ← ne_eq] at x_not_in_center
  obtain  x_ne_one, x_ne_neg_one  := x_not_in_center
  have  _ne_zero :    0 := by
    rintro rfl
    simp at x_IsConj_s_or_neg_s
    symm at x_IsConj_s_or_neg_s
    rcases x_IsConj_s_or_neg_s with (rfl | rfl) <;> contradiction
  rcases x_IsConj_s_or_neg_s with (x_IsConj_s | x_IsConj_neg_s)
  · obtain  c, c_smul_SZ_eq_centralizer  :=
      conjugate_centralizers_of_IsConj (s ) x x_IsConj_s
    rw [centralizer_s_eq_SZ  _ne_zero] at c_smul_SZ_eq_centralizer
    exact Exists.intro c c_smul_SZ_eq_centralizer
  · obtain  c, c_smul_SZ_eq_centralizer  :=
      conjugate_centralizers_of_IsConj (- s ) x x_IsConj_neg_s
    rw [← centralizer_neg_eq_centralizer,
      centralizer_s_eq_SZ  _ne_zero] at c_smul_SZ_eq_centralizer
    exact Exists.intro c c_smul_SZ_eq_centralizer
```

We need the following computations that will allow us to treat the complete lattice structure as a complete *distributive*, that is, a complete lattice that furthermore satisfies $(H \sqcup K) \sqcap L = (H \sqcap L) \sqcup (K \sqcap L)$. An interesting remark on lattices is that the two distinct distributivity laws automatically imply the other.

Lemma 6.30. *SpecialSubgroups.S, SpecialSubgroups.Z MaximalAbelianSubgroup.conj*$_{S\,j}oin_{Z\,m}eet_{G\,e}q_{c}onj_{S\,m}eet$ $\in \mathrm{SL}_2(F)$ *and* G *be a subgroup of* $\mathrm{SL}_2(F)$ *then* $c(S \sqcup Z)c^{-1} \sqcap G = (cSc^{-1} \sqcap G) \sqcup Z$

Proof. SpecialSubgroups.center$_S L2_e q_Z W e s h o w t h i s b y d i r e c t c o m p u t a t i o n$

$$\begin{aligned} c(S \sqcup Z)c^{-1} \sqcap G &= (cSc^{-1} \sqcup Z) \sqcap G \\ &\qquad \text{(because } c \text{ and } c^{-1} \text{ commute with elements in } Z) \\ &= (cSc^{-1} \sqcap G) \sqcup (Z \sqcap G) \qquad \text{(see the reasoning below †)} \\ &= (cSc^{-1} \sqcap G) \sqcup Z \qquad \text{(since } Z \leq G) \end{aligned}$$

The justification for † is the following, it sufficient to prove that $(cSc^{-1} \sqcup Z) \sqcap G$ and $(cSc^{-1} \sqcap G) \sqcup (Z \sqcap G)$ are equal as subsets. Considering $A \sqcap B = AcapB$ and for a if either subgroup is normal $A \sqcup B = AB$ where the right hand side is the pointwise product. Thus proving

$$(cSc^{-1} \sqcup Z) \sqcap G = (cSc^{-1} \sqcap G) \sqcup (Z \sqcap G)$$

is equivalent to showing the subset equality

$$(cSc^{-1}Z) \cap G = (cSc^{-1} \cap G)Z$$

We show this by antisymmetry

- We show $(cSc^{-1}Z) \cap G \subseteq (cSc^{-1} \cap G)Z$

  Let $csc^{-1}z \in (cSc^{-1}Z) \cap G$, since $z \in Z \subseteq G$ we have that $csc^{-1}zz^{-1} = csc^{-1} \in (cSc^{-1} \cap G)$ it then follows that $csc^{-1}z \in (cSc^{-1} \cap G)Z$

- We show $(cSc^{-1}Z) \cap G \supseteq (cSc^{-1} \cap G)Z$

  Let $csc^{-1}z(cSc^{-1} \cap G)Z$ then since $csc^{-1} \in (cSc^{-1}Z)$, we only need show $csc^{-1}z \in G$, by assumption $csc^{-1} \in G$ and since $z \in Z \subseteq G$, the claim follows.

□

```
lemma conj_S_join_Z_meet_G_eq_conj_S_meet_G_join_Z {F : Type*} [Field F]{G : Subgroup SL(2,F)}
  (center_le_G : center SL(2,F)  G) (c : SL(2,F)) :
  (conj c • (S F  Z F))  G = conj c • S F  G  Z F :=
  calc
  (conj c • (S F  Z F))  G = (conj c • S F  Z F)  G := by
    simp [smul_sup, ← center_SL2_eq_Z, smul_normal c]
  _ = (conj c • S F  G)  (Z F  G) := by
        ext y
        rw [← SetLike.mem_coe, ← Z_eq_Z_meet_G F G center_le_G, ← center_SL2_eq_Z,
          Subgroup.coe_inf, Subgroup.mul_normal (N := center SL(2,F)), ← SetLike.mem_coe,
          Subgroup.mul_normal (N := center SL(2,F)), Subgroup.coe_inf]
        constructor
        · rintro  s, s_in_S, z, hz, rfl , y_in_G
          simp at y_in_G
          use s
          split_ands
          · exact s_in_S
          · rw [← mul_one s, ← mul_inv_cancel z, ← mul_assoc]
            exact Subgroup.mul_mem G y_in_G <| inv_mem (center_le_G hz)
          use z
        · rintro  s,  s_in_S, s_in_G , z, z_in_Z, rfl
          simp
          split_ands
          · use s
            split_ands
            exact s_in_S
            use z
          exact Subgroup.mul_mem G s_in_G <| center_le_G z_in_Z
  _ = (conj c • S F  G)  Z F := by rw [← Z_eq_Z_meet_G F G center_le_G]
```

We also need the following computation:

Lemma 6.31. *SpecialSubgroups.Z, SpecialSubgroups.S MaximalAbelianSubgroup.conj$_i$nv$_c$onj$_e$qLet c* $\in \mathrm{SL}_2(F)$ *and G be a subgroup of* $\mathrm{SL}_2(F)$ *then*

$$c^{-1}(c(S \sqcap G)c^{-1} \sqcup Z)c = (S \sqcap c^{-1}Gc) \sqcup Z$$

Proof. SpecialSubgroups.center$_S L2_e q_Z Sinceeveryelementof$Z$commuteswitheveryelementof\mathrm{SL}_2(F)$ the claim follows. □

```
lemma conj_inv_conj_eq (F : Type*) [Field F](G : Subgroup SL(2,F)) (c : SL(2,F)):
  conj c ⁻¹ • ((conj c • S F   G)   Z F) = (S F   conj c ⁻¹ • G)   Z F := by
  simp only [smul_inf, ← center_SL2_eq_Z, smul_normal c ⁻¹, smul_sup]
  simp [map_inv, inv_smul_smul]
```

Corollary 6.32. *IsElementaryAbelian IsElementaryAbelian.subgroupOf If a subgroup H of a group G is an elementary abelian subgroup then for any subgroup K we have that $H \sqcap K$ is also an elementary abelian subgroup.*

Proof. The only difficulty is verifying is that every element is thought of as an element of K, since we are restricting the subgroup H to be a subgroup of K by taking the infimum $H \sqcap K$. □

```
lemma subgroupOf {G : Type*} [Group G]
  (H K : Subgroup G) {p :  } [Fact (Nat.Prime p)] (hH : IsElementaryAbelian p H) :
  IsElementaryAbelian p (H.subgroupOf K) := by
  refine  ?IsCommutative, ?orderOf_eq_p
  case IsCommutative =>
    let IsCommutative_H : IsCommutative H := hH.left
    exact subgroupOf_isCommutative K H
  case orderOf_eq_p =>
    rintro  h, hh  h_ne_one
    have h_in_H := hh
    simp [mem_subgroupOf] at h_in_H
    have h_ne_one' :  (h : G), h_in_H   (1 : H) := by
      simp
      rintro rfl
      simp_all
    have order_of_eq_p' := hH.right  (h : G), h_in_H  h_ne_one'
    simp [← order_of_eq_p']
```

Lemma 6.33. *SpecialSubgroups.center$_S L2_e q_Z$, SpecialSubgroups.card$_{Ze} q_o ne_o f_t wo_e q_z ero$, SpecialSubgroups.c
let S be a p-Sylow subgroup of G where p is the characteristic of the field F and furthermore suppose $p \leq |Z|$ then there exists a noncenter element in S, that is, $S \setminus Z \neq \varnothing$.*

Proof. SpecialSubgroups.center$_S L2_e q_Z$, SpecialSubgroups.card$_{Ze} q_o ne_o f_t wo_e q_z ero$, SpecialSubgroups.card$_{Ze} q$
$< |\mathrm{S}|$*andtherefore*, *regardlesstowhat*Z*and*S*actuallylooklike*, *theremustexistanelementin*S*thatdoesnotbelongt*

- When $p = \mathrm{char}(F) = 2$
  by 5.39 it follows $|Z| = 1 < 2 = p \leq |S|$, as required.
- When $p = \mathrm{char}(F) \neq 2$
  by 5.38 it follows $|Z| = 2 < 3 \leq p \leq |S|$, as required.

□

```
lemma exists_noncenter_of_card_center_lt_card_center_Sylow (F : Type*) [Field F] {p :  }
  [hp' : Fact (Nat.Prime p)] [hC : CharP F p] (G : Subgroup SL(2,F)) [Finite G] (S : Sylow p G)
  (p_le_card_center_S : p   Nat.card  (center S)) :
   x   (Subgroup.map (G.subtype.comp S.toSubgroup.subtype) (center S)), x   center SL(2,F) := by
  let fintype_G : Fintype G := Fintype.ofFinite  G
```

```
let fintype_center_S : Fintype (center S) := Fintype.ofFinite  (center S)
let fintype_set_center_S :
  Fintype (center SL(2, F)) := Fintype.ofFinite  (center SL(2, F))
let fintype_map :
      Fintype
        ((Subgroup.map (G.subtype.comp S.toSubgroup.subtype) (center S)) : Set SL(2,F)) := by
      rw [Subgroup.coe_map, MonoidHom.coe_comp]
      exact Fintype.ofFinite ↑( G.subtype   (S.toSubgroup).subtype '' ↑(center S))
let fintype_image :
      Fintype
        ↑(( G.subtype.comp S.toSubgroup.subtype) '' (center S)) : Set SL(2,F)) := fintype_map
have : Fintype.card
      ((Subgroup.map (G.subtype.comp S.toSubgroup.subtype) (center S)) : Set SL(2,F)) =
        Fintype.card (center S) := by
      apply Set.card_image_of_injective
      rw [MonoidHom.coe_comp]
      refine Injective.comp ?h1 ?h2
      · exact subtype_injective G
      · exact subtype_injective S.toSubgroup
let inst  : CommRing F := Field.toCommRing
let inst  : NoZeroDivisors F := IsLeftCancelMulZero.to_noZeroDivisors F
have card_center_lt_card_center_S :
  Fintype.card ((center SL(2,F)) : Set SL(2,F)) <
    Fintype.card
      ((Subgroup.map (G.subtype.comp S.toSubgroup.subtype) (center S)) : Set SL(2,F)) := by
  by_cases hp : p = 2
  · calc
    Fintype.card (center SL(2, F)) = Nat.card (center SL(2,F)) := Fintype.card_eq_nat_card
    _ = 1 := by
      rw [center_SL2_eq_Z, card_Z_eq_one_of_two_eq_zero];
      simp only [hp] at hC
      exact CharTwo.two_eq_zero
    _ < 2 := by norm_num
    _  Nat.card  (center S) := hp  p_le_card_center_S
    _ = Fintype.card (center S) := Nat.card_eq_fintype_card
    _ = Fintype.card ↑↑(Subgroup.map (G.subtype.comp S.toSubgroup.subtype) (center S)) := by
      symm
      apply Set.card_image_of_injective
      rw [MonoidHom.coe_comp]
      apply Injective.comp
      exact subtype_injective G
      exact subtype_injective _
  · let two_ne_zero : NeZero (2 : F) := ne_zero_two_of_char_ne_two F hp
    calc
    Fintype.card (center SL(2, F)) = Nat.card (center SL(2,F)) := Fintype.card_eq_nat_card
    _ = 2 := by rw [center_SL2_eq_Z, card_Z_eq_two_of_two_ne_zero]
    _ < 3 := by norm_num
    _  p := Nat.Prime.three_le_of_ne_two hp'.out hp
    _  Nat.card  (center S) := p_le_card_center_S
    _ = Fintype.card (center S) := Nat.card_eq_fintype_card
    _ = Fintype.card ↑↑(Subgroup.map (G.subtype.comp S.toSubgroup.subtype) (center S)) := by
      symm
      apply Set.card_image_of_injective
      rw [MonoidHom.coe_comp]
      apply Injective.comp
      exact subtype_injective G
      exact subtype_injective _
have coe  :
  Set.ncard ((center SL(2,F)) : Set SL(2,F)) = Fintype.card (center SL(2, F)) := by
    rw [Fintype.card_eq_nat_card]; rfl
have coe  :
  Set.ncard ((Subgroup.map (G.subtype.comp S.toSubgroup.subtype) (center S)) : Set SL(2,F))
    = Fintype.card
        ((Subgroup.map (G.subtype.comp S.toSubgroup.subtype) (center S)) : Set SL(2,F)) := by
          rw [Fintype.card_eq_nat_card]; rfl
have ncard_center_lt_ncard_center_S : Set.ncard ((center SL(2,F)) : Set SL(2,F)) <
  Set.ncard ((Subgroup.map (G.subtype.comp S.toSubgroup.subtype) (center S)) : Set SL(2,F)) := by
      rw [coe , coe ]
      exact card_center_lt_card_center_S
exact Set.exists_mem_not_mem_of_ncard_lt_ncard ncard_center_lt_ncard_center_S
```

To show the Sylowness of the subgroup we shall construct we need the following lemma:

Lemma 6.34. *MaximalAbelianSubgroup.mul*$_c$*enter*$_i$*njLetSandQbesubgroupsofagroup*$\mathrm{SL}_2(F)$ *where* $S \leq Q$ *and furthermore, we have the added condition that either* $I = -I$ *or* $-I \notin S$ *and suppose* $SZ = QZ$ *then* $S = Q$

Proof. SpecialSubgroups.center$_S$*L*2$_e$*q*$_Z$*Weprovethat*Q = S*byantisymmetry*, *butsince*Q $\leq S$ by assumption, we only need show that $S \leq Q$

Let $s \in S$ and $s = s \cdot I \in SZ = QZ$ we can find a $q \in Q$ and $z \in Z$ such

that $s = qz$. By 5.36 we only need split on the case where $z = I$ or $z = -I$. If $z = I$ then we are done $s = q \in Q$.

However, if $z = -1$ since either $I = -I$ or $-I \notin S$ we split in to two cases

- In the first case we can conclude $s = q - I = qI = q \in Q$
- In the second case where $-I \notin S$ we yield a contradiction since $q^{-1}s = -I \in S$ where this last inclusion follows because $q \in Q \leq S$.

□

```
theorem mul_center_inj {F : Type*} [Field F] (S Q : Subgroup SL(2,F))
(Q_le_S : Q  S) (h' : (1 : SL(2,F)) = -1  -1  S)
(hSQ : S.carrier * center SL(2,F) = Q.carrier * center SL(2,F)) : S = Q := by
symm
apply le_antisymm Q_le_S
intro s s_in_S
have key : s * 1  S.carrier * center SL(2,F) := by
  use s, s_in_S, 1, Subgroup.one_mem _
simp [hSQ] at key
obtain  q, q_in_Q, z, z_in_center, hx  := key
simp [center_SL2_eq_Z] at z_in_center
rcases z_in_center with (rfl | rfl)
· simp at hx
  simp [← hx]
  exact q_in_Q
· rcases h' with (one_eq_neg_one | h')
  · rw [one_eq_neg_one] at hx
    simp at hx
    rw [← hx]
    exact q_in_Q
  -- order of every element must divide p^S and 2 does not divide p^S
  · have neg_one_in_S : q ⁻¹ * s  S := by
      refine Subgroup.mul_mem S ?q_inv_in_S s_in_S
      apply Subgroup.inv_mem
      apply Q_le_S q_in_Q
    have : -1 = q ⁻¹ * s := by rw [← hx]; group
    rw [← this] at neg_one_in_S
    contradiction
```

Theorem 6.35. *MaximalAbelianSubgroupsOf, SpecialMatrices.s, SpecialSubgroups.Z MaximalAbelianSubgroup.A$_e$q$_{Q_j}$oin$_{Z_o}$f$_I$sConj$_{s_o}$r$_n$eg$_s$LetFbeanalgebraicallyclosedfieldofcharacteris containing Z, let A be a subgroup of* $\mathrm{SL}_2(F)$ *which is a maximal abelian subgroup of G and furthermore suppose* $Z < A$ *and* $A = C_{\mathrm{SL}_2(F)}(x) \sqcap G$ *where* $x \in G \setminus Z \subseteq \mathrm{SL}_2(F)$ *and x is conjugate to* s_σ *for some* $\sigma \in F$ *then there exists a finite nontrivial elementary abelian Sylow p-subgroup of G such that* $A = Q \sqcup Z$.

Proof. MaximalAbelianSubgroup.centralizer$_e$q$_c$onj$_S$Z$_o$f$_I$sConj$_{s_o}$r$_I$sConj$_n$eg$_s$, *SpecialSubgroups.S$_j$oin$_{Z_e}$q$_S$Z* $C_G(\pm s_\sigma) < C_{\mathrm{SL}_2(F)}(\pm s_\sigma) \quad = S \times Z \cong F \times Z$.

So A is isomorphic to a finite subgroup of $F \times Z$, call it $Q \times Z$. Now $A = Q \times Z \cong QZ$ by Corollary 3.27, which means that an arbitrary element of

A is of the form $q_1 z_1$, where $q_1 \in Q$, $z_1 \in Z$.

$$\begin{aligned} q_1 z_1 q_2 z_2 &= q_2 z_2 q_1 z_1, && (A \in \mathfrak{M}) \\ q_1 q_2 z_1 z_2 &= q_2 q_1 z_1 z_2, && (z_1,\, z_2 \in Z) \\ q_1 q_2 z_1 z_2 (z_1 z_2)^{-1} &= q_2 q_1 z_1 z_2 (z_1 z_2)^{-1}, \\ q_1 q_2 &= q_2 q_1. \end{aligned}$$

Thus Q is also abelian. Recall from the proof of Proposition **??**(ii) that all non-trivial elements of S have order p, so each non-trivial element of Q has order p which means that Q is elementary abelian. Thus Q has order p^m, for some $m \in \mathbb{Z}^+$.

Now let S be a Sylow p-subgroup containing Q. We apply Lemma 6.8 to determine that p divides $|Z(S)|$, moreover $|Z(S)| \geq p$.

If $p = 2$, then $Z = I_L$ by Lemma **??**. So $|Z| = 1$ and hence $|Z(S)| \geq 2 > |Z|$. If $p > 2$, then $Z = \langle -I_L \rangle$ also by Lemma **??**. So $|Z| = 2$ and again we get $|Z(S)| > 2 = |Z|$.

So $Z(S)$ must contain at least one element which is not in Z, let y be one such element. Let $s_1 z_1$ be an arbitrary element of $S \times Z$.

