Galois $SL(2,q)$-Coverings of $\mathbb{P}^1(\mathbb{C}) \setminus \{0,1,\infty\}$

Guido Helmers

Department of
Mathematics

RuG

Master's thesis

Galois $SL(2,q)$-Coverings of $\mathbb{P}^1(\mathbb{C}) \setminus \{0,1,\infty\}$

Guido Helmers

University of Groningen
Department of Mathematics
P.O. Box 800
9700 AV Groningen

December 1999

Contents

Introduction

In this master's thesis I investigate Galois coverings of $\mathbb{P}^1(\mathbb{C})$ which are unbranched outside the set $\{0, 1, \infty\}$ and have Galois group $SL(2, q)$. In the first chapter it is explained very briefly why such coverings are interesting. The second chapter introduces Galois coverings of a topological space and the most elementary properties of such coverings. We also present a classification of Galois G-coverings, and derive from that a classification of Galois G-coverings of $\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$ in terms of so-called admissible triples of the group G. In the last section of chapter 2 it is shown how Galois coverings of a punctured Riemann surface $X \setminus S$ extend to branched coverings of the whole Riemann surface X, and how admissible triples contain all the information about the ramification of these extensions.

The theory from chapter 2 can be put in an algebraic setting. This is done in chapter 3, and in the same chapter we will prove that in the case of smooth irreducible projective curves and finite groups G of automorphisms, Galois G-coverings and quotients by the group G are one and the same thing; this knowledge enables us to construct, in chapter five, some $SL(2, q)$-coverings for small q.

The fourth chapter - which is purely group theoretical in nature - is devoted to the groups $SL(2, q)$. In chapter 3, we have given a classification of the (algebraic) Galois $SL(2, q)$-coverings of the complex projective line, which are unbranched outside $0, 1$ and ∞, in terms of admissible triples of generators of $SL(2, q)$; in chapter 4 it will be shown how the set of admissible triples, modulo equivalence, can be computed explicitly. In the same chapter, some results of Dickson (namely the classification of the subgroups of $SL(2, q)$ and *Dickson's lemma*; the proofs of these results can be found in the appendix) are used to prove the existence of certain admissible triples of $SL(2, q)$.

Since a Galois cover is nothing but a quotient by a group of automorphisms, the question whether $SL(2, q)$ can occur as the Galois group of a map $f : C \to \mathbb{P}^1$ is equivalent with the question whether $SL(2, q)$ can be embedded in $Aut(C)$. We show in chapter 5 that if C has genus 0 or 1, then $SL(2, q)$ is a subgroup of the group of automorphisms of C only if $q = 2$ or 4. We conclude the fifth chapter by constructing, for these q, explicit rational and elliptic $SL(2, q)$-coverings of $\mathbb{P}^1$ with three