$$\begin{aligned} (s_1 z_1) y (s_1 z_1)^{-1} &= (s_1 z_1) y (z_1^{-1} s_1^{-1}) \\ &= s_1 y (z_1 z_1^{-1}) s_1^{-1} && (\text{since } y \in L,\, z_1 \in Z) \\ &= y (s_1 s_1^{-1}) && (\text{since } s_1 \in S,\, y \in Z(S)) \\ &= y \end{aligned}$$

Thus $s_1 z_1 \in C_G(y)$ and since it was chosen arbitrarily, $S \times Z \subset C_G(y)$. Also since $y \in G \backslash Z$ we have $C_G(y) \in \mathfrak{M}$ by part (i). □

```
theorem A_eq_Q_join_Z_of_IsConj_s_or_neg_s {F : Type*} [Field F]
  [IsAlgClosed F] [DecidableEq F] {p :  } [hp' : Fact (Nat.Prime p)] [hC : CharP F p]
  (G : Subgroup SL(2,F))[hG  : Finite G] (A : Subgroup SL(2,F))
  (hA : A   MaximalAbelianSubgroupsOf G) (center_le_G : center SL(2,F)   G)
  (center_lt_A : center SL(2,F) < A) (x : SL(2,F))
  (x_in_G : x   G.carrier) (x_not_in_center : x   center SL(2,F))
  (A_eq_centra : A = centralizer {x}   G) (  : F)
  (x_IsConj_t_or_neg_t : IsConj (s  ) x  IsConj (- s  ) x) :
   Q : Subgroup SL(2,F),
  Nontrivial Q
  Finite Q
  Q   G
  A = Q   Z F
  IsElementaryAbelian p Q
   S : Sylow p G, Q.subgroupOf G = S := by
  -- centralizer {x} = conj c • TZ F
  obtain  c, c_smul_TZ_eq_centralizer  :=
    centralizer_eq_conj_SZ_of_IsConj_s_or_IsConj_neg_s
      A G   x x_IsConj_t_or_neg_t x_in_G x_not_in_center A_eq_centra.symm
  have A_eq_conj_T_join_Z_meet_G : A = (conj c • (S F   Z F))   G := by
      rw [A_eq_centra, S_join_Z_eq_SZ, c_smul_TZ_eq_centralizer]
  -- from the subgroup equality and conjugacy isomorphisms
  -- we construct the isomorphisms and compose all of them
  -- `A = conj c • (S F   Z F)   G `
  let f  := (MulEquiv.subgroupCongr A_eq_conj_T_join_Z_meet_G)
  -- `(conj c • S F   Z F)   G = ((conj c • (S F   Z F))   G) * A`
  let f  := (MulEquiv.subgroupCongr (conj_S_join_Z_meet_G_eq_conj_S_meet_G_join_Z center_le_G c))
  -- `conj c ⁻¹ • ((conj c • S F   G)   Z F) * conj c • S F   G   Z F`
  let f  := (equivSMul (conj c ⁻¹) (conj c • S F   G   Z F))
  -- `(S F   conj c ⁻¹ • G)   Z F = conj c ⁻¹ • ((conj c • S F   G)   Z F)`
```

```
let f  := MulEquiv.subgroupCongr (conj_inv_conj_eq F G c)
-- Compose all isomorphism together to get the desired isomorphism
let   : A  * ((S F   conj c ¹ • G)   Z F :) := ((f .trans f ).trans f ).trans f
-- the monoid homomorphism composed by the pull back composed with
-- the inclusion of A into SL(2,F)
let f : ((S F   conj c ¹ • G)   Z F :) →* SL(2,F) := A.subtype.comp ( .symm.toMonoidHom)
have f_inj : Injective f := by
  apply Injective.comp (Subtype.val_injective) <| MulEquiv.injective  .symm
-- pull back `S F   conj c ¹ • G ` along the monoid homomorphism
let Q := Subgroup.map f ((S F   conj c ¹ • G :).subgroupOf ((S F   conj c ¹ • G)   Z F :))
-- necessary for proving Q is p-Sylow
have nontrivial_Q : Nontrivial Q := by
  refine (nontrivial_iff_ne_bot Q).mpr ?_
  intro Q_eq_bot
  simp only [Q] at Q_eq_bot
  -- injective map has trivial kernel
  rw [(map_eq_bot_iff_of_injective ((S F   conj c ¹ • G).subgroupOf (S F   conj c ¹ • G   Z F))
       f_inj)] at Q_eq_bot
  have : S F   conj c ¹ • G   S F   conj c ¹ • G   Z F := le_sup_left
  rw [← bot_subgroupOf, subgroupOf_inj, bot_inf_eq, inf_of_le_left this] at Q_eq_bot
  -- if S F   conj c ¹ • G =   then there is an isomorphism from A to Z
  -- the different sizes of the cardinality provide a contradiction
  rw [Q_eq_bot, bot_sup_eq, ← center_SL2_eq_Z] at
  have card_A_le_two : Nat.card A   Nat.card (center SL(2,F)) :=
    le_of_eq (Nat.card_eq_of_bijective   <| MulEquiv.bijective )
  let fin_center : Finite (center SL(2,F)) := by
    rw [center_SL2_eq_Z]
    infer_instance
  let Fintype_center : Fintype (center SL(2,F)) := Fintype.ofFinite  (center SL(2, F))
  let fin_A : Finite A := Set.Finite.subset hG  hA.right
  let Fintype_A : Fintype A := Fintype.ofFinite  A
  have card_center_lt_card_A : Nat.card (center SL(2,F)) < Nat.card A := by
    calc Nat.card (center SL(2,F)) = Fintype.card (center SL(2,F)) := Nat.card_eq_fintype_card
    _ < Fintype.card A := Set.card_lt_card center_lt_A
    _ = Nat.card A := Fintype.card_eq_nat_card
  linarith
have Q_le_G : Q   G := by
  let Q  := ((S F   conj c ¹ • G).subgroupOf (S F   conj c ¹ • G   Z F))
  have h : Subgroup.map  .symm.toMonoidHom Q     := le_top
  have h  :
    Subgroup.map A.subtype (Subgroup.map  .symm.toMonoidHom Q )   Subgroup.map A.subtype   :=
    map_subtype_le_map_subtype.mpr h
  have eq_A : Subgroup.map A.subtype   = A := by ext; simp
  rw [eq_A, Subgroup.map_map] at h
  exact le_trans h  hA.right
have Q_fin : Finite Q := by
  apply Set.Finite.image
  apply Set.Finite.preimage
  · exact Injective.injOn fun  a  a   a   a
  apply Set.Finite.preimage
  · simp [Set.injOn_subtype_val]
  · apply Set.Finite.inf_of_right
    exact Set.Finite.of_surjOn
        ( ((MulDistribMulAction.toMonoidEnd (MulAut SL(2, F)) SL(2, F)) (conj c ¹)))
        (fun  a  a   a) hG
have orderOf_eq_p :   (h :  Q), h   1 → orderOf h = p := by
  rintro  q, t , t _in_subgroupOf, hf  q_ne_one
  obtain   , h  , t _in_conj_G  := t _in_subgroupOf
  have : ((1 : (S F   conj c ¹ • G   Z F :)) : SL(2,F)) = 1 := rfl
  --    0, as otherwise f q = 1 → q = 1; a contradiction
  have  _ne_zero :     0 := by
    intro  _eq_zero
    simp [ _eq_zero] at h
    rw [← this, ← Subtype.ext_iff] at h
    simp [← h ] at hf
    simp [← hf] at q_ne_one
  have orderOf_t _eq_p := @order_s_eq_char F _ p _ _    _ne_zero
  simp [h ] at orderOf_t _eq_p
  -- By injectivity of f the orders must be the same
  have orderOf_q_eq_p : orderOf q = p :=
    hf.symm   orderOf_t _eq_p   orderOf_injective f f_inj t
  rw [← orderOf_q_eq_p]
  exact orderOf_mk q (Exists.intro t   Exists.intro   h  , t _in_conj_G , hf )
have IsElementaryAbelian_Q : IsElementaryAbelian p Q := by
  refine  ?IsCommutative_Q, ?orderOf_eq_p
  case IsCommutative_Q =>
    let CommInst  : IsCommutative (S F   conj c ¹ • G) :=
      inf_IsCommutative_of_IsCommutative_left (S F) (conj c ¹ • G) (IsCommutative_S F)
    let CommInst  : IsCommutative ((S F   conj c ¹ • G).subgroupOf (S F   conj c ¹ • G   Z F)) :=
      subgroupOf_isCommutative _ _
    exact Subgroup.map_isCommutative _ _
    -- Every element is order p
  case orderOf_eq_p => exact orderOf_eq_p
-- We show A is the join of Q and Z
have A_eq_Q_join_Z : A = Q   Z F := by
  have ker_f_eq_bot : f.ker =   := by
    exact (MonoidHom.ker_eq_bot_iff f).mpr f_inj
  have Z_le_A : Z F   A := (le_of_lt ((center_SL2_eq_Z F).symm   center_lt_A))
  have Z_le_range : Z F   f.range := by
    intro z hz
    use ( .toMonoidHom  z, Z_le_A hz )
```

```
    simp [f]
  have map_eq_map_iff := ker_f_eq_bot
    @map_eq_map_iff (S F   conj c ¹ • G   Z F:) _ SL(2,F)
      _ f (Subgroup.comap f (Z F)) ((Z F).subgroupOf (S F   conj c ¹ • G   Z F))
  -- Manually check that every element in Z is preserved under f
  let inst : Nonempty  (S F   (conj c) ¹ • G   Z F) := One.instNonempty
  have key :
    Subgroup.map  .symm.toMonoidHom (((Z F).subgroupOf (S F   conj c ¹ • G   Z F))) =
      (Z F).subgroupOf A := by
    ext z
    -- easier than unpacking all layers of conjugation and isomorphisms
    constructor
    · intro hz
      simp at hz
      obtain  a, ha, a_mem_Z, rfl  := hz
      simp [mem_subgroupOf] at a_mem_Z
      rcases a_mem_Z with (rfl | rfl)
      · left; rfl
      · right
        simp [ , f , f , f , f ]
    · intro hz
      simp [mem_subgroupOf] at hz
      rcases hz with (rfl | h)
      · left; rfl
      · right
        have z_eq_neg_one : z =  -1, Z_le_A <| neg_one_mem_Z  := by
          simp only [← h, Subtype.coe_eta]
        simp [z_eq_neg_one]
        have Z_le_join : Z F   S F   (conj c) ¹ • G   Z F := le_sup_right
        use Z_le_join <| neg_one_mem_Z
        simp [Subtype.ext_iff,  , f , f , f , f ]
  have comap_Z_eq_Z : Subgroup.comap f (Z F) = (Z F).subgroupOf (S F   conj c ¹ • G   Z F) := by
    rw [← sup_bot_eq (Subgroup.comap f (Z F)),
    ← sup_bot_eq ((Z F).subgroupOf (S F   conj c ¹ • G   Z F)),
    ← map_eq_map_iff, map_comap_eq, inf_of_le_right Z_le_range,
    ← Subgroup.map_map, key, subgroupOf_map_subtype, left_eq_inf]
    exact Z_le_A
  have Q_le_range : Q   f.range := by
    exact map_le_range f ((S F   conj c ¹ • G).subgroupOf (S F   conj c ¹ • G   Z F))
  have A_le_range : A   f.range := by
    intro a ha
    use ( .toMonoidHom  a, ha )
    simp [f]
  apply le_antisymm
  · rw [← comap_le_comap_of_le_range A_le_range,
      ← comap_sup_eq_of_le_range f Q_le_range Z_le_range,
      comap_map_eq_self_of_injective f_inj, comap_Z_eq_Z,
      sup_subgroupOf_eq ?h1 ?h2]
    rw [subgroupOf_self]
    exact le_top
    case h1 => exact SemilatticeSup.le_sup_left (S F   conj c ¹ • G) (Z F)
    case h2 => exact SemilatticeSup.le_sup_right (S F   conj c ¹ • G) (Z F)
  · have Q_join_Z_le_range : Q   Z F   f.range := sup_le Q_le_range Z_le_range
    rw [← comap_le_comap_of_le_range Q_join_Z_le_range,
      ← comap_sup_eq_of_le_range f Q_le_range Z_le_range]
    rw [comap_map_eq_self_of_injective f_inj]
    rw [comap_Z_eq_Z, sup_subgroupOf_eq ?h1 ?h2]
    rw [subgroupOf_self]
    case h1 => exact SemilatticeSup.le_sup_left (S F   conj c ¹ • G) (Z F)
    case h2 => exact SemilatticeSup.le_sup_right (S F   conj c ¹ • G) (Z F)
    intro q _hq
    simp [f]
-- Show Q satisfies the desired properties
use Q
refine  ?Q_is_nontrivial, ?Q_is_finite, ?Q_le_G, ?A_eq_Q_join_Z, ?IsElementaryAbelian, ?IsPSylow
case Q_is_nontrivial => exact nontrivial_Q
-- Q is finite as it is the image of a subgroup of a finite group S F   conj c ¹ • G   Z F
case Q_is_finite => exact Q_fin
-- Q   A   G, have to extract data before it is sent through the inclusion
case Q_le_G => exact Q_le_G
-- pushing Q   Z through f ¹ will yield (S F   conj c ¹ • G   Z which is isomorphic to A
case A_eq_Q_join_Z => exact A_eq_Q_join_Z
-- Q is commutative because it is the image of a subgroup of a commutative group
case IsElementaryAbelian => exact IsElementaryAbelian_Q
-- Is p-Sylow
case IsPSylow =>
  -- as Q.subgroupOf G  * Q, Q.subgroupOf G is nontrivial as Q is nontrivial
  have nontrivial_Q_subgroupOf_G: Nontrivial (Q.subgroupOf G) :=
    (subgroupOfEquivOfLe Q_le_G).nontrivial
  -- Q.subgroupOf G is finite as it is the preimage of a finite set on an injective function
  let subgroupOf_fin : Finite (Q.subgroupOf G) := by
    apply Set.Finite.preimage
    · exact Injective.injOn fun  a a  a   a
    exact Set.toFinite (Q.subgroupOf G).carrier
  have IsElementaryAbelian_Q_subgroupOf_G :=
    @subgroupOf SL(2,F) _ Q G p _ IsElementaryAbelian_Q
  have bot_lt_Q_subgroupOf_G :   < Q.subgroupOf G := by
    apply Ne.bot_lt'
    symm
    rw [← nontrivial_iff_ne_bot]
    exact nontrivial_Q_subgroupOf_G
```

```
have IsPGroup_Q_subgroupOf_G:=
  @IsPGroup
    G _ p hp'.out (Q.subgroupOf G) _ IsElementaryAbelian_Q_subgroupOf_G bot_lt_Q_subgroupOf_G
have exists_Sylow := @IsPGroup.exists_le_sylow p G _ (Q.subgroupOf G) IsPGroup_Q_subgroupOf_G
obtain ⟨S, hS⟩ := exists_Sylow
use S
refine le_antisymm ?Q_le_S ?S_le_Q
case Q_le_S =>
  exact hS
case S_le_Q =>
  -- As Q is nontrivial, S must be nontrivial as there is an injection from Q to S
  have nontrivial_S : Nontrivial S := Injective.nontrivial (inclusion_injective hS)
  let nonempty_center_S : Nonempty (center S) := One.instNonempty
  have zero_lt_card_center_S : 0 < Nat.card (center S) := Nat.card_pos
  have p_dvd_card_center_S :=
    @IsPGroup.p_dvd_card_center S p hp'.out _ _ nontrivial_S S.isPGroup'
  have p_le_card_center_S : p ∣ Nat.card (center S) := by
    apply Nat.le_of_dvd zero_lt_card_center_S p_dvd_card_center_S
  -- Given the cardinality of `center S` is greater than cardinality of `center SL(2,F)`,
  -- there must exist an element of center S that does not lie in SL(2,F)
  obtain ⟨y, y_in_center_S, y_not_in_center⟩ :=
    @exists_noncenter_of_card_center_lt_card_center_Sylow F _ p _ _ G _ S p_le_card_center_S
  let inst : CommGroup (center S) := IsCommutative.commGroup (center S)
  have y_commutes_in_S : ∀ w : S, w * y = y * w := by
    intro w
    simp only [mem_map] at y_in_center_S
    obtain ⟨y', y'_in_center, rfl⟩ := y_in_center_S
    have w_eq : (G.subtype.comp S.toSubgroup.subtype) w = ((w : G) : SL(2,F)) := rfl
    -- Pull back w through the inclusion
    rw [← w_eq, ← MonoidHom.map_mul, ← MonoidHom.map_mul]
    congr 1
    rw [mem_center_iff] at y'_in_center
    exact y'_in_center _
  have S_join_Z_le_centra_meet_G :
    ((Subgroup.map G.subtype S.toSubgroup) ⊔ Z F :) ≤ centralizer {y} ⊓ G := by
    intro w hw
    rw [← center_SL2_eq_Z, ← SetLike.mem_coe, mul_normal (N := center SL(2,F))] at hw
    obtain ⟨s', hs, z, z_in_center, rfl⟩ := hw
    simp at hs
    obtain ⟨s'_in_G, s''_in_S⟩ := hs
    simp
    split_ands
    · simp [mem_centralizer_iff]
      -- Coerce the following equality
      have y_commutes_with_s :
        ∀ y * ((⟨s', s'_in_G⟩ : G), (⟨s''_in_S⟩ : S)) =
          ((⟨s', s'_in_G⟩ : G), (⟨s''_in_S⟩ : S)) * y := by
        symm; exact y_commutes_in_S _
      simp at y_commutes_with_s
      simp [mem_center_iff] at z_in_center
      rw [mul_assoc, ← z_in_center y, ← mul_assoc, y_commutes_with_s]
      group
    · exact (Subgroup.mul_mem_cancel_right G (center_le_G z_in_center)).mpr s'_in_G
  have Q_le_range_inclusion_G : Q ≤ G.subtype.range := by simp only [range_subtype, Q_le_G]
  have Q_le_map_S : Q ≤ (Subgroup.map G.subtype S.toSubgroup) := by
    rw [← comap_le_comap_of_le_range Q_le_range_inclusion_G]
    apply le_trans hS
    exact le_comap_map G.subtype ↑S
  -- A = Q ⊔ Z ⊓ S ⊓ Z = centralizer {y} ⊓ G
  -- so by the maximality of A and because S ⊓ Z = centralizer {y} ⊓ G is commutative
  -- Q ⊔ Z = S ⊓ Z and Q ⊓ S which implies Q = S
  have Q_join_Z_le_S_join_Z : Q ⊔ Z F ≤ (Subgroup.map G.subtype S.toSubgroup) ⊔ Z F :=
    sup_le_sup_right Q_le_map_S (Z F)
  have y_in_G : y ∈ G := by
    simp only [mem_map] at y_in_center_S
    obtain ⟨w, w_in_center_S, hw⟩ := y_in_center_S
    simp at hw
    rw [← hw]
    simp only [← SetLike.mem_coe, Subtype.coe_prop]
  have y_in_G_sdif_center_SL : y ∈ G.carrier \ ↑(center SL(2, F)) := by
    split_ands
    · exact y_in_G
    · exact y_not_in_center
  have centra_y_meet_G_in_MaxAbSub :=
    centralizer_meet_G_in_MaximalAbelianSubgroups_of_noncentral G
  have A_le_centra_meet_G : A ≤ centralizer {y} ⊓ G := by
    apply le_trans <| le_of_eq A_eq_Q_join_Z
    apply le_trans Q_join_Z_le_S_join_Z
    exact S_join_Z_le_centra_meet_G
  have A_le_range : A ≤ G.subtype.range := by simp; exact hA.right
  have A_subgroupOf_G_le_centra_meet_G_subgroupOf_G :
    A.subgroupOf G ≤ (centralizer {y} ⊓ G).subgroupOf G := by
    simp only [Subgroup.subgroupOf, comap_le_comap_of_le_range A_le_range]
    exact A_le_centra_meet_G
  have IsCommutative_centra_y_meet_G : IsCommutative ((centralizer {y} ⊓ G)) := by
    apply inf_IsCommutative_of_IsCommutative_left
    apply IsCommutative_centralizer_of_not_mem_center _ y_not_in_center
  -- A subgroup of commutative group is commutative
  have IsCommutative_centra_y_meet_G_subgroupOf_G :
    IsCommutative ((centralizer {y} ⊓ G).subgroupOf G) := by
    exact subgroupOf_isCommutative G (centralizer {y} ⊓ G)
```

```
have centra_meet_G_le_range : centralizer {y}  G  G.subtype.range := by simp
-- By the maximality of A we have that in fact A = centralizer {y}  G
have A_eq_centra_y_meet_G : A = centralizer {y}  G := by
  apply le_antisymm
  · exact A_le_centra_meet_G
  · have centra_meet_G_le_A := @hA.left.right
      ((centralizer {y}  G).subgroupOf G)
        IsCommutative_centra_y_meet_G_subgroupOf_G
          A_subgroupOf_G_le_centra_meet_G_subgroupOf_G
    simp only [← comap_le_comap_of_le_range centra_meet_G_le_range]
    exact centra_meet_G_le_A
-- From this equality we have that Q  Z = S  Z
have Q_join_Z_eq_S_join_Z : Q  Z F = (Subgroup.map G.subtype S.toSubgroup)  Z F := by
  apply le_antisymm
  · exact Q_join_Z_le_S_join_Z
  · rw [← A_eq_Q_join_Z]
    apply le_trans
    exact S_join_Z_le_centra_meet_G
    exact le_of_eq A_eq_centra_y_meet_G.symm
simp only [← center_SL2_eq_Z,
  ← SetLike.coe_set_eq, mul_normal (N := center SL(2,F))] at Q_join_Z_eq_S_join_Z
-- This statement is key to show that from S  Z = Q  Z and S  Q we have that S = Q
have h' : (1 : SL(2,F)) = (-1 : SL(2,F))  -1  (Subgroup.map G.subtype S.toSubgroup) := by
  by_cases hp : p = 2
  -- In char F = 2, -1 = 1
  · left
    apply SpecialLinearGroup.neg_one_eq_one_of_two_eq_zero
    simp only [hp] at hC
    apply CharTwo.two_eq_zero
  -- Order of every element is p but -1 has order 2
  · right
    rw [← ne_eq] at hp
    have ne_zero_two : NeZero (2 : F) := @ne_zero_two_of_char_ne_two F _ p hp' hC hp
    intro neg_one_in_S
    have order_neg_one_eq_two : orderOf (-1 : SL(2,F)) = 2 := orderOf_neg_one_eq_two
    have two_dvd_pow_p :=
      @Subgroup.orderOf_dvd_natCard
        SL(2,F) _ (Subgroup.map G.subtype S.toSubgroup) (-1) neg_one_in_S
    have card_image_eq : Nat.card (Subgroup.map G.subtype S) = Nat.card S.toSubgroup := by
      apply card_map_of_injective <| subtype_injective G
    rw [order_neg_one_eq_two, card_image_eq, Sylow.card_eq_multiplicity] at two_dvd_pow_p
    have two_dvd_p : 2  p := Nat.Prime.dvd_of_dvd_pow Nat.prime_two two_dvd_pow_p
    have two_eq_p : p = 2 :=
      ((Nat.prime_dvd_prime_iff_eq Nat.prime_two hp'.out).mp two_dvd_p).symm
    contradiction
apply le_of_eq
have := @mul_center_inj
  F _ (Subgroup.map G.subtype S) Q Q_le_map_S h' Q_join_Z_eq_S_join_Z.symm
have ker_G_subtype_le_S : G.subtype.ker  S :=
  calc
  G.subtype.ker =  := ker_subtype G
  _  S := by apply bot_le
simp only [Subgroup.subgroupOf, ← this]
rw [comap_map_eq_self ker_G_subtype_le_S]
```

Remark 6.36 (Constructing the elementary abelian p-Sylow subgroup).

Lemma 6.37. *MaximalAbelianSubgroupsOf, SpecialSubgroups.Z MaximalAbelianSubgroup.IsCyclic$_a$nd$_c$ard$_c$opr $\neq Z(G)$ then an element of A of $\mathfrak{M}$, the maximal abelian subgroups of G, is either cyclic group whose order is relatively prime to p, the characteristic of the field F; or of the form $Q \times Z = Q \sqcup Z$ where Q is an elementary abelian Sylow p-subgroup of G.*

Proof. MaximalAbelianSubgroup.center$_n ot_m em, MaximalAbelianSubgroup.eq_c entralizer_m eet_o f_c enter_l t, SL2$ $\notin \mathfrak{M}$, each $A \in \mathfrak{M}$ contains at least one $x \notin Z$. By Proposition 5.48 this x is conjugate to either d_δ or $\pm s_\sigma$ in $\mathrm{SL}_2(F)$. Furthermore, by 6.26 it follows that $A = C_{\mathrm{SL}_2(F)}(x) \sqcap G$.

In view of 5.59, it suffices to only consider these cases:

***x* conjugate to d_δ in** $\mathrm{SL}_2(F)$ then by 6.27 it follows that A is cyclic and its cardinality is coprime to p, the characteristic of the field.

***x* conjugate to $\pm s_\sigma$ in L** then by 6.35 it follows that there exists a subgroup nontrivial finite subgroup Q of $\mathrm{SL}_2(F)$ such that which is an elementary abelian p-Sylow subgroup of G. □

Theorem 6.38. *MaximalAbelianSubgroupsOf MaximalAbelianSubgroup.IsCyclic$_a$nd$_c$ard$_c$oprime$_C$harP$_o$r$_e$q$_{Qj}$o*
$\times Z$ where Q is an elementary abelian Sylow p-subgroup of G.

Proof. MaximalAbelianSubgroup.IsCyclic$_a$nd$_c$ard$_c$oprime$_C$harP$_o$r$_e$q$_{Qj}$oin$_Z$o f$_c$enter$_n$e, $MaximalAbelianSub$
$Nowassume$G $\neq Z$. By 6.37 we yield that A is either a cyclic group whose order is relatively prime to p, or of the form $Q \times Z$ where Q is an elementary abelian Sylow p-subgroup of G. □

Theorem 6.39. *MaximalAbelianSubgroupsOf MaximalAbelianSubgroup.index$_n$ormalizer$_l$e$_t$woIf A*
$\in \mathfrak{M}$ and $|A|$ is relatively prime to p, then we have $[N_G(A) : A] \leq 2$.

Proof. MaximalAbelianSubgroup.IsCyclic$_a$nd$_c$ard$_c$oprime$_C$harP$_o$r$_e$q$_{Qj}$oin$_Z$, normalizer$_s$ubgroup$_{De}$q$_D$W(iv)I
≤ 2 then $A = Z = G$. So A is trivially normal in G and $[N_G(A) : A] = 1$.

Now assume that $|A| > 2$. Since $|A|$ is relatively prime to p, we have that A is a cyclic group conjugate to a finite subgroup of D in $\mathrm{SL}_2(F)$ by the proof of part 6.38, call this subgroup $\widetilde{A}$. Thus both $\widetilde{A}$ and D have orders greater than 2. Applying Proposition 5.54 we observe that

$$N_{\mathrm{SL}_2(F)}(\widetilde{A}) = \langle D, w\rangle = N_{\mathrm{SL}_2(F)}(D). \tag{6.2}$$

Since A and $\widetilde{A}$ are conjugate in $\mathrm{SL}_2(F)$, there exists an element $z \in L$ such that $zAz^{-1} = \widetilde{A}$. This z determines an inner automorphism of $\mathrm{SL}_2(F)$ defined by

$$i_z : L \longrightarrow L, \qquad \text{where} \quad i_z(t) = ztz^{-1} \quad \forall\, t \in L.$$

Let $i_z(G) = \widetilde{G}$ denote the image of G under i_z. Since A is a maximal abelain subgroup of G it's a simple task to show that $\widetilde{A}$ is a maximal abelian subgroup of $\widetilde{G}$ and I will leave this to the reader to verify. We now show that $i_z(N_G(A)) = N_{\widetilde{G}}(\widetilde{A})$. Take an arbitrary $g \in N_G(A)$.

$$\begin{aligned}
(zgz^{-1})\widetilde{A}(zgz^{-1})^{-1} &= zg(z^{-1}\widetilde{A}z)g^{-1}z^{-1} \\
&= z(gAg^{-1})z^{-1} && (\text{since } zAz^{-1} = \widetilde{A}) \\
&= zAz^{-1} && (\text{since } g \in N_G(A)) \\
&= \widetilde{A}.
\end{aligned}$$

So $zgz^{-1} = i_z(g) \in N_{\widetilde{G}}(\widetilde{A})$ and since it was chosen arbitrarily, $i_z(N_G(A)) \subset N_{\widetilde{G}}(\widetilde{A})$. Now take an arbitrary $zhz^{-1} \in N_{\widetilde{G}}(\widetilde{A})$.

$$\begin{aligned}
\widetilde{A} &= (zhz^{-1})\widetilde{A}(zhz^{-1})^{-1} \\
&= zh(z^{-1}\widetilde{A}z)h^{-1}z^{-1} \\
&= zhAh^{-1}z^{-1}. && (\text{since } A = z^{-1}\widetilde{A}z)
\end{aligned}$$

Now multiplication on the left by z^{-1} and right by z gives:

$$A = z^{-1}\widetilde{A}z = hAh^{-1},$$

so $h \in N_G(A)$. Furthermore, zhz^{-1} and indeed the whole of $N_{\widetilde{G}}(\widetilde{A})$ is contained in $i_z(N_G(A))$. Thus $i_z(N_G(A)) = N_{\widetilde{G}}(\widetilde{A})$. In particular, we have,

$$[N_G(A) : A] = [N_{\widetilde{G}}(\widetilde{A}) : \widetilde{A}]. \tag{6.3}$$

Since $\widetilde{G} < L$, the normaliser of $\widetilde{A}$ in $\widetilde{G}$ is simply the normaliser of $\widetilde{A}$ in $\mathrm{SL}_2(F)$ restricted to $\widetilde{G}$, thus $N_{\widetilde{G}}(\widetilde{A}) < N_{\mathrm{SL}_2(F)}(\widetilde{A}) = N_{\mathrm{SL}_2(F)}(D)$ by (6.2). Now since $D \lhd N_{\mathrm{SL}_2(F)}(D)$, the Second Isomorphism Theorem shows that,

$$N_{\widetilde{G}}(\widetilde{A})/(N_{\widetilde{G}}(\widetilde{A}) \cap D) \;\cong\; DN_{\widetilde{G}}(\widetilde{A})/D. \tag{6.4}$$

Clearly $\widetilde{A} \subset \widetilde{G} \cap D$. We show that this inclusion is infact an equality. Assume that there exists some $d_\delta \in \widetilde{G} \cap D$ which is not in $\widetilde{A}$. The group $\langle d_\delta, \widetilde{A}\rangle$ is thus an abelian subgroup of $\widetilde{G}$, strictly larger than $\widetilde{A}$ and contradicting the fact that $\widetilde{A}$ is maximal abelian in $\widetilde{G}$. Thus $\widetilde{A} = \widetilde{G} \cap D$. It is trivial to see that $\widetilde{A} \subset N_{\widetilde{G}}(\widetilde{A}) \cap D$. Also $N_{\widetilde{G}}(\widetilde{A}) \cap D \subset \widetilde{G} \cap D = \widetilde{A}$. So,

$$\widetilde{A} = N_{\widetilde{G}}(\widetilde{A}) \cap D. \tag{6.5}$$

Observe also that,

$$DN_{\widetilde{G}}(\widetilde{A}) = \{D, \langle D, w\rangle\} \subset \langle D, w\rangle = N_{\mathrm{SL}_2(F)}(D). \tag{6.6}$$

Now we piece the preceding results together to give the desired result.

$$\begin{aligned}
N_{\widetilde{G}}(\widetilde{A})/\widetilde{A} \;&\cong\; N_{\widetilde{G}}(\widetilde{A})/(N_{\widetilde{G}}(\widetilde{A}) \cap D) && \text{(by (6.5))}\\
&\cong\; DN_{\widetilde{G}}(\widetilde{A})/D && \text{(by (6.4))}\\
&\subset N_{\mathrm{SL}_2(F)}(D)/D && \text{(by (6.6))}\\
&= \langle D, w\rangle/D \;\cong\; \mathbb{Z}_2.
\end{aligned}$$

We have shown that $N_{\widetilde{G}}(\widetilde{A})/\widetilde{A}$ is isomorphic to a subset of $\mathbb{Z}_2$. Thus by (6.3) we have established that,

$$[N_G(A) : A] = [N_{\widetilde{G}}(\widetilde{A}) : \widetilde{A}] \leq 2.$$

□

Theorem 6.40. *MaximalAbelianSubgroupsOf MaximalAbelianSubgroup.of$_i$ndex$_n$ormalizer$_e$q$_t$woIf A $\in \mathfrak{M}$, $|A|$ is relatively prime to p, and if $[N_G(A) : A] = 2$, then there is an element y of $N_G(A)\backslash A$ such that,*

$$yxy^{-1} = x^{-1} \qquad \forall x \in A.$$

Proof. MaximalAbelianSubgroup.index$_n ormalizer_l e_t wo$

If $[N_G(A) : A] = 2$, then the above argument at 6.39 shows that $N_{\widetilde{G}}(\widetilde{A})/\widetilde{A} \cong \mathbb{Z}_2$. Thus $DN_{\widetilde{G}}(\widetilde{A}) = N_{\mathrm{SL}_2(F)}(D) = \langle D, w\rangle$. This means that $N_{\widetilde{G}}(\widetilde{A})$ contains some element wd_ω. In fact, since $wd_\delta \notin D$, we have $wd_\delta \in N_{\widetilde{G}}(\widetilde{A}) \setminus \widetilde{A}$. Take any element $x \in A$. Since $\widetilde{A} = zAz^{-1}$, $zxz^{-1} \in \widetilde{A}$, call it d_σ. Let $y = z^{-1}wd_\delta z$. Since $wd_\omega \in N_{\widetilde{G}}(\widetilde{A}) \setminus \widetilde{A}$ it follows that $y \in N_G(A) \setminus A$. We show that this y inverts x:

$$\begin{aligned} yxy^{-1} &= (z^{-1}wd_\delta z)(z^{-1}d_\sigma z)(z^{-1}d_\omega^{-1}w^{-1}z) \\ &= z^{-1}wd_\delta d_\sigma d_\omega^{-1}w^{-1}z \\ &= z^{-1}wd_\sigma w^{-1}z \\ &= z^{-1}d_\sigma^{-1}z \qquad \text{(by Lemma ??)} \\ &= x^{-1}. \end{aligned}$$

□

Theorem 6.41. *MaximalAbelianSubgroup.IsCyclic$_a$nd$_c$ard$_c$oprime$_C$har$P_o r_e q_{Q\,j}$oin$_Z$MaximalAbelianSubgro* $\neq \{I_G\}$*, then there is a cyclic subgroup K of G such that $N_G(Q) = Q \sqcup K = QK$.*

Proof. normalizer$_s ubgroup_S l e_L Bypart$6.38,Q$isconjugatetoafinitesubgroupof$S$in\mathrm{SL}_2(F)$. In fact, without loss of generality we can assume that $Q \subset S$, moreoever $Q \subset S \cap G$. We show that this is in fact an equality by showing that the reverse inclusion also holds. Let s_σ be an arbitrary element of $S \cap G$. Then $\langle s_\sigma, Q\rangle$ is a p-group of G which must be equal to Q since it is a Sylow p-subgroup of G. Thus $s_\sigma \in Q$ and

$$Q = S \cap G. \tag{6.7}$$

Since $|Q| > 1$, Proposition 5.52 gives that $N_G(Q) \subset N_{\mathrm{SL}_2(F)}(Q) \subset H$. So $N_G(Q) \subset H \cap G$. Now take an arbitrarily chosen $d_\delta s_\sigma \in H \cap G$ and $s_\gamma \in Q$.

$$\begin{aligned} (d_\delta s_\sigma)s_\gamma(d_\delta s_\sigma)^{-1} &= d_\delta(s_\sigma s_\gamma s_{-\sigma})d_\delta^{-1} \\ &= d_\delta s_\gamma d_\delta^{-1} \qquad \text{(by Lemma ??)} \\ &= t_\sigma. \qquad \text{(where } \sigma = \mu\omega^{-2}\text{, by Lemma ??)} \end{aligned}$$

Since it is a product of elements of G, $s_\sigma \in S \cap G = Q$ by (6.7). Thus $d_\delta s_\sigma \in N_G(Q)$ and indeed the whole of $H \cap G$ is contained in $N_G(Q)$ and

$$N_G(Q) = H \cap G. \tag{6.8}$$

We now define a map ϕ by,

$$\phi : N_G(Q) \longrightarrow D, \qquad \text{where} \quad \phi(d_\delta s_\sigma) = d_\delta \quad \forall\, d_\delta s_\sigma \in N_G(Q).$$

Next we determine the kernel of ϕ.

$$\begin{aligned}\ker(\phi) &= \{d_\delta s_\sigma \in N_G(Q) : \phi(d_\delta s_\sigma) = I_G\} \\ &= N_G(Q) \cap T \\ &= H \cap G \cap T && \text{(by (6.8))} \\ &= T \cap G = Q. && \text{(by (6.7))}\end{aligned}$$

We show that ϕ is a group homomorphism. Take $d_\delta s_\sigma$, $d_\rho s_\gamma$ from $N_G(Q)$.

$$\begin{aligned}\phi(d_\delta s_\sigma d_\rho s_\gamma) &= \phi(d_\delta d_\rho t_\sigma s_\gamma) && \text{(where } \sigma = \lambda\rho^2\text{, by Lemma ??)} \\ &= d_\delta d_\rho \\ &= \phi(d_\delta s_\sigma)\phi(d_\rho s_\gamma).\end{aligned}$$

Thus by the First Isomorphism Theorem,

$$N_G(Q)/Q \cong \phi(N_G(Q)), \tag{6.9}$$

Since $N_G(Q)$ is a finite group, it's image under ϕ is thus a finite subgroup of D. Furthermore, since $D \cong F^*$ (by Lemma **??**), $\phi(N_G(Q))$ is a cyclic group whose order divides $p^m - 1$ and is therefore relatively prime to p, and by (6.9), so too is $N_G(Q)/Q$.

Let r be the order of $N_G(Q)/Q$. Since it is cyclic, $N_G(Q)/Q$ is generated by a single element, namely a coset of Q in $N_G(Q)$, call it kQ. So $|kQ| = r$. Observe that,

$$\begin{aligned}(kQ)^r &= Q, \\ k^r Q &= Q, \\ k^r &\in Q.\end{aligned}$$

Since Q is elementary abelian, each of it's non-trivial elements has order p, so k has order r or rp. In either case, since $\gcd(r, p) = 1$, the order of k^p is r. Let $K = \langle k^p \rangle$. Now $|K| = r$ and

$$\begin{aligned}|N_G(Q)| &= r|Q| \\ &= |K||Q| \\ &= |QK|. && \text{(since } Q \cap K = I_G\text{)}\end{aligned}$$

Thus,

$$N_G(Q) = QK. \tag{6.10}$$

□

Theorem 6.42. *MaximalAbelianSubgroup.IsCyclic$_a$nd$_c$ard$_c$oprime$_C$harP$_o$r$_e$q$_{Qj}$oin$_Z$MaximalAbelianSubgro* $\neq \{I_G\}$*, then there is a cyclic subgroup K of G such that $N_G(Q) = Q \sqcup K = QK$. Furthermore, If $|K| > |Z|$, then $K \in \mathfrak{M}$*

Proof. Assume $|K| > |Z|$. Since K is abelian, it must be contained in some maximal abelian group $A \in \mathfrak{M}$. By part 6.38, A must also be a cyclic group whose order is relatively prime to p.

Since A is conjugate in $\mathrm{SL}_2(F)$ to a subgroup of D, each non-central element of A has exactly 2 fixed points on the projective line L by Proposition 5.64. Let $A = \langle x \rangle$ and let P_1 and P_2 be the points fixed by x. We show by induction on n that x^n also fixes P_1 and P_2, for all $n \in \mathbb{Z}^+$. We do this by assuming first that x^{n-1} fixes P_i.

$$x^n P_i = x(x^{n-1} P_i) = x(P_i) = P_i.$$

The importance of this is that since each element of A can be expressed as some power of x, they must have the same two fixed points, namely P_1 and P_2. In other words,

$$A \subset S_L(P_i), \qquad (i = 1 \text{ or } 2) \tag{6.11}$$

By Proposition 5.64(ii), each element of S has a common fixed point P and $\mathrm{Stab}(P) = H$. Since $K \subset H$, each element in K fixes P. Also, since $K \subset A$, this P must be equal to either P_1 or P_2. Therefore by (6.11), $A \subset \mathrm{Stab}(P) = H$. We arrive at the following result:

$$\begin{aligned} A &\subset H \cap G \\ &= N_G(Q) && \text{(by (6.8))} \\ &= QK. && \text{(by (6.10))} \end{aligned}$$

Furthermore, we get,

$$\begin{aligned} A &= QK \cap A \\ &= QK \cap AK && (K \subset A \text{ so } A = AK) \\ &= (Q \cap A)K \\ &= K && (Q \cap A = I_G) \end{aligned}$$

Thus $K \in \mathfrak{M}$.

□

For the duration of this paper, unless otherwise stated, Q will denote a Sylow p-subgroup of G and K will be as described above.

6.3 Conjugacy of Maximal Abelian Subgroups

Definition 6.43 (Conjugacy class of subgroup)**.** MaximalAbelianSubgroupsOf ConjClassOfSet Let G be a subgroup of $\mathrm{SL}_2(F)$ and let $A \in \mathfrak{M}$ then define the conjugacy class of A to be

$$\mathcal{C}(A) = \{xAx^{-1} : x \in G\}.$$

Definition 6.44 (Noncenter of a subgroup)**.** Subgroup.noncenter Let A be a subgroup of a group G let $A^* = A \setminus Z(G)$ be the "noncenter" part of A.

Now we define the noncenter version of 6.43

Definition 6.45 (Conjugacy class of *noncenter* subgroup)**.** MaximalAbelianSubgroupsOf, Subgroup.noncenter $\text{noncenter}_{C}onjClassOfSetLet\text{G}beasubgroupof\text{SL}_2(F)$ and let $A^* \in \mathfrak{M}^*$ then define the conjugacy class of A^* to be

$$\mathcal{C}(A^*) = \left\{ xA^*x^{-1} \mid x \in G \right\}$$

Definition 6.46. MaximalAbelianSubgroupsOf, Subgroup.noncenter $\text{noncenter}_{M}aximalAbelianSubgroupsOf$ be the set of all A^* where $A \in \mathfrak{M}$.

Definition 6.47. C Let $A \in \mathfrak{M}$ and define the union of the conjugacy classes of A to

$$C(A) = \bigcup_{x \in G} xAx^{-1}$$

Similarly, we define the analogous for the noncenter part of a maximal abelian subgroup:

Definition 6.48 (Cover of conjugacy class of a noncenter part of a subgroup)**.** $\text{noncenter}_{C}Let\text{A}^* \in \mathfrak{M}^*$ then denote union of the conjugacy class of A^* to be the map $C : \mathfrak{M}^* \to \mathcal{P}(\text{SL}_2(F))$ be defined by

$$A^* \mapsto \bigcup_{x \in G} xA^*x^{-1} = \bigcup_{B \in \mathcal{C}(A^*)} B.$$

Then we define the following maps as we will need to prove some properties about them, and eventually we will need to lift them to state and prove the maximal abelian class equation.

Definition 6.49. $\text{card}_{n}oncenterLet\text{A}^* \in \mathfrak{M}^*$ then denote the cardinality the noncenter by the map $|\cdot| : \mathfrak{M}^* \to \mathbb{N}$ which is defined by $A^* \mapsto |A^*|$.

Definition 6.50. $\text{card}_{n}oncenter_{C}onjClassOfSetLet\text{A}^* \in \mathfrak{M}^*$ then denote the cardinality of the conjugacy class of A^* by the map $\varphi_{\mathcal{C}^*} : \mathfrak{M}^* \to \mathbb{N}$ which is defined by $A^* \mapsto |\mathcal{C}(A^*)|$.

In other words, C_i denotes the set of elements of G which belong to some element of $\mathcal{C}_i$. It's evident that $C_i^* = C_i \setminus Z$ and that there is a C_i corresponding to each $\mathcal{C}_i$. Clearly we have the relation,

Lemma 6.51. *$\text{noncenter}_{M}aximalAbelianSubgroupsOf, \text{noncenter}_{C}, \text{card}_{n}oncenter_{C}onjClassOfSet\text{card}_{n}on$ $\mathfrak{M}^*$, noncenter maximal abelian subgroups we have that*

$$|C(A^*)| = |A^*||\mathcal{C}(A^*)|. \tag{6.12}$$

Here the argument from Christopher Butler's exposition has been modified, it turns out to be significantly more idiomatic to Lean to first define the following equivalence relation and its corresponding quotient to eventually set up the maximal abelian class equation.

Lemma 6.52 (Equivalence relation on $\mathfrak{M}^*$)**.** *MaximalAbelianSubgroupsOf lift$_n$oncenter$_M$aximalAbelianSubgr then the relation $\sim$ on the set of noncenter part of maximal abelian subgroups of G, $\mathfrak{M}^*$ defined by*

$$A \sim B \text{ if and only if } \exists x \in G \text{ such that } xAx^{-1} = B$$

is in fact an equivalence relation.

Proof. We show the relation $\sim$ defined above is in fact an equivalence relation on $\mathfrak{M}^*$:

- $\sim$ is reflexive:

  For any $x \in A$ as conjugation by an element in the subgroup defines an automorphism and so $A = xAx^{-1}$ as this automorphism fixes the subgroup.

  Therefore, $A \sim A$ and $\sim$ is thus reflexive.

- $\sim$ is symmetric:

  If $A \sim B$, then $\exists\, x \in G$ such that,

  $$A = xBx^{-1} \iff x^{-1}Ax = B \iff B = yAy^{-1} \quad \text{for } y = x^{-1} \in G.$$

  Thus $B \sim A$ and $\sim$ is symmetric.

- $\sim$ is transitive:

  If $A \sim B$ and $B \sim C$, then $\exists\, x, y \in G$ such that,

  $$A = xBx^{-1} \text{ and } B = yCy^{-1} \Rightarrow A = xyCy^{-1}x^{-1} = (xy)C(xy)^{-1}.$$

  Thus $A \sim C$ (since $xy \in G$), which shows that $\sim$ is transitive.

Therefore, we have shown that $\sim$ relation is in fact an equivalence relation on $\mathfrak{M}$ □

Remark 6.53 (Setoid typeclass in Lean). A setoid is a type with a distinguished equivalence relation, that is to say, if one wants to attach the `Setoid` typeclass to a type, and so say define the corresponding `Quotient` type which allows one to clump together objects which are equivalent, one has to:

1. Define the binary relation `r`.

2. Prove the binary relation is an equivalence relation, that is a provide a proof term for the field `iseqv` which in itself requires proof terms for the fields corresponding to reflexivity, symmetry and transitivity; `refl`, `symm` and `trans`.

Now that we have set up the equivalence relation on maximal abelian subgroups we proceed to lift particular functions that will be of interest to set up the maximal abelian class equation and other suitable results.

Lemma 6.54. *Subgroup.noncenter, lift$_n$oncenter$_M$aximalAbelianSubgroupsOfcard$_n$oncenter$_e$q$_o$f$_r$elatedLet*
$\mathfrak{M}$ *and suppose* $A^* \sim B^*$ *then* $|A^*| = |B^*|$

Proof. Let G be a finite subgroup of $\mathrm{SL}_2(F)$, recall that if $A^* \sim B^*$ then there exists a $x \in G$ such that $xAx^{-1} = B^*$. Since conjugation by an element $x \in G$ of group defines an automorphism, $\phi_x : \mathrm{SL}_2(F) \to \mathrm{SL}_2(F)$. In particular, an automorphism is injective; therefore the cardinality of the image of a finite set

$$|A^*| = |\phi_x(A^*)| = |B^*|$$

□

We are now ready to lift the function which computes the cardinality of a noncenter maximal abelian subgroup

Definition 6.55. lift$_n$oncenter$_M$aximalAbelianSubgroupsOflift$_c$ard$_n$oncenterGivenforallA$^* \sim$ $B^* \in \mathfrak{M}^*$ we have that $|A^*| = |B^*|$ by 6.54 we can define the lift $|\cdot| : \mathfrak{M}^*/\sim$ $\to \mathbb{N}$ which is given by $[A^*] \mapsto |A^*|$.

Similarly, we now proceed to show that the map which sends a noncenter maximal abelian subgroup to the cover generated by its conjugacy class is respected by the equivalence relation $\sim$ on $\mathfrak{M}^*$

Lemma 6.56 (Equivalent noncenter subgroups of $\mathfrak{M}^*$ have the equal union of their conjugacy class)**.** *noncenter$_C$, noncenter$_M$aximalAbelianSubgroupsOfnoncenter$_C$e q$_o$f$_r$elatedLetGbeasu*
and let $A^*, B^* \in \mathfrak{M}*$ *be a noncenter maximal abelian subgroups of* G *where* $A^* \sim B^*$ *then*

$$\bigcup_{x \in G} xA^*x^{-1} = \bigcup_{x \in G} xB^*x^{-1}$$

Definition 6.57 (Lift of the union of the conjugacy class of noncenter of a subgroup)**.** noncenter$_C$, *noncenter$_C$e q$_o$f$_r$elated, noncenter$_M$aximalAbelianSubgroupsOf, lift$_n$oncenter$_M$aximal* $B^* \in \mathfrak{M}^*$ we have that $C(A^*) = C(B^*)$ by 6.56 we can define the lift of $C : \mathfrak{M}^* \to \mathcal{P}(\mathrm{SL}_2(F))$ to be $\tilde{C}([A^*]) = \bigcup_{x \in G} xA^*x^{-1}$ where this map is well-defined for any choice of a representative of $[A^*]$.

Theorem 6.58 (The union of conjugacy classes of the set representatives of $\mathfrak{M}^*/\sim$ cover $G \backslash Z(\mathrm{SL}_2(F))$)**.** *lift$_n$oncenter$_M$aximalAbelianSubgroupsOf, lift$_n$oncenter$_C$unionlift$_n$oncenter$_C$*
provided $\mathfrak{M}^*/\sim$ *is a finite then we have the set equality*

$$G \setminus Z(\mathrm{SL}_2(F)) = \bigcup_{[A^*] \in \mathfrak{M}^*/\sim} C([A^*])$$

Theorem 6.59 (Distinct elements of $\mathfrak{M}^*/\sim$ are mapped to disjoint sets through $\tilde{C}$)**.** *$lift_noncenter_MaximalAbelianSubgroupsOf, lift_noncenter_Cdisjoint_of_nelift_noncenter_MaximalA$ $\mathfrak{M}^*/\sim$ then*

$$\tilde{C}([A^*]) = \tilde{C}([B^*]) \iff [A^*] = [B^*]$$

Or equivalently,

$$C(A^*) \cap C(B^*) = \varnothing, \qquad \forall\ A^* \not\sim B^*$$

Theorem 6.60. *MaximalAbelianSubgroupsOf, noncenter_MaximalAbelianSubgroupsOf, noncenter_ConjClass* $\in \mathfrak{M}$ *we have that*

$$|\mathcal{C}(A)| = |\mathcal{C}(A^*)|$$

Theorem 6.61. *MaximalAbelianSubgroupsOf, ConjClassOfSet card_ConjClassOfSet_eq_index_normalizer*

Let G be a finite subgroup of $\mathrm{SL}_2(F)$ and let A be a maximal abelian subgroup of G, $A \in \mathfrak{M}$ then $|\mathcal{C}(A)| = [G : N_G(A)]$.

Theorem 6.62 (The maximal subgroup class equation)**.** *$lift_noncenter_MaximalAbelianSubgroupsOf, lift_card_$*

Let G be a finite subgroup of $\mathrm{SL}_2(F)$, define the equivalence relation on the maximal abelian subgroups of G, $\mathfrak{M}^*$ as above in 6.52 then $|G \setminus Z| = \sum_{[A^*]\in\mathfrak{M}^*/\sim} |A^*|[\tilde{C}([A^*])]$.

Proof. (i)
The equivalence class of A^* in $\mathfrak{M}^*$ therefore coincides with the set $\mathcal{C}_i^* = \{xA^*x^{-1} : x \in G\}$. Furthermore, this tells us that each A^* belongs to exactly one conjugacy class. Thus the conjugacy classes $\mathcal{C}_i^*$ form a partition of $\mathfrak{M}^*$,

$$\mathfrak{M}^* = \bigcup_{A^*\in S} \mathcal{C}_i^*, \qquad \text{and} \qquad \mathcal{C}_i^* \cap \mathcal{C}_j^* = \varnothing, \qquad \forall\ i \neq j.$$

Since the set of $\mathcal{C}_i^*$ are pairwise disjoint, it follows that the set of C_i^* are also pairwise disjoint and we get the desired result,

$$G\setminus Z = \bigcup_{A^*\in S} C_i^*, \qquad \text{and} \qquad C_i^* \cap C_j^* = \varnothing, \qquad \forall\ i \neq j.$$

(ii) Let $xAx^{-1} \in \mathcal{C}_i$ and $xA^*x^{-1} \in \mathcal{C}_i^*$. Since $xAx^{-1} \setminus Z = xA^*x^{-1}$, it is quite clear that,

$$xAx^{-1} \in \mathcal{C}_i \iff xA^*x^{-1} \in \mathcal{C}_i^*.$$

Thus $|\mathcal{C}_i^*| = |\mathcal{C}_i|$ as desired.

(iii) Now we define a map ϕ by:

$$\begin{aligned} \phi : \mathcal{C}_i &\longrightarrow G/N_G(A), \\ \phi(xAx^{-1}) &= xN_G(A). \qquad (\forall\ x \in G,\ A \in \mathfrak{M}) \end{aligned}$$

Clearly ϕ is trivially surjective. We now show that it is both well-defined and injective.

$$\begin{aligned} xN_G(A) = yN_G(A) &\iff y^{-1}xN_G(A) = N_G(A) \\ &\iff y^{-1}x \in N_G(A) \\ &\iff (y^{-1}x)A(y^{-1}x)^{-1} = A \\ &\iff y^{-1}xAx^{-1}y = A \\ &\iff xAx^{-1} = yAy^{-1}. \end{aligned}$$

Hence ϕ is well-defined and injective. This shows that ϕ is a bijection proving that $|\mathcal{C}_i| = [G : N_G(A)]$. This is a crucial result which shows that the number of maximal abelian subgroups conjugate to A is equal to the index of the normaliser of A in G.

(iv) This follows directly from parts (i), (ii) and (iii) and (6.51).

$$\begin{aligned} G\backslash Z &= \bigcup_{A^* \in S} C_i^*, \qquad \text{and} \qquad C_i^* \cap C_j^* = \varnothing, \qquad \forall\, i \neq j, \\ |G\backslash Z| &= \sum_{A^* \in S} |C_i^*| = \sum_{A^* \in S} |A^*||\mathcal{C}_i^*| = \sum_{A^* \in S} |A^*||\mathcal{C}_i| \\ &= \sum_{A^* \in S} |A^*|[G : N_G(A)]. \end{aligned}$$

□

This theorem proves that the non-central parts of the maximal abelian subgroups form a partition of the non-central part of G. This will serve as a powerful tool in decomposing G and counting its elements.

6.4 Constructing The Class Equation

It is necessary to prove the following 2 short lemmas before we proceed further.

Lemma 6.63. *$normalizer_noncentral_eqThenormalizersN_G(A) = N_G(A^*)$.*

Proof. Let $x \in N_G(A^*)$. Take an arbitary $a \in A = A^* \cup Z$. If $a \in A^*$, then since $x \in N_G(A^*)$, we have $xax^{-1} \in A^* \subset A$. If $a \in Z$, then $xzx^{-1} = zxx^{-1} = z \in A$. Therefore x is in the normaliser of A and $N_G(A^*) \subset N_G(A)$.

Conversely, take $y \in N_G(A)$ and $a \in A^*$. $yay^{-1} \in A = A^* \cup Z$. If $yay^{-1} \in Z$, then

$$\begin{aligned} yay^{-1} &= z, && \text{(some } z \in Z\text{)} \\ a &= y^{-1}zy = y^{-1}yz = z \notin A^*. \end{aligned}$$

This contradicts the fact that $a \in A^*$. Therefore $yay^{-1} \in A^*$ and $y \in N_G(A^*)$. Since y was chosen arbitrarily we get $N_G(A) \subset N_G(A^*)$ and hence $N_G(A) = N_G(A^*)$.

□

Lemma 6.64. *MaximalAbelianSubgroup.IsCyclic*$_a$*nd*$_c$*ard*$_c$*oprime*$_C$*harP*$_o$*r*$_e$*q*$_Q$*j*$oin_Z normalizer_S ylow_j oin_c ente$ $Z) = N_G(Q)$.

Proof. MaximalAbelianSubgroup.index$_n$*ormalizer*$_l$*e*$_t$*wo*

If $p = 2$ then $Z = I_G$ and the result is trivial. Now assume $p \neq 2$. Thus $|Z| = 2$. Let x and q_1 be arbitrarily chosen elements of $N_G(Q)$ and Q respectively.

$$\begin{aligned} xq_1x^{-1} &= q_2, && \text{(for some } q_2 \in Q) \\ xq_1x^{-1}z_1 &= q_2z_1, \\ xq_1z_1x^{-1} &= q_2z_1 \in Q \times Z. \end{aligned}$$

Thus any element x which is in $N_G(Q)$ is also in $N_G(Q \times Z)$ so we have $N_G(Q) \subset N_G(Q \times Z)$.

Let q_1z_1 be an arbitrarily chosen element of $Q \times Z$ such that $q_1 \in Q$ and $z_1 \in Z$. Now let y be an arbitrarily chosen element of $N_G(Q \times Z)$.

$$yq_1z_1y^{-1} = q_2z_2 \in Q \times Z. \qquad \text{(where } q_2 \in Q \text{ and } z_2 \in Z)$$

Consider now the order of q_1z_1 in G. Since $p \neq 2$, $Q \cap Z = I_G$ and $|q_1z_1| = |q_1||z_1|$. Note that q_1z_1 and q_2z_2 are conjugate in G, and thus their orders are equal. This means that $|z_1| = |z_2|$, because otherwise 2 would divide one of them and not the other. Thus $z_1 = z_2$ and,

$$\begin{aligned} yq_1z_1y^{-1} &= q_2z_2 = q_2z_1 \\ yq_1y^{-1}z_1 &= q_2z_1, \\ yq_1y^{-1} &= q_2 \in Q \end{aligned}$$

Hence $y \in N_G(Q)$. Furthermore, since y was chosen arbitrarily, any element which is in $N_G(Q \times Z)$ is also in $N_G(Q)$, so $N_G(Q \times Z) = N_G(Q)$ as desired.

□

We now start to count the elements of the seperate components of G and use the preceeding 2 theorems to construct what will be an invaluable formula in determining the structure of G, something we will call the **Maximal Abelian Subgroup Class Equation** of G.

First we split $\mathfrak{M}$ into the conjugacy classes of it's elements. Theorem 6.38 tells us that every maximal abelian subgroup is either a cyclic subgroup whose order is relatively prime to p or of the form $Q \times Z$ where Q is a Sylow p-subgroup. Let $\mathcal{C}_1, \mathcal{C}_2, ..., \mathcal{C}_s, \mathcal{C}_{s+1}, ..., \mathcal{C}_{s+t}$ (where $s, t \in \mathbb{Z}^+$) denote the conjugacy classes of the cyclic subgroups whose order is relatively prime to p. Recall that part (iv)

of Theorem 6.39 tells us that $[N_G(A) : A] = 1$ or 2. Let A be a representative from each $\mathcal{C}_i$ such that,

$$[N_G(A) : A] = 1, \qquad \text{(for } i \leq s\text{)}$$

$$[N_G(A) : A] = 2., \qquad \text{(for } s < i \leq s + t\text{)}$$

Now let Q_1 and Q_2 be any two Sylow p-subgroups of G. By the Second Sylow Theorem, Q_1 and Q_2 are conjugate to each other in G. That is, there exists a $g \in G$ such that $gQ_1g^{-1} = Q_2$.

$$\begin{aligned} gQ_1g^{-1} = Q_2 &\iff gQ_1g^{-1}Z = Q_2Z \\ &\iff gQ_1Zg^{-1} = Q_2Z \\ &\iff g(Q_1 \times Z)g^{-1} = (Q_2 \times Z). \qquad \text{(by Corollary 3.27)} \end{aligned}$$

So $Q_1 \times Z$ and $Q_2 \times Z$ belong to the same conjugacy class, furthermore there is thus only 1 conjugacy class of elements of this form in $\mathfrak{M}$. Let $\mathcal{C}_{Q\times Z}$ denote this conjugacy class and let $Q \times Z$ be a representative from it. The following diagram provides a visual representation of G divided into it's maximal abelian subgroups.

We can reformulate the counting formula in Theorem 6.62 using the notation we have introduced to show that it agrees with the intuitive approach that Fig 1 suggests.

$$|G\backslash Z| = \sum_{[A^*]\in S} |A^*|[G : N_G(A)] = \sum_{A^*\in S} |C_i^*| = |C_{Q\times Z}^*| + \sum_{i=1}^{s+t} |C_i^*|.$$

We are now able to begin to evaluate G. Firstly, let $|Z| = e$ and $|G| = eg$. We know well by now that $e = 1$ or 2 depending on whether p equals 2 or not, and by Lagrange's Theorem, the order of a subgroup divides the order of the group, so e divides $|G|$ since $Z < G$.

We consider the cyclic case first. Again, by Lagrange's Theorem, since Z is a subgroup of each A, e divides $|A|$. So set $|A| = eg_i$. Since $Z \notin \mathfrak{M}$, each A is therefore strictly larger than Z and so each g_i is an integer greater than or equal to 2.

To determine the order of each C_i, we return to the set $\mathfrak{M}^*$. The size of one representative of each class is,

$$|A^*| = |A\backslash Z| = eg_i - e = e(g_i - 1).$$

The number of A^* in each conjugacy class $\mathcal{C}_i$ for $i \leq s$ is thus,

$$|\mathcal{C}_i^*| = |\mathcal{C}_i| = [G : N_G(A)] = \frac{|G|}{|A|} = \frac{eg}{eg_i} = \frac{g}{g_i}.$$

Therefore the total number of elements of G in the noncentral part of C_i for $i \leq s$ is,

$$\sum_{i=1}^{s} |C_i^*| = \sum_{i=1}^{s} |A^*||\mathcal{C}_i^*| = \sum_{i=1}^{s} \frac{eg(g_i - 1)}{g_i}. \tag{6.13}$$

The number of A^* in each conjugacy class $\mathcal{C}_i$ for $s < i \leq s + t$ is thus,

$$|\mathcal{C}_i^*| = |\mathcal{C}_i| = [G : N_G(A)] = \frac{|G|}{2|A|} = \frac{eg}{2eg_i} = \frac{g}{2g_i}.$$

Therefore the total number of elements of G in the noncentral part of C_i for $s < i \leq s + t$ is,

$$\sum_{i=s+1}^{s+t} |C_i^*| = \sum_{i=s+1}^{s+t} |A^*||\mathcal{C}_i^*| = \sum_{i=s+1}^{s+t} \frac{eg(g_i - 1)}{2g_i}. \tag{6.14}$$

We next determine the order of $C_{Q\times Z}$. Let $|Q| = q$. If $p \nmid |G|$ then $q = 1$ and if $p = 0$, then we consider a Sylow p-subgroup to simply be I_G. So q is always at least 1. Since $Z < K$, we can let $|K| = ek$. Observe that if $K \in \mathfrak{M}$, then by Theorem 6.42, $K = A$ for some $0 < i \leq t$ and $k = g_i$. Recall that $N_G(Q) = QK$ and so,

$$\begin{aligned} |N_G(Q \times Z)^*| &= |N_G(Q \times Z)| && \text{(by Lemma 6.63)} \\ &= |N_G(Q)| && \text{(by Lemma ??)} \\ &= |QK| = eqk. \end{aligned}$$

Again we count the size and number of these maximal abelian groups.

$$|(Q \times Z)^*| = |QZ| - |Z| = e(q - 1).$$

Since there is only one conjugacy class of $Q \times Z$, the number of $(Q \times Z)^*$ in $\mathfrak{M}^*$ is thus,

$$|\mathcal{C}_{Q\times Z}^*| = |\mathcal{C}_{Q\times Z}| = [G : N_G(Q \times Z)] = \frac{|G|}{|N_G(Q \times Z)^*|} = \frac{eg}{eqk} = \frac{g}{qk}.$$

Therefore the total number of elements of G in the noncentral parts of each $Q \times Z$ is,

$$|C_{Q\times Z}^*| = |(Q \times Z)^*||\mathcal{C}_{Q\times Z}^*| = \frac{eg(q - 1)}{qk}. \tag{6.15}$$

We now sum together (6.13), (6.14) and (6.15) to create the **Maximal Abelian Subgroup Class Equation** of G.

$$|G\backslash Z| = |C^*_{Q\times Z}| + \sum_{i=1}^{s+t} |C^*_i|,$$

$$|G\backslash Z| = |(Q\times Z)^*||\mathcal{C}^*_{Q\times Z}| + \sum_{i=1}^{s} |A^*||\mathcal{C}^*_i| + \sum_{i=s+1}^{s+t} |A^*||\mathcal{C}^*_i|,$$

$$eg - e = \frac{eg(q-1)}{qk} + \sum_{i=1}^{s} \frac{eg(g_i-1)}{g_i} + \sum_{i=s+1}^{s+t} \frac{eg(g_i-1)}{2g_i},$$

$$1 = \frac{1}{g} + \frac{q-1}{qk} + \sum_{i=1}^{s} \frac{g_i-1}{g_i} + \sum_{i=s+1}^{s+t} \frac{g_i-1}{2g_i}. \tag{6.16}$$

Since $g, k, q \in \mathbb{Z}^+$ this implies that,

$$\frac{1}{g} > 0 \quad \text{and} \quad \frac{q-1}{qk} \geq 0.$$

Also, since $g_i \geq 2$ for $1 \leq i \leq s+t$, we have,

$$\frac{g_i-1}{g_i} \geq \frac{1}{2}, \quad \sum_{i=1}^{s} \frac{g_i-1}{g_i} \geq \frac{s}{2} \quad \text{and} \quad \sum_{i=s+1}^{s+t} \frac{g_i-1}{2g_i} \geq \frac{t}{4}.$$

Thus we can find a lower bound for (6.16) which limits the possible number of conjugacy classes somewhat,

$$1 > \frac{s}{2} + \frac{t}{4}.$$

There are only 6 possible different pairs of values which s and t can take:

Case	I	II	III	IV	V	VI
s	1	1	0	0	0	0
t	0	1	0	1	2	3

Each case will be examined individually in the next chapter.

Chapter 7

Dickson's Classification Theorem for finite subgroups of $\mathrm{SL}_2(F)$

7.1 Five Lemmas

Before we detemine the structure of G in each of the 6 cases, it is necessary to prove a number of lemmas which will be used.

Lemma 7.1. *IsPGroup.notIenormalizerLetHbeapropersubgroupofap−groupG.ThenH* $\subsetneq N_G(H)$.

Proof. Let S denote the set of left cosets of H in G. That is,

$$S = \{xH : x \in G\}, \quad \text{and} \quad |S| = [G : H] = p^k. \quad (\text{for some } k \geq 1)$$

Consider the action of H on S by left multiplication. We calculate the stabiliser of $xH \in S$ in H.

$$\begin{aligned} \mathrm{Stab}(xH) &= \{y \in H : yxH = xH\} \\ &= \{y \in H : x^{-1}yx \in H\}. \end{aligned}$$

If $x \in H$ then $x^{-1}yx \in H$ for all $y \in H$. Thus the $\mathrm{Stab}(xH) = H$ and by the Orbit-Stabiliser Theorem,

$$|\mathrm{Orb}(xH)| = [H : \mathrm{Stab}(xH)] = 1.$$

Observe that,

$$S = \bigcup_{xH \in S} \mathrm{Orb}(xH),$$

where the orbits are pairwise disjoint. Now since p divides $|S|$, p divides the sum of all the orbit sizes. Furthermore, since each orbit size is 1 or a multiple of p, there must be at least p elements of S which have an orbit of 1. In particular, there exists an $x_1H \in S$ which has an orbit of 1 and $x_1 \notin H$. That is,

$$\begin{aligned} yx_1H &= x_1H, && (\forall y \in H) \\ x_1^{-1}yx_1 &\in H, \\ x_1^{-1}Hx_1 &\subset H, \\ x_1 &\in N_G(H)\backslash H. \square \end{aligned}$$

Lemma 7.2. *MaximalAbelianSubgroupsOf Sylow.not$_n$ormal$_s$ubgroup$_o$f$_G$Let Qbea Sylowp−subgroupandKama*
QK and $Q \cap K = \{I_G\}$. If $[N_G(K) : K] = 2$, then Q is not a normal subgroup of G.

Proof. The approach here is proof by contradiction, so we begin by assuming that $Q \lhd G$. Thus $N_G(Q) = G$ and $N_G(K) \subset N_G(Q)$. Consider the natural homomorphism of $N_G(Q)$ onto $N_G(Q)/Q$,

$$\begin{aligned} \phi : N_G(Q) &\longrightarrow N_G(Q)/Q, \\ \phi(x) &= xQ, \\ ker(\phi) &= \{x \in N_G(Q) : \phi(x) = I_GQ\} = Q. \end{aligned}$$

Let ϕ' be the restiction of ϕ to $N_G(K)$:

$$\phi' = \phi|_{N_G(K)} : N_G(K) \longrightarrow N_G(Q)/Q.$$

Thus $ker(\phi') = ker(\phi) \cap N_G(K) = Q \cap N_G(K)$. By the 1st Isomorphism Theorem,

$$\begin{aligned} \mathrm{Im}(\phi') &\cong N_G(K)/ker(\phi'), \\ N_G(Q)/Q &\cong N_G(K)/(Q \cap N_G(K)), \\ K &\cong N_G(K)/(Q \cap N_G(K)), && (N_G(Q) = QK) \\ |Q \cap N_G(K)| &= [N_G(K) : K] = 2. && (\text{by assumption}) \end{aligned}$$

So 2 divides $|Q|$, which implies that $2 \nmid |K|$ since $Q \cap K = \{I_G\}$. Moreover, $|Q \cap N_G(K)|$ and $|K|$ are relatively prime.

Take $a \in ker(\phi') = Q \cap N_G(K)$ and $b \in N_G(K)$.

$$\begin{aligned} \phi'(bab^{-1}) &= \phi'(b)\phi'(a)\phi'(b^{-1}) \\ &= \phi'(b)(I_GQ)\phi'(b^{-1}) \\ &= \phi'(b)\phi'(b^{-1})(I_GQ) = I_GQ. \end{aligned}$$

Thus $bab^{-1} \in ker(\phi') = Q \cap N_G(K)$ and so $Q \cap N_G(K) \lhd N_G(K)$.

Now let $x \in Q \cap N_G(K)$ and $y \in K$. Notice that both x and y are elements of $N_G(K)$,

$$\begin{aligned} xyx^{-1}y^{-1} &= (xyx^{-1})y^{-1} \in K, && \text{(since } K \lhd N_G(K)\text{)} \\ xyx^{-1}y^{-1} &= x(yx^{-1}y^{-1}) \in Q \cap N_G(K), && \text{(since } Q \cap N_G(K) \lhd N_G(K)\text{)} \\ xyx^{-1}y^{-1} &\in K \cap (Q \cap N_G(K)) \\ &= I_G, && \text{(since } \gcd(|Q \cap N_G(K)|, |K|) = 1\text{)} \\ xy &= yx. \end{aligned}$$

Therefore $(Q \cap N_G(K)) \times K$ is an abelian subgroup of which K is a proper subgroup. This contradicts the fact that K is a maximal abelian subgroup, thus Q is not a normal subgroup of G.

□

Lemma 7.3. *Let p be the prime characteristic of F and let $q = p^k$ for some $k > 0$. Set,*

$$R = \{\lambda \in F : \lambda^q - \lambda = 0\}. \tag{7.1}$$

Then R is a subfield of F.

Proof. Since R is a subset of F it suffices to show that the following 3 criteria are met:

(i) $0, 1 \in R$.
(ii) If $\lambda_1, \lambda_2 \in R$, then $\lambda_1 - \lambda_2 \in R$.
(iii) If $\lambda_1, \lambda_2 \in R$ and $\lambda_1 \neq 0 \neq \lambda_2$, then $\lambda_1\lambda_2^{-1} \in R$.

We see immediately that (i) is satified. Since p is the characteristic of F, any coeffiecients which are a multiple of p vanish. We get,

$$(\lambda_1 - \lambda_2)^q = (\lambda_1^p - \lambda_2^p)^{p^{k-1}} = ... = \lambda_1^q - \lambda_2^q = \lambda_1 - \lambda_2.$$

Thus $\lambda_1 - \lambda_2 \in R$ and (ii) is also satisifed. Finally observe that if λ_2 is a non-zero element of R, then $\lambda_2^{-1} = \lambda_2^{-q}$ and,

$$(\lambda_1\lambda_2^{-1})^q = \lambda_1^q\lambda_2^{-q} = \lambda_1\lambda_2^{-1}.$$

So $\lambda_1\lambda_2^{-1} \in R$ and R is a subfield of F.

□

Each finite field is uniquely determined up to isomorphism by the number of elements it contains [**?**, p.227]. Since the R defined in (7.1) has q elements, from now on when we use the notation $\mathbb{F}_q$ to denote a field of q elements, we shall actually mean,

$$\mathbb{F}_q = R \subset F. \tag{7.2}$$

Lemma 7.4. *Let $\mathbb{F}_q$ be the field of q elements, where q is the power of a prime. The order of $GL(2, \mathbb{F}_q)$ is $(q^2 - 1)(q^2 - q)$.*

Proof. In order to prove this, we again take a geometric viewpoint. Recall that $GL(2, \mathbb{F}_q)$ is the group of 2 x 2 invertible matrices over $\mathbb{F}_q$ under ordinary matrix multiplication. The order of $GL(2, \mathbb{F}_q)$ is thus equal to the number of ordered pairs $\{u, v\}$ of linearly independent vectors in a 2-dimensional vector space over $\mathbb{F}_q$.

There are clearly q^2 different vectors in the 2-dimensional vector space over $\mathbb{F}_q$. The only restriction on the first vector u, is that it must be non-zero, so there are $(q^2 - 1)$ choices for u. To ensure the second vector v is linearly independent of u, it must not be of the form αu, where $\alpha \in \mathbb{F}_q$. Since there are q choices for α, there are $(q^2 - q)$ choices for v.

Thus the order of $GL(2, \mathbb{F}_q)$ is the product of the number of choices of u and the number of choices of v, that is, $(q^2 - 1)(q^2 - q)$ as required. □

Lemma 7.5. *$card_S L_f ield The order of the group \mathrm{SL}_2(\mathbb{F}_q)$ is $q(q^2 - 1)$.*

Proof. Consider the map ϕ defined as,

$$\phi : GL(2, \mathbb{F}_q) \longrightarrow \mathbb{F}_q^*, \qquad \text{where } \ \phi(x) = \det(x), \quad \forall\, x \in GL(2, \mathbb{F}_q).$$

Next we determine the kernel of ϕ.

$$ker(\phi) = \{GL(2, \mathbb{F}_q) : \det(x) = 1\} = \mathrm{SL}_2(\mathbb{F}_q).$$

We show that ϕ is a group homomorphism. Take $x, y \in GL(2, \mathbb{F}_q)$,

$$\phi(xy) = \det(xy) = \det(x)\det(y) = \phi(x)\phi(y).$$

Clearly ϕ is surjective, since $\alpha \in \mathbb{F}_q^*$ is the determinant of $\begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix} \in GL(2, \mathbb{F}_q)$. Therefore because $\mathrm{SL}_2(F) \lhd \mathrm{GL}_2(F)$, by the First Isomorphism Theorem,

$$GL(2, \mathbb{F}_q)/\,\mathrm{SL}_2(\mathbb{F}_q) \cong \mathbb{F}_q^*.$$

Thus,

$$|\,\mathrm{SL}_2(\mathbb{F}_q)| = \frac{|GL(2, \mathbb{F}_q)|}{|\mathbb{F}_q^*|} = \frac{(q^2 - 1)(q^2 - q)}{q - 1} = q(q^2 - 1).$$

□

Lemma 7.6. *Let N be a normal subgroup of a group G and let H be a subgroup of G which contains N. Then,*

$$H/N \lhd G/N \iff H \lhd G$$

Remark 7.7. Theorem 7.6 is in mathlib under the identifier `QuotientGroup.comapMk'OrderIso`.

Proof. If $H \lhd G$, then it follows from the Third Isomorphism Theorem that $H/N \lhd G/N$. Conversely, assume that H/N is normal in G/N. Let x be an arbitrary element of G and h be an arbitrary element of H. Since H/N is normal in G/N we have,

$$xhx^{-1}N = (xN)(hN)(x^{-1}N) = (xN)(hN)(xN)^{-1} \in H/N.$$

Thus $xhx^{-1} \in H$. Since x and h were chosen arbitrarily, we have that $H \lhd G$. □

7.2 The Six Cases

We now address individually the 6 possible combinations of s and t in (6.16) and determine the structure of G in each case.

Theorem 7.8 (Case I)**.** *$card_noncenter_fin_subgroup_equm_card_noncenter_multi_index_normalizer, MaximalAbelia
In this case, the Sylow p-subgroup Q is different from G and is an elementary abelian normal subgroup of G.*

Proof. Here, $s = 1$ and $t = 0$. Equation (6.16) simplifies to:

$$\begin{aligned} 1 &= \frac{1}{g} + \frac{q-1}{qk} + \frac{g_1 - 1}{g_1}, \\ 1 &= \frac{1}{g} + \frac{1}{k} - \frac{1}{qk} + 1 - \frac{1}{g_1}, \\ \frac{1}{qk} + \frac{1}{g_1} &= \frac{1}{g} + \frac{1}{k}. \end{aligned} \tag{7.3}$$

Case Ia: $q = 1$. Here we have $Q = I_G$ and is trivially an elementary abelian normal subgroup of G. Equation (7.3) gives $g = g_1$, thus $G/Q = G = A_1$, which indeed is a cyclic group whose order is relatively prime to p.

Case Ib: $q > 1$. If $k = 1$ then (7.3) gives,

$$\frac{1}{q} + \frac{1}{g_1} = \frac{1}{g} + 1 \ > \ 1.$$

But since both $1/q$ and $1/g_i$ are at most $1/2$ each, this is a contradiction. Thus $k > 1$. This means that $|K| = ek > e = |Z|$, so $k = g_1$ by Theorem 6.42. Equation (7.3) now gives $qk = g$.

$$|G| = eg = eqk = |N_G(Q)|.$$

Thus $G = N_G(Q)$ and so $Q \lhd G$. Therefore $Q \neq G$ and is an elementary abelian normal subgroup of G. Also,

$$G/Q = N_G(Q)/Q \cong K = A_1.$$

Thus G/Q is a cyclic group whose order is relatively prime to p.

□

Theorem 7.9 (Case II)**.** *$card_noncenter_finsubgroup_eq_sum_ccard_noncenter_mul_iindex_normalizer, MaximalAbeli$ The order of G is relatively prime to p and either $G \cong \mathrm{SL}_2(3)$ or G is the group of order $4n$, where n is odd,*

Proof. Here, $s = 1 = t$. Equation (6.16) simplifies to:

$$\begin{aligned} 1 &= \frac{1}{g} + \frac{q-1}{qk} + \frac{g_1 - 1}{g_1} + \frac{g_2 - 1}{2g_2}, \\ 1 &= \frac{1}{g} + \frac{q-1}{qk} + 1 - \frac{1}{g_1} + \frac{1}{2} - \frac{1}{2g_2}, \\ \frac{1}{g_1} + \frac{1}{2g_2} &= \frac{1}{2} + \frac{1}{g} + \frac{q-1}{qk}. \end{aligned} \tag{7.4}$$

First assume that $q > 1$. This means $(q-1)/qk \geq 1/2k$ and consequently we bound (7.4) from below:

$$\frac{1}{2g_2} = \frac{1}{2} - \frac{1}{g_1} + \frac{1}{g} + \frac{q-1}{qk} \;>\; \frac{1}{2k}.$$

Thus $k > g_2 \geq 2$. So $K \in \mathfrak{M}$ and $k = g_i$ for some i. Since it is strictly greater than g_2, we have $k = g_1$. Equation (7.4) now becomes

$$\begin{aligned} \frac{1}{g_1} + \frac{1}{2g_2} \;&=\; \frac{1}{2} + \frac{1}{g} + \frac{q-1}{qg_1}, \\ \frac{1}{g_1} + \frac{1}{2g_2} \;&>\; \frac{1}{2} + \frac{1}{2g_1}, \\ \frac{1}{4} + \frac{1}{4} \;\geq\; \frac{1}{2g_1} + \frac{1}{2g_2} \;&>\; \frac{1}{2}. \end{aligned}$$

This contradiction disproves the assumption that $q > 1$, so we have that $q = 1$. This means that Q, a Sylow p-subgroup of G, is simply the identity element and so $|G|$ is relatively prime to p. Also, Equation (7.4) now reduces to:

$$\frac{1}{g_1} + \frac{1}{2g_2} = \frac{1}{2} + \frac{1}{g}. \tag{7.5}$$

If $g_1 \geq 4$ we get

$$\frac{1}{2g_2} = \frac{1}{2} + \frac{1}{g} - \frac{1}{g_1} \;>\; \frac{1}{4}.$$

Since $g_2 > 1$ this gives a contradiction and thus $g_1 < 4$. We now have two seperate cases to consider.

Case IIa: $g_1 = 2$. Equation (7.5) becomes

$$\frac{1}{2g_2} = \frac{1}{g}, \implies g = 2g_2.$$

If $e = 1$, then $p = 2$. Also since $q = 1$, 2 does not divide $|G|$, but $|G| = eg = e2g_2$ which is a contradiction. So $e = 2$ and $p \neq 2$. We now have:

$$|N_G(A_2)| = 2|A_2| = 2eg_2 = eg = |G|, \qquad \text{(since } s + t = 2\text{)}$$
$$|N_G(A_1)| = |A_1| = eg_1 = 4. \qquad \text{(since } s = 1\text{)}$$

Thus $G = N_G(A_2)$, that is $A_2 \lhd G$.

By Corollary **??**, A_1 is contained in a Sylow 2-subgroup of G, call it S. If S is strictly larger than A_1, then by Lemma **??**, $A_1 \subsetneq N_S(A_1) \subset N_G(A_1)$. Since $A_1 = N_G(A_1)$ we conclude that A_1 is a Sylow 2-subgroup of G. This means that 8 does not divide $|G| = 4g_2$ and so $g_2 = n$, where n is odd.

Since A_2 is cyclic it is generated by a single element, so let $A_2 = \langle x \rangle$ and thus $x^{2n} = I_G$. Recall that because $[N_G(A_2) : A_2] = 2$, Theorem 6.40 tells us that there exists a $y \in N_G(A_2) \backslash A_2$ such that $yxy^{-1} = x^{-1}$.

Recall from Chapter 2 that the number of A_i in each conjugacy class $\mathcal{C}_i$ is equal to $[G : N_G(A_i)]$ so,

$$|\mathcal{C}_2| = [G : N_G(A_2)] = 1.$$

Due to the fact that y belongs to some maximal abelian subgroup of G, and since $y \notin A_2$ and $|\mathcal{C}_2| = 1$, it must be that y belongs to A_1 or one of its conjugate subgroups. Thus y has an order which divides $|A_1| = 4$ and since the only elements of order 1 and 2 lie in Z, the order of y is 4. Furthermore, both x^n and y^2 have order 2. Recalling that G has at most 1 element of order 2, this gives the relation $x^n = y^2$.

Let H be the group generated by x and y and the above relations:

$$H = \langle\, x, y \,|\, x^n = y^2,\, yxy^{-1} = x^{-1} \rangle.$$

Notice that the second relation gives that $yx^ny^{-1} = x^{-n}$, so

$$x^{-n} = yx^ny^{-1} = yy^2y^{-1} = y^2 = x^n.$$

This shows that $y^4 = x^{2n} = I_G$ and that H is finite. Moreoever,

$$H = \{x^k, x^k y : 0 < k \leq 2n\}.$$

Thus $|H| = 4n = |G|$ and $H = G$.

Case IIb: $g_1 = 3$. Equation (7.5) becomes

$$\frac{1}{2g_2} = \frac{1}{6} + \frac{1}{g} > \frac{1}{6}.$$

Therefore $g_2 = 2$ and $g = 12$. Again, since $q = 1$ and 2 divides $|G|$, we have $p \neq 2$ and so $e = 2$. Thus we have,

$$|G| = eg = 24, \qquad |A_1| = eg_1 = 6, \qquad |A_2| = eg_2 = 4.$$

Again we determine the number of maximal abelian subgroups in each conjugacy class.

$$|\mathcal{C}_1| = [G : N_G(A_1)] = \frac{|G|}{|A_1|} = \frac{24}{6} = 4,$$

$$|\mathcal{C}_2| = [G : N_G(A_2)] = \frac{|G|}{2|A_2|} = \frac{24}{8} = 3.$$

The figure below shows G divided into it's maximal abelian subgroups:

Let $A_2 = \langle x \rangle$. By Theorem 6.40, there is an element $y \in N_G(A_2) \backslash A_2$ such that $yxy^{-1} = x^{-1}$. Since $N_G(A_2)$ has order 8, the order of y must divide 8. The order of y cannot be 8 since $N_G(A_2)$ is not cyclic and the only elements with order 1 or 2 are found in Z, thus y has order 4. By the uniqueness of the element of order 2, we have $x^2 = y^2$. So

$$N_G(A_2) = \langle x, y \mid x^2 = y^2, yxy^{-1} = x^{-1} \rangle.$$

For simplicity let $N = N_G(A_2)$. Since $|A_1| = 6$, the only elements in C_1 with order 2^k are those in Z, so every element of G with order 2^k must belong to C_2. Since C_2 has order 8 it is equal to N because each element of N has order 2^k. Furthermore, N is thus a unique Sylow 2-subgroup of G and by Corollary **??**, we have $N \lhd G$.

Now consider the quotient group G/N, that is the set of left (or right) cosets of N in G.

$$G/N = \{N, rN, r^2N\} \cong \langle r \rangle \cong \mathbb{Z}_3,$$

where r is some element of $G \backslash N$ with order 3. Without loss of generality we may regard r to be a generator of H, where H is the cyclic subgroup of A_1 of order 3.

Let H act on N by conjugation. Since $|H| = 3$ the orbit of $x \in N$ has size 1 or 3.

$$\text{Orb}(x) = \{r^k x r^{-k} : r^k \in H\}.$$

Since H is not contained in the centraliser of x we conclude that the orbit of x has size 3. Let A_2, A_2' and A_2'' be the 3 elements of $\mathcal{C}_2$. Without loss of generality we may assume $y \in A_2'$ and consequently $xy \in A_2''$. Using the two relations between x and y we observe that,

$$(xy)^{-1} = y^{-1}x^{-1} = y^{-1}(yxy^{-1}) = xy^{-1} = x^{-1}x^2y^{-1} = x^{-1}y = yx$$

The elements of Z are fixed points under this group action and the remaining 6 elements of N form 2 orbit cycles of order 3, with each cycle containing exactly one element from the noncentral parts of A_2, A_2' and A_2'' in some order. If y inverts x, then y inverts all powers of x including x^{-1}. Also, if y inverts x, then y^{-1} inverts x^{-1} and thus inverts x also. So the 2 relations we have established between x and y actually hold for any pair of elements of $N\backslash Z$ which belong to different elements of $\mathfrak{M}$. Therefore without loss of generality, we may assume that x and y are in the same orbit cycle and that $rxr^{-1} = y$. Fig 3 shows that there are only 2 elements which could complete this cycle, xy and yx. If $ryr^{-1} = xy$, then we have the following 3 relations on G.

$$rxr^{-1} = y, \qquad ryr^{-1} = xy, \qquad rxyx^{-1} = x. \tag{7.6}$$

Otherwise $ryr^{-1} = yx$. In this case, consider the orbit of x under conjugation by r^2 instead. This gives the same orbit cycle but in the opposite direction:

$$r^2xr^{-2} = yx, \qquad r^2yxr^{-2} = y, \qquad r^2yr^{-2} = x.$$

Observe that $x(yx) = x(x^{-1}y) = y$. Thus without loss of generality we can rename r^2 as r, yx as y and y as xy. Notice that this now gives the same relations as in (7.6). Since x and y generate a group of order 8 and r has order 3, the group given by the following presentation has order at most 24 and is thus a presentation of G.

$$\langle x, y, r \,|\, x^2 = y^2,\, yxy^{-1} = x^{-1},\, r^3 = I,\, rxr^{-1} = y,\, ryr^{-1} = xy,\, rxyr^{-1} = x\rangle,$$

By Lemma **??**, we observe that the order of $\mathrm{SL}_2(3)$ is $3(3^2 - 1) = 24$. Now consider the following the elements of $\mathrm{SL}_2(3)$:

$$a = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}, \qquad b = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}, \qquad c = \begin{bmatrix} 2 & 1 \\ 2 & 0 \end{bmatrix}.$$

One can verify easily that each of the following relations hold:

$$\begin{aligned} a^2 = b^2, \qquad & bab^{-1} = a^{-1}, \qquad & c^3 = I, \\ cac^{-1} = b, \qquad & cbc^{-1} = ab, \qquad & cabc^{-1} = a. \end{aligned}$$

Since G and $\mathrm{SL}_2(3)$ have the same order and since their respective generators satisfy the corresponding relations, there is an isomorphism mapping $x \mapsto a$, $y \mapsto b$ and $r \mapsto c$. Thus,

$$G = \langle x, y, r\rangle \cong \langle a, b, c\rangle = \mathrm{SL}_2(3).$$

□

Theorem 7.10 (Case III)**.** *$card_noncenter_fin_subgroup_eq_sum_c ard_noncenter_mul_index_normalizer, MaximalAbe$
We have $G = Q \times Z$.*

Proof. Here, $s = 0 = t$. Equation (6.16) simplifies to:

$$\begin{aligned} 1 &= \frac{1}{g} + \frac{q-1}{qk}, \\ 1 &= \frac{1}{g} + \frac{1}{k} - \frac{1}{qk}, \\ 1 + \frac{1}{qk} &= \frac{1}{g} + \frac{1}{k}. \end{aligned} \tag{7.7}$$

Since $s = 0 = t$, there are no cyclic maximal abelian subgroups whose order is relatively prime to p, so $K \notin \mathfrak{M}$. Then by Theorem 6.42 we have,

$$ek = |K| \leq |Z| = e.$$

Thus $k = 1$ and equation (7.7) reduces to $1/q = 1/g$, that is $g = q$.

$$\begin{aligned} |G| = eg = eq = |Q \times Z|, \\ G = Q \times Z. \end{aligned}$$

□

Theorem 7.11 (Case IV)**.** *$card_noncenter_fin_subgroup_eq_sum_c ard_noncenter_mul_index_normalizercase_IVClaim$
Either $p = 2$ and G is isomorphic to the dihedral group of order $2n$, where n is odd, or $p = 3$ and $G \cong \mathrm{SL}_2(3)$*

Proof. Here, $s = 0$ and $t = 1$. Equation (6.16) simplifies to:

$$\begin{aligned} 1 &= \frac{1}{g} + \frac{q-1}{qk} + \frac{g_1 - 1}{2g_1}, \\ 1 &= \frac{1}{g} + \frac{q-1}{qk} + \frac{1}{2} - \frac{1}{2g_1}, \\ \frac{1}{2} + \frac{1}{2g_1} &= \frac{1}{g} + \frac{q-1}{qk}. \end{aligned} \tag{7.8}$$

Recall that $|A_1| = eg_1$ and $[N_G(A_1) : A_1] = 2$ and so,

$$eg = |G| \geq |N_G(A_1)| = 2eg_1.$$

So $g \geq 2g_1$ and $1/2g_1 \geq 1/g$ and hence we can bound Equation (7.8):

$$\frac{1}{2} \;\leq\; \frac{1}{2} + \frac{1}{2g_1} - \frac{1}{g} = \frac{q-1}{qk}.$$

Clearly this forces $k = 1$ and also $q > 1$. We can now simplify and bound Equation (7.8) as follows:

$$\frac{1}{q} + \frac{1}{4} \;\geq\; \frac{1}{q} + \frac{1}{2g_1} = \frac{1}{g} + \frac{1}{2} \;>\; \frac{1}{2}.$$

This gives $1/q > 1/4$ and so q is equal to either 2 or 3. We examine each case individually.

Case IVa: $q = 2$. Equation (7.8) becomes

$$\frac{1}{2g_1} = \frac{1}{g}, \implies g = 2g_1,$$

and we show that A_1 is a normal subgroup of G:

$$|G| = eg = e2g_1 = 2|A_1| = |N_G(A_1)|.$$

In this case, a Sylow p-subgroup has order 2 so we have $p = 2$ and also $e = 1$. By it's definition, the order of A_1 is relatively prime to $p = 2$, so we have that $|A_1| = g_1 = n$, where n is odd, and consequently G has order $2n$.

We now know enough about the structure of G to establish some relations on it. Let $A_1 = \langle x \rangle$, so $x^n = I_G$. By Theorem 6.40 there exists a $y \in N_G(A_1) \backslash A_1$ such that $yxy^{-1} = x^{-1}$.

$$|\mathcal{C}_1| = [G : N_G(A_1)] = 1.$$
$$|\mathcal{C}_{Q\times Z}| = [G : N_G(Q \times Z)] = \frac{|G|}{eqk} = \frac{2n}{2} = n.$$

The only maximal abelian subgroups of G are thus A_1 and the n conjugate subgroups of $\mathcal{C}_{Q\times Z}$.

Since y belongs to some maximal abelian subgroup and $y \notin A_1$, y must belong to some element of $\mathcal{C}_{Q\times Z}$. Since $|Q \times Z| = 2$, the order of y is 2 and $y^2 = I_G$. We have established the following presentation of G.

$$G = \langle x, y \mid x^n = I_G = y^2,\ yxy^{-1} = x^{-1} \rangle.$$

Let D_n denote the dihedral group of order $2n$, that is the group of symmetries of a regular polygon wih n vertices. Let r denote a clockwise rotation by $2\theta/n$ radians and s denote a reflection. For n odd, it can easily be verified that D_n has the following presentation.

$$D_n = \langle r, s \mid r^n = I = s^2,\ srs^{-1} = r^{-1} \rangle.$$

Since G and D_n have the same order and since their respective generators satisfy the corresponding relations, there is an isomorphism mapping $x \mapsto r$ and $y \mapsto s$. Thus,

$$G = \langle x, y \rangle \cong \langle r, s \rangle = D_n.$$

Case IVb: $q = 3$. Now equation (7.8) becomes

$$\frac{1}{2g_1} = \frac{1}{g} + \frac{1}{6} > \frac{1}{6}.$$

This means that $g_1 = 2$ and $g = 12$. Since $q = 3$ we have $p = 3$ and $e = 2$. Furthermore we have,

$$|G| = 24, \quad |A_1| = 4, \quad |N_G(A_1)| = 8, \quad |Q \times Z| = 6 \quad |N_G(Q \times Z)| = 6$$

$$|\mathcal{C}_1| = [G : N_G(A_1)] = \frac{24}{8} = 3$$
$$|\mathcal{C}_{Q\times Z}| = [G : N_G(Q \times Z)] = \frac{24}{6} = 4$$

Notice that Fig 5 is almost identical to Fig 2 in the study of Case IIb. This is a strong indication that these 2 cases are isomorphic to each other and hence also to $\mathrm{SL}_2(3)$, albeit not a proof. However, an argument analogous to the one outlined in the proof of Case IIb can be directly applied here with a simple renaming of the conjugacy classes and representatives. It would be to repeat this argument again and I will leave it to the reader to verify.

□

Theorem 7.12 (Case V)**.** *case$_V$Claim : We have one of the following three cases:(i) $G \cong \mathrm{SL}_2(\mathbb{F}_q)$.(ii) $G \cong \langle$S*

Proof. card$_n$oncenter$_f$in$_s$ubgroup$_e$q$_s$um$_c$ard$_n$oncenter$_m$ul$_i$ndex$_n$ormalizer, $MaximalAbelianSubgroup.K_m$e
$= 0$and$t = 2.Equation(6.16)simplifiesto$:

Recall that,

$$eg = |G| \geq |N_G(A_i)| \geq 2eg_i, \qquad \text{thus} \quad \frac{1}{g} \leq \frac{1}{2g_i}.$$

Equation (**??**) is therefore bounded from below:

$$\frac{2}{g} \leq \frac{1}{2g_1} + \frac{1}{2g_2} = \frac{1}{g} + \frac{q-1}{qk}.$$

Therefore $q > 1$, since if $q = 1$ we arrive at the contradiction $2/g \leq 1/g$. With this in mind we have $(q-1)/q \geq 1/2$ and since $g_i \geq 2$ this allows us to bound (**??**) on either side.

$$\frac{1}{2} \geq \frac{1}{2g_1} + \frac{1}{2g_2} = \frac{1}{g} + \frac{q-1}{qk} > \frac{q-1}{qk} \geq \frac{1}{2k}.$$

This gives $k > 1$ and so by Theorem 6.42, k must equal g_1 or g_2 since the inequality $ek = |K| > |Z| = e$ holds. Without loss of generality we let $k = g_1$ and (**??**) becomes,

$$\frac{1}{2g_1} + \frac{1}{2g_2} = \frac{1}{g} + \frac{q-1}{qg_1} = \frac{1}{g} + \frac{1}{g_1} - \frac{1}{qg_1},$$
$$\frac{1}{2g_2} = \frac{1}{g} + \frac{1}{2g_1} - \frac{1}{qg_1}. \tag{7.9}$$

Let $N_G(Q)$ act on $Q\backslash I_G$ by conjugation and consider the stabiliser in $N_G(Q)$ of an arbitrarily chosen $x \in Q\backslash I_G$.

$$\begin{aligned}
\mathrm{Stab}(x) &= \{g \in N_G(Q) : gxg^{-1} = x\} \\
&= C_G(x) \cap N_G(Q) \\
&= (Q \times Z) \cap N_G(Q) && \text{(by Theorem 6.38)} \\
&= Q \times Z. && \text{(since } Q \times Z \subset N_G(Q)\text{)}
\end{aligned}$$

Thus by the Orbit-Stabiliser Theorem,

$$|\mathrm{Orb}(x)| = [N_G(Q) : Q \times Z] = \frac{eqk}{eq} = k$$

Since x was chosen arbitrarily from $Q\backslash I_G$, each element of $Q\backslash I_G$ has an orbit in $N_G(Q)$ of size k. Considering also the fact that $Q\backslash I_G$ is equal to the union of the pairwise disjoint orbits of its elements, we conclude that $k = g_1$ divides $|Q\backslash I_G|$. Thus there exists some $d \in \mathbb{Z}^+$ such that,

$$q - 1 = dg_1. \tag{7.10}$$

Now set,

$$i = \frac{2g_1g_2q}{g} > 0, \tag{7.11}$$

and multiply (7.9) by ig to give,

$$g_1q = i + (q-2)g_2. \tag{7.12}$$

Thus i is an integer and since it is greater than zero by definition, (7.12) gives,

$$g_1 > \frac{(q-2)g_2}{q}. \tag{7.13}$$

Also, using (7.10) and (7.12) we get,

$$\begin{aligned}
g_1q &= i + (q-1)g_2 - g_2 \\
&= i + dg_1g_2 - g_2, \\
g_2 &= i + (dg_2 - q)g_1.
\end{aligned} \tag{7.14}$$

Applying Lemma **??** we observe that Q is not normal in G, and so

$$eg = |G| > |N_G(Q)| = eqk = eqg_1,$$

$$\frac{1}{qg_1} > \frac{1}{g}.$$

And (7.9) gives us,

$$\frac{1}{2g_2} = \frac{1}{g} - \frac{1}{qg_1} + \frac{1}{2g_1} < \frac{1}{2g_1},$$

$$g_1 < g_2. \tag{7.15}$$

Consider now,

$$[G : N_G(Q)] = \frac{eg}{eqk} = \frac{g}{qg_1} = \frac{2g_2}{i} \in \mathbb{Z}. \qquad \text{(by (7.11))}$$

Thus i divides $2g_2$. Recall that the order of A_2 is relatively prime to p by Theorem 6.38, so g_2 is also relatively prime to p. Therefore if $p \neq 2$, i is relatively prime to p and if $p = 2$ then p divides i but p^2 does not. Now since Q is a Sylow p-subgroup of G, this means that greatest common denominator of i and q is either 1 or 2. Now consider,

$$[G : N_G(A_2)] = \frac{eg}{2eg_2} = \frac{g_1 q}{i} \in \mathbb{Z}. \qquad \text{(by (7.11))}$$

Thus i divides $g_1 q$ and since $\gcd(i, q) = 1$ or 2, i must divide $2g_1$. So there exists some $m \in \mathbb{Z}^+$ such that,

$$i = \frac{2g_1}{m}. \tag{7.16}$$

We consider now the separate cases which arise for different values of q.

Cases Va and Vb: $q \geq 4$. This condition gives us a lower bound for the inequality in (7.13),

$$g_1 > \frac{(q-2)g_2}{q} > \frac{g_2}{2}.$$

Combining this with (7.15) we have,

$$g_1 < g_2 < 2g_1. \tag{7.17}$$

Substituting (7.16) into (7.14) gives,

$$g_2 = \left(\frac{2}{m} + dg_2 - q\right) g_1$$

Thus (7.17) gives that,

$$1 < \frac{2}{m} + dg_2 - q < 2.$$

This means that $2/m$ is some fraction between 0 and 1 and $dg_2 - q = 1$. So (7.14) becomes,

$$g_2 = g_1 + i. \tag{7.18}$$

Substituting this into (7.9) we find that,

$$\begin{aligned} g_1 q &= i + (q-2)(g_1 + i), \\ 2g_1 &= i(q-1) = idg_1, \qquad \text{(by (7.10))} \\ 2 &= id. \end{aligned}$$

We remark that since both i and d are positive integers, i (and indeed d) must equal 1 or 2. Thus by (7.18) and (7.11),

$$g_1 = \frac{i(q-1)}{2}, \qquad g_2 = \frac{i(q+1)}{2}, \qquad g = \frac{2g_1 g_2 q}{i} = \frac{iq(q^2-1)}{2}.$$

Thus we have the following expressions for the orders of K and G:

$$|K| = \frac{ei(q-1)}{2}, \qquad |G| = \frac{eiq(q^2-1)}{2}. \tag{7.19}$$

By Proposition 5.64, each noncentral element of Q has a unique common fixed point on the projective line L, call it P_1. Furthermore, we saw in the proof of Theorem 6.42 that each noncentral element of K also fixes P_1 as well as one other point, call it P_2. Let u be a noncentral element of Q and set $P_3 = P_2^u$. Clearly P_3 is different from P_1 and P_2 because otherwise a contradiction is reached. By Theorem 5.63, $PSL(L)$ is triply transitive, so there exists a $v \in L$ such that,

$$P_1^v = R_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \qquad P_2^v = R_2 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad P_3^v = R_3 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

Observe that,

$$\begin{aligned} vQv^{-1}R_1 &= vQP_1 = vP_1 = R_1, \\ vKv^{-1}R_i &= vKP_i = vP_i = R_i. \qquad (i = 1, 2) \end{aligned}$$

Thus vQv^{-1} fixes R_1 whilst vKv^{-1} fixes both R_1 and R_2. The only elements of L that fix R_1 are the lower triangular matrices, thus $vQv^{-1} \subset H$, whilst the only elements that fix R_2 are the upper triangular matrices, thus $vKv^{-1} \subset D$. Furthermore, each noncentral element of vQv^{-1} has order p. The only elements of H with order p are those in T, thus $vQv^{-1} \subset T$. Since $u \in Q \setminus I_G$, we have that $vuv^{-1} = t_\gamma$ for some $\gamma \in F$.

$$vuv^{-1}R_2 = vuP_2 = vP_3 = R_3,$$

$$\begin{bmatrix} 1 & 0 \\ \gamma & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ \gamma \end{bmatrix} \sim \begin{bmatrix} 1 \\ 1 \end{bmatrix}. \Longrightarrow \gamma = 1.$$

So $vuv^{-1} = t_1$. If we now consider $\widetilde{G} = vGv^{-1}$ instead of G, we can assume without loss of generality that,

$$Q \subset T, \qquad K \subset D, \qquad u = t_1.$$

Let x be a generator of K. By Theorem 6.40 there exists a $y \in N_{\widetilde{G}}(K)\backslash K$ such that $yx = x^{-1}y$. Since R_1 is fixed by both x and x^{-1} we have,

$$x^{-1}yR_1 = yxR_1 = yR_1.$$

Thus x^{-1} fixes yR_1, that is $yR_1 \in \{R_1, R_2\}$. Similarly, $yR_2 \in \{R_1, R_2\}$. Assume $yR_1 = R_1$. Since R_1 and R_2 are distinct points in L this implies that $yR_2 = R_2$.

$$yR_1 = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \beta \\ \delta \end{bmatrix} \sim \begin{bmatrix} 0 \\ 1 \end{bmatrix} \Longrightarrow \beta = 0.$$

$$yR_2 = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \alpha \\ \gamma \end{bmatrix} \sim \begin{bmatrix} 1 \\ 0 \end{bmatrix} \Longrightarrow \gamma = 0.$$

Thus $y \in D$, which is a contradiction since elements in D do not invert $x \in D$, hence,

$$yR_1 = R_2, \qquad \text{and} \quad yR_2 = R_1. \tag{7.20}$$

This allows us to determine more about y,

$$yR_1 = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \beta \\ \delta \end{bmatrix} \sim \begin{bmatrix} 1 \\ 0 \end{bmatrix} \Longrightarrow \delta = 0.$$

$$yR_2 = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \alpha \\ \gamma \end{bmatrix} \sim \begin{bmatrix} 0 \\ 1 \end{bmatrix} \Longrightarrow \alpha = 0.$$

Thus y is an anti-diagonal matrix. Recalling (5.1), for some $\rho \in F^*$ we have,

$$y = d_\rho w = \begin{bmatrix} 0 & \rho \\ -\rho^{-1} & 0 \end{bmatrix}.$$

Consider now the set of right cosets of $N_{\widetilde{G}}(Q)$ of the form $N_{\widetilde{G}}(Q)yq$, (where $q \in Q$) in $N_{\widetilde{G}}(Q)yQ$. For $q_1, q_2 \in Q$ we have,

$$\begin{aligned} N_{\widetilde{G}}(Q)yq_1 = N_{\widetilde{G}}(Q)yq_2 &\iff yq_2{q_1}^{-1}y^{-1} \in N_{\widetilde{G}}(Q) \\ &\iff q_2{q_1}^{-1} \in y^{-1}N_{\widetilde{G}}(Q)y \\ &\iff (Q \cap y^{-1}N_{\widetilde{G}}(Q)y)q_2 = (Q \cap y^{-1}N_{\widetilde{G}}(Q)y)q_1. \end{aligned}$$

So the number of right cosets of $N_{\widetilde{G}}(Q)$ in $N_{\widetilde{G}}(Q)yQ$ is equal to the number of right cosets of $Q \cap y^{-1}N_{\widetilde{G}}(Q)y$ in Q. That is,

$$[N_{\widetilde{G}}(Q)yQ : N_{\widetilde{G}}(Q)] = [Q : Q \cap y^{-1}N_{\widetilde{G}}(Q)y]. \tag{7.21}$$

Let g be an arbitrary element of $N_{\widetilde{G}}(Q)$. By Theorems **??**(i) and 5.64(ii) we have $N_{\widetilde{G}}(Q) \subset H = \mathrm{Stab}(R_1)$, thus g fixes R_1. Using (7.20) we see that,

$$y^{-1}gyR_2 = y^{-1}gR_1 = y^{-1}R_1 = R_2.$$

Hence R_2 is a fixed point of $y^{-1}gy$. Since g was chosen arbitrarily, we assert that each element of $y^{-1}N_{\widetilde{G}}(Q)y$ fixes R_2. On the contrary, the only element of Q which fixes R_2 is $I_{\widetilde{G}}$, thus $Q \cap yN_{\widetilde{G}}(Q)y^{-1} = I_{\widetilde{G}}$.

$$\begin{aligned} [N_{\widetilde{G}}(Q)yQ : N_{\widetilde{G}}(Q)] &= [Q : Q \cap y^{-1}N_{\widetilde{G}}(Q)y] = q, \\ |N_{\widetilde{G}}(Q)yQ| &= q|N_{\widetilde{G}}(Q)|. \end{aligned} \tag{7.22}$$

We show next that $N_{\widetilde{G}}(Q)yQ \cap N_{\widetilde{G}}(Q) = \varnothing$. Let $t_\lambda d_\omega$ and t_μ be arbitrarily chosen from $N_{\widetilde{G}}(Q)$ and Q respectively so that $t_\lambda d_\omega y t_\mu$ is an arbitrary element of $N_{\widetilde{G}}(Q)yQ$.

$$\begin{aligned} t_\lambda d_\omega y t_\mu &= \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix} \begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{bmatrix} \begin{bmatrix} 0 & \rho \\ -\rho^{-1} & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \mu & 1 \end{bmatrix} \\ &= \begin{bmatrix} \omega & 0 \\ \omega\lambda & \omega^{-1} \end{bmatrix} \begin{bmatrix} \rho\mu & \rho \\ -\rho^{-1} & 0 \end{bmatrix} \\ &= \begin{bmatrix} \omega\rho\mu & \omega\rho \\ \omega\lambda\rho\mu - \omega^{-1}\rho^{-1} & \omega\rho\lambda \end{bmatrix}. \end{aligned} \tag{7.23}$$

Since ω, $\rho \in F^*$, the top right entry of (7.23) is non-zero. Recall also that $N_{\widetilde{G}}(Q) \subset H$ by Theorem **??**(i) and that H is the set of all lower triangular matrices of L. Since $t_\lambda d_\omega d_\rho w t_\mu$ was chosen arbitraily, no element of $N_{\widetilde{G}}(Q)yQ$ is in H whilst the whole of $N_{\widetilde{G}}(Q)$ is contained in H, thus they are disjoint. Using (7.22) and (7.19) we also observe that,

$$|N_{\widetilde{G}}(Q)yQ| + |N_{\widetilde{G}}(Q)| = (q+1)|N_{\widetilde{G}}(Q)| = (q+1)eqg_1 = \frac{eiq(q^2-1)}{2} = |\widetilde{G}|.$$

Since $N_{\widetilde{G}}(Q)yQ$ and $N_{\widetilde{G}}(Q)$ are disjoint and the sum of their orders is equal to the order of $\widetilde{G}$, they partition $\widetilde{G}$ into the set of elements that belong to H and the set that don't.

$$\widetilde{G} = N_{\widetilde{G}}(Q)yQ \cup N_{\widetilde{G}}(Q). \tag{7.24}$$

Let $\mathbb{N} = \{\lambda : t_\lambda \in Q\}$. We will show that $\mathbb{N} = \mathbb{F}_q$. For each $t_\lambda \in Q \setminus Z$, the element $yt_\lambda y^{-1} \notin H$, so by (7.24), $yt_\lambda y^{-1} \in N_{\widetilde{G}}(Q)yQ$. Thus there exists

$t_\mu, t_\upsilon \in Q$ and $d_\omega \in K$ such that,

$$yt_\lambda y^{-1} = t_\mu d_\omega y t_\upsilon,$$

$$\begin{bmatrix} 0 & \rho \\ -\rho^{-1} & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix} \begin{bmatrix} 0 & -\rho \\ \rho^{-1} & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \mu & 1 \end{bmatrix} \begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{bmatrix} \begin{bmatrix} 0 & \rho \\ -\rho^{-1} & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \upsilon & 1 \end{bmatrix},$$

$$\begin{bmatrix} 0 & \rho \\ -\rho^{-1} & 0 \end{bmatrix} \begin{bmatrix} 0 & -\rho \\ \rho^{-1} & -\rho\lambda \end{bmatrix} = \begin{bmatrix} \omega & 0 \\ \omega\mu & \omega^{-1} \end{bmatrix} \begin{bmatrix} \rho\upsilon & \rho \\ -\rho^{-1} & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & -\rho^2\lambda \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \omega\rho\upsilon & \omega\rho \\ \omega\rho\mu\upsilon - \omega^{-1}\rho^{-1} & \omega\rho\mu \end{bmatrix}.$$

Equating the top right entries gives,

$$\omega = -\rho\lambda. \tag{7.25}$$

Since $t_1 \in Q$, so is it's inverse, thus $-1 \in \mathbb{N}$. Letting $\lambda = -1$ in (7.25) gives $\omega = \rho$, which means that $d_\rho \in K$. Consequently, this shows that $w = d_\rho^{-1} y \in \widetilde{G}$ and we may replace y by w in (7.24) without it affecting the partition of $\widetilde{G}$. This is equivalent to letting $\rho = 1$, and (7.25) simplifies to,

$$\omega = -\lambda. \tag{7.26}$$

Let $\mathbb{M} = \{\omega : d_\omega \in K\}$. Recall from (7.19) that $|K| = i(q-1)$. We consider the different cases which arise depending on the values of i and e.

Let **Case Va** be the case when $e = 1$ or $i = 1$. Observe that i and e cannot both equal 1, since this would imply that 2 divides $q-1$ (by (7.19)), but if $e = 1$ it follows that $q-1$ is even. Hence $ei = 2$ and K has order $q-1$. Furthermore, the order of each element of K divides $q-1$, so for each $\omega \in \mathbb{M}$,

$$\omega^{q-1} = 1. \tag{7.27}$$

Also, the following polynomial has at most $q-1$ roots in F.

$$x^{q-1} = 1. \tag{7.28}$$

By (7.2), $\mathbb{F}_q \subset F$ and each element of $\mathbb{F}_q^*$ is a root of (7.28). Thus each ω of $\mathbb{M}$ is in $\mathbb{F}_q^*$ and since they have the same cardinality, $\mathbb{M} = \mathbb{F}_q^*$. By (7.26), λ also ranges over $\mathbb{F}_q^*$ and considering also that λ can be 0, we have $\mathbb{N} = \mathbb{F}_q$.

Observe that each element of $\widetilde{G}$ is either of the form $t_\lambda d_\omega$ or $t_\lambda d_\omega w t_\mu$ (where $\lambda, \mu \in \mathbb{F}_q, \omega \in \mathbb{F}_q^*$), so $\widetilde{G} \subset \mathrm{SL}_2(\mathbb{F}_q)$. Also, Propostion **??** gives that, $|\mathrm{SL}_2(\mathbb{F}_q)| = q(q^2-1) = |\widetilde{G}|$, so $\widetilde{G} = \mathrm{SL}_2(\mathbb{F}_q)$. Since $\widetilde{G}$ is conjugate in L to G, we have $G \cong \mathrm{SL}_2(\mathbb{F}_q)$ as desired.

Let **Case Vb** be the case when $i = 2 = e$. This time the order of each element of K divides $2(q-1)$, so for each $\omega \in \mathbb{M}$,

$$\omega^{2(q-1)} = 1. \tag{7.29}$$

As in the case of $i = 1$, each element of $\mathbb{F}_q^*$ is a root of the polynomial in (7.28), as are each ω^2. Thus ω^2 ranges over $\mathbb{F}_q^*$ and by (7.2), $\omega \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Simple matrix multiplication shows that,

$$d_\omega^{-1} t_\lambda d_\omega = t_{\omega^2 \lambda}.$$

Hence since $t_0, t_1 \in Q$, it follows that $t_{\omega^2} \in Q$ for each $\omega^2 \in \mathbb{F}_q^*$, thus $\mathbb{N} = \mathbb{F}_q$. Since K is a cyclic group of order $2(q-1)$, so too is $\mathbb{M}$. Let π be a generator of $\mathbb{M}$. It follows that π^2 has order $q-1$ and is therefore a generator of $\mathbb{F}_q^*$. Since $K = \langle d_\pi \rangle$, we have:

$$\widetilde{G} = \langle t_\lambda, d_\pi, w : \lambda \in \mathbb{F}_q \rangle = \langle \mathrm{SL}_2(\mathbb{F}_q), d_\pi \rangle.$$

Again, since $\widetilde{G}$ is conjugate in L to G, we have $G \cong \langle \mathrm{SL}_2(\mathbb{F}_q), d_\pi \rangle$ as desired. Now we take an arbitrary x from $\mathrm{SL}_2(\mathbb{F}_q)$ and conjugate it by d_π.

$$\begin{aligned} d_\pi x d_\pi^{-1} &= \begin{bmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} \pi^{-1} & 0 \\ 0 & \pi \end{bmatrix} \\ &= \begin{bmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{bmatrix} \begin{bmatrix} \alpha\pi^{-1} & \beta\pi \\ \gamma\pi^{-1} & \delta\pi \end{bmatrix} \\ &= \begin{bmatrix} \alpha & \beta\pi^{-2} \\ \gamma\pi^2 & \delta \end{bmatrix}. \end{aligned}$$

Since $\pi^2 \in \mathbb{F}_q$, we have that $d_\pi x d_\pi^{-1} \in \mathrm{SL}_2(\mathbb{F}_q)$ and since x was chosen arbitrarily, d_π belongs to the normaliser of $\mathrm{SL}_2(\mathbb{F}_q)$ in $\langle \mathrm{SL}_2(\mathbb{F}_q), d_\pi \rangle$. This shows that $\mathrm{SL}_2(\mathbb{F}_q) \lhd \langle \mathrm{SL}_2(\mathbb{F}_q), d_\pi \rangle$ as desired.

Cases Vc and Vd: $q \leq 3$. Since $q - 1 = dg_1 \geq 2$ by (7.10), q cannot equal 2. So $q = 3 = p$, $e = 2$ and thus $g_1 = 2$. The inequalities in (7.15) and (7.13) give,

$$2 < g_2 < 6.$$

Also, since g_2 is relatively prime to $p = 3$, we have $g_2 = 4$ or 5. Let **Case Vc** be the case when $g_2 = 4$. (7.9) becomes,

$$\frac{1}{8} = \frac{1}{g} + \frac{1}{4} - \frac{1}{6},$$

which gives $g = 24$. Observe that,

$$|K| = 4 = i(q-1), \qquad |G| = 48 = iq(q^2-1),$$

where $i = 2$, thus we have the situation as described in Case Vb. That is, $G \cong \langle \mathrm{SL}_2(\mathbb{F}_q), d_\pi \rangle$ with $q = 3$.

Alternatively, **Case Vd** occurs when $g_2 = 5$. (7.9) becomes,

$$\frac{1}{10} = \frac{1}{g} + \frac{1}{4} - \frac{1}{6}.$$

Thus $g = 60$ and $|G| = 120$. We verify, using Proposition **??**, that $\mathrm{SL}_2(5)$ has the same order as G, that is $|\mathrm{SL}_2(5)| = 5(5^2 - 1) = 120$. Observe that,

$$|\mathcal{C}_1| = [G : N_G(A_1)] = \frac{eg}{2eg_1} = 15,$$

$$|\mathcal{C}_2| = [G : N_G(A_2)] = \frac{eg}{2eg_2} = 6,$$

$$|\mathcal{C}_{Q\times Z}| = [G : N_G(Q \times Z)] = \frac{eg}{ekq} = 10.$$

Now consider the quotient group G/Z of order 60. It's trivial that for all $A_i, A_j \in \mathfrak{M}$, A_i/Z belongs to the same conjugacy class as A_j/Z if and only A_i and A_j belong to the same conjugacy class. So the number of subgroups conjugate to A_i/Z is $|\mathcal{C}_i|$. Similarly, the number of subgroups conjugate to $(Q \times Z)/Z$ is $|\mathcal{C}_{Q\times Z}|$.

We now calculate the order of each maximal abelian subgroup of G when we quotient out Z.

$$|A_1/Z| = 2, \qquad |A_2/Z| = 5, \qquad |(Q \times Z)/Z| = 3.$$

We now know enough about G/Z to determine the order of each of it's elements:

The identity has order 1.gives
The non-central element of A_1/Z has order 2, as does the non-central element in each of the $|\mathcal{C}_1| = 15$ subgroups conjugate to A_1/Z. So there are 15 elements of order 2.
The 4 non-central elements of A_2/Z have order 5, as do the non-central elements in each of the $|\mathcal{C}_2| = 6$ subgroups conjugate to A_2/Z. Thus there are 24 elements of order 5.
The 2 non-central elements of $(Q \times Z)/Z$ have order 3, as do the non-central elements in each of the $|\mathcal{C}_{Q\times Z}| = 10$ subgroups conjugate to $(Q \times Z)/Z$. Thus there are 20 elements of order 3.

Since $1 + 15 + 24 + 20 = 60$, all elements of G/Z are accounted for.

Let N be a normal subgroup of G/Z. Observe that each non-central element of A_2/Z is a generator of it, so if N contains one non-central element of A_2/Z,

then it contains the whole of it, due to the closure of the group under multiplication and the fact that each element of A_2/Z is a power of any non-central element. Also, it can easily be seen that normal subgroups are composed of whole conjugacy classes, so since N is normal in G, if it contains A_2/Z, it must contain all subgroups conjugate to A_2/Z. The consequence of this is that if N has an element of order 5, then it contains all 24 elements of G/Z of order 5. Similarly, if it contains an element of order 2, it contains all 15 of them and if it contains an element of order 3, it contains all 20 of them. This means that $|N|$ is partitioned by some or all of the elements in $\{1, 15, 20, 24\}$. Bearing in mind that the order of N divides 60 and that N contains the identity element, this means that N is equal to either the identity element or it is the whole of G/Z, since it's easy to see that no other partition of those numbers divides 60. Thus G/Z has no non-trivial normal subgroups and is simple.

By [**?**, p.145], the only simple groups of order 60 are those isomorphic to the alternating group A_5 (not to be confused with an element of $\mathfrak{M}$), thus $G/Z \cong A_5$. Since $Z \cong \mathbb{Z}_2$, we have that G is isomorphic to a central extension of A_5 which, according to Schur [**?**], is unique and isomorphic to $\mathrm{SL}_2(5)$ as desired. The proofs of these 2 claims are beyond the scope of this thesis. □

Theorem 7.13 (Case VI)**.** *$card_noncenter_fin_subgroup_eq_sum_ccard_noncenter_mul_index_normalizer, MaximalAbe*
We have one of the following three cases:(i) $G = \langle x, y \,|\, x^n = y^2,\, yxy^{-1} = x^{-1} \rangle$, where n is even.(ii) $G = \widehat{S}_4.($

Proof. Here, $s = 0$ and $t = 3$. Equation (6.16) simplifies to:

$$1 = \frac{1}{g} + \frac{q-1}{qk} + \frac{g_1 - 1}{2g_1} + \frac{g_2 - 1}{2g_2} + \frac{g_3 - 1}{2g_3},$$

$$\frac{1}{2g_1} + \frac{1}{2g_2} + \frac{1}{2g_3} = \frac{1}{g} + \frac{q-1}{qk} + \frac{1}{2}. \tag{7.30}$$

First assume that $q > 1$ and $k = 1$. (7.30) is thus bounded as follows,

$$\frac{3}{4} > \frac{1}{2g_1} + \frac{1}{2g_2} + \frac{1}{2g_3} = \frac{1}{g} + \frac{q-1}{qk} + \frac{1}{2} > 1,$$

which is a contradiction. Now assume that $q > 1$ and $k > 1$. This means that $k = g_i$ for some i. Without loss of generality we can assume that $k = g_1$. Now (7.30) becomes,

$$\frac{1}{2} \geq \frac{1}{2g_2} + \frac{1}{2g_3} \geq \frac{1}{g} + \frac{1}{2} > \frac{1}{2},$$

which again is a contradiction, thus we conclude that $q = 1$. (7.30) simplifies and we can now determine the possible values of each g_i.

$$\frac{1}{2g_1} + \frac{1}{2g_2} + \frac{1}{2g_3} = \frac{1}{g} + \frac{1}{2}. \tag{7.31}$$

Without loss of generality we may assume that $2 \leq g_1 \leq g_2 \leq g_3$. If $g_1 \neq 2$ we arrive at the following contradiction

$$\frac{1}{6} + \frac{1}{6} + \frac{1}{6} \geq \frac{1}{2g_1} + \frac{1}{2g_2} + \frac{1}{2g_3} = \frac{1}{g} + \frac{1}{2}.$$

Thus $g_1 = 2$ and we have,

$$\frac{1}{2g_2} + \frac{1}{2g_3} > \frac{1}{4}. \tag{7.32}$$

Clearly g_2 must equal either 2 or 3. If $g_2 = 2$ it is easily shown that $g = 2g_3$. If $g_2 = 3$ we see that $g_3 \in \{3, 4, 5\}$. Assume that g_2 and $g_3 = 3$. Notice that since $g_1 = 2$, 2 must divide the order of G. Recall also that a Sylow p-subgroup of G has order 1, so we assert that $p \neq 2$ and $e = 2$. We see from (7.31) that $|G| = 24$ and thus a Sylow 3-subgroup has order 3. The maximal abelian subgroups conjugate to A_2 or A_3 have order 6 and therefore each contains a Sylow 3-subgroup of G. Let B_2 and B_3 be the Sylow 3-subgroups contained in A_2 and A_3 respectively. Observe that for $i = 2$ or 3,

$$A_i \cong \mathbb{Z}_6 \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \cong B_i \times Z \cong B_i Z. \tag{7.33}$$

Let $b_2 \in B_2$, $b_3 \in B_3$ and $z \in Z$. Recall that B_2 and B_3 are conjugate in G by Sylow's Second Theorem, so there exists an $x \in G$ such that,

$$\begin{aligned} x b_2 x^{-1} &= b_3, \\ x b_2 x^{-1} z &= b_3 z, \\ x b_2 z x^{-1} &= b_3 z. \end{aligned}$$

Since b_2, b_3 and z were chosen arbitrarily, we observe that $B_2 Z$ is conjuagate to $B_3 Z$ and thus by (7.33), $A_2 \cong A_3$. This contradicts the fact that A_2 and A_3 are representatives of different conjugacy classes of maximal abelian subgroups of G, which means that g_2 and g_3 cannot both equal 3. Thus we are left with the following three cases:

$$\begin{aligned} &g_1 = 2, \qquad g_2 = 2, \qquad g = 2g_3. \\ &g_1 = 2, \qquad g_2 = 3, \qquad g_3 = 4. \\ &g_1 = 2, \qquad g_2 = 3, \qquad g_3 = 5. \end{aligned}$$

Case VIa: $g_1 = 2, g_2 = 2, g = 2g_3$. First observe that,

$$[G : N_G(A_1)] = \frac{eg}{2eg_1} = \frac{g_3}{2}.$$

Thus $g_3/2$ is an integer which means that g_3 must be even, call it n. Now let $A_3 = \langle x \rangle$. Since $|A_3| = eg_3$, the order of x is $2n$ and x^n has order 2. By Theorem (**??**)(iv) there exists a $y \in N_G(A_3) \backslash A_3$ such that $yxy^{-1} = x^{-1}$. Also,

$$|\mathcal{C}_3| = [G : N_G(A_3)] = 1.$$

Since $y \notin A_3$ and A_3 has no conjugate subgroups (aside from itself), y must lie in a maximal abelian subgroup conjugate to either A_1 or A_2. This means that since $|A_1| = 4 = |A_2|$ and $y \notin Z$, the order of y must be 4. By the uniqueness of the element of order 2, we have the relation $x^n = y^2$ and G is given by the presentation,

$$G = \langle\, x, y \,|\, x^n = y^2,\, yxy^{-1} = x^{-1} \,\rangle. \qquad \text{(where } n \text{ is even)}$$

Case VIb: $g_1 = 2, g_2 = 3, g_3 = 4$. In this case (7.31) becomes,

$$\frac{1}{4} + \frac{1}{6} + \frac{1}{8} = \frac{1}{g} + \frac{1}{2}.$$

Thus $g = 24$ and $|G| = 48$. Consider the quotient group G/Z of order 24 and the quotient group $N_G(A_2)/Z$ which, for convenience, we will call H.

$$|H| = \frac{2eg_2}{e} = 6.$$

Let x be an element of order 6 from A_2. By Theorem 6.40 there exists a $y \in N_G(A_2) \backslash A_2$ such that $yx = x^{-1}y$. Thus for $xZ, yZ, x^{-1}Z \in H$ we have,

$$yZxZ = yxZ = x^{-1}yZ = x^{-1}ZyZ.$$

If H is abelian, then $xZ = x^{-1}Z$ and thus $x^2 \in Z$. Also, since x has order 6, x^2 has order 3. This is contradiction since there is no element of order 3 in Z. Thus H is non-abelian and is therefore isomorphic to the symmetric group S_3.

Now we determine the normal subgroups of H. The identity and H itself are trivially normal. Furthermore, the elementary result that any subgroup of index 2 is normal implies that A_2/Z, the subgroup of H of order 3, is normal. It remains to check the subgroups of order 2. Let r be a generator of one of the subgroups of order 2 and let x be an arbitrary element of H. If $\langle r \rangle$ is normal in H, then $xrx^{-1} \in \{I, r\}$. Since $r \neq I$ it follows that $xrx^{-1} \neq I$. Alternatively if $xrx^{-1} = r$, then $r \in Z(H)$. By the elementary result that $Z(S_n) = \{I\}$ for $n > 2$, we have that $Z(H) = \{I\}$ and the contradiction $r = I$. Thus $xrx^{-1} \notin \langle r \rangle$ and H has no normal subgroup of order 2. We conclude that the only normal subgroups of H are those of order 1, 3 or 6.

Note that the index of H in G/Z is 4. Let G/Z act by left multiplication on the set of left cosets of H. By Theorem 3.16, this action induces a homomorphism $\phi : G/Z \longrightarrow S_4$ with kernel,

$$ker(\phi) = \bigcap_{x \in G/Z} xHx^{-1} \subset H.$$

Recall the elementary result that the kernel of a homomorphism is a normal subgroup of it's domain. Thus the kernel of ϕ is normal in G/Z and consequently in H as well, that is $ker(\phi) \in \{I, A_2/Z, H\}$.

If $ker(\phi) = A_2/Z$, then $A_2/Z \lhd G/Z$ and by Lemma 7.6 $A_2 \lhd G$. This is a contradiction since the normaliser in G of A_2 is a proper subgroup of G, thus $ker(\phi) \neq A_2/Z$.

If $ker(\phi) = H$, then $H \lhd G/Z$. Take an arbitrary $x \in G/Z$. Since A_2/Z is a subgroup of H we get,

$$x(A_2/Z)x^{-1} \subset H.$$

Furthermore, since A_2/Z has order 3, any subgroup conjugate to it has order 3. Since the only subgroup of H of order 3 is A_2/Z, and since x was chosen arbitrarily, $A_2/Z \lhd G/Z$. We have already shown that this leads to a contradiction, thus $ker(\phi) \neq H$.

We conclude that $ker(\phi) = \{I\}$ and so ϕ is injective. Since G/Z has 24 elements, it's image under ϕ is the whole of S_4, that is $G/Z \cong S_4$. Thus G is a *representation group* of S_4, denoted by $\widehat{S}_4$ (for a full defintion of this, see [**?**]). Suzuki proves that S_4 has 2 distinct representation groups up to isomorphism [**?**, p.301], which are distinguished by the property that the elements corresponding to transpositions have either order 2 or order 4. Since G has a unique element of order 2, it must be isomorphic to the representation group of S_4 in which the transpositions correspond to the elements of order 4, as desired.

Case VIc: $g_1 = 2, g_2 = 3, g_3 = 5$. In this case (7.31) becomes,

$$\frac{1}{4} + \frac{1}{6} + \frac{1}{10} = \frac{1}{g} + \frac{1}{2}.$$

Thus $|g| = 60$ and $|G| = 120$. Observe that a simple relabelling of the maximal abelian subgroups gives the same situation as described in **Case Vd:**. Thus $G \cong \mathrm{SL}_2(5)$, however in this case p does not divide $|G|$.

□

7.3 Dickson's Classification Theorem

We now state the main result of this paper, Dickson's classification of finite subgroups of $\mathrm{SL}_2(F)$. Observe that it is not the focus of this paper to determine whether the following groups actually exist, rather that this theorem can be regarded as an *upper bound*, so to speak, of the only possible subgroups of $\mathrm{SL}_2(F)$.

Theorem 7.14 (Class I)**.** $dicksons_c lassification_t heorem_c lass_I$

Let F be an arbitary algebraically closed field of characteristic p. Any finite subgroup G of $\mathrm{SL}_2(F)$ is isomorphic to one of the following groups.

: When $p = 0$ or $|G|$ is relatively prime to p:

(i) A cyclic group.

(ii) The group defined by the presentation:

$$\langle\, x, y \,|\, x^n = y^2,\, yxy^{-1} = x^{-1} \,\rangle.$$

(iii) The Special Linear Group $\mathrm{SL}_2(3)$.

(iv) The Special Linear Group $\mathrm{SL}_2(5)$.

(v) $\widehat{S}_4$, the representation group of S_4 in which the transpositions correspond to

the elements of order 4.

Proof. case$_I$, $case_I I$, $case_I II$, $case_V ICaseIa : ThisleadstoClassI(i)$.
$CaseIIa : ThisleadstoClassI(ii) where n is odd.$
$CaseIIb : ThisleadstoClassI(iii)$.
$CaseIII where$ G=Z: $ThisleadstoClassI(i)$.
$CaseV Ia : ThisleadstoClassI(ii) where n is even.$
$CaseV Ib : ThisleadstoClassI(v)$.
$CaseV Ic : ThisleadstoClassI(iv)$.

□

Theorem 7.15 (Class II)**.** $dicksons_classification_theorem_class_I IWhen|G|isdivisiblebyp$:

$(vi) Q is elementary abelian, Q \lhd G$ *and* G/Q *is a cyclic group whose order is relatively prime to* p.

(vii) $p = 2$ *and* G *is a dihedral group of order* $2n$*, where* n *is odd.*

(viii) The Special Linear Group $\mathrm{SL}_2(5)$*, where* $p = 3 = q$.

(ix) The Special Linear Group $\mathrm{SL}_2(\mathbb{F}_q)$.

(x) The group $\langle \mathrm{SL}_2(\mathbb{F}_q), d_\pi \rangle$*, where* $\mathrm{SL}_2(\mathbb{F}_q) \lhd \langle \mathrm{SL}_2(\mathbb{F}_q), d_\pi \rangle$.

Here, Q *is a Sylow* p*-subgroup of* G *of order* q*,* $\mathbb{F}_q$ *is a field of* q *elements,* $\mathbb{F}_{q^2}$ *is a field of* q^2 *elements,* $\pi \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ *and* $\pi^2 \in \mathbb{F}_q$.

Proof. case$_I$, $case_I II$, $case_I V$, $case_V$
Case Ib: This leads to Class II (vi).
Case III where $G \neq Z$: This leads to Class II (vi).
Case IVa: This leads to Class II (vii).
Case IVb: This leads to Class II (ix) with $q = 3$.
Case Va: This leads to Class II (ix).
Case Vb: This leads to Class II (x).
Case Vc: This leads to Class II (x) with $q = 3$.
Case Vd: This leads to Class II (viii).

□

Lemma 7.16. *If* $Z \not\subset G$*, then* G *has no element of order 2 and* $|G|$ *is therefore odd. Observe that in Cases II, IV, V and VI,* $|G|$ *is always even, thus we have either Case I or III. These correspond to Class I (i) or Class II (vi).*

Proof. SpecialSubgroups.exists$_u nique_o rderOf_e q_t wo$

□

7.4 Classification of finite subgroups of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$

Theorem 7.17 (Classification of finite subgroup of $\mathrm{PGL}_2(\bar{\mathbb{F}})$)**.** *$dicksons_classification_theorem_class_I, dickson$s
then G is isomorphic to either a cyclic group, a dihedral group, A_4, S_5, A_5, or
is isomorphic to $\mathrm{PSL}_2(k)$ or $\mathrm{PGL}_2(k)$ for some finite field k of characteristic p.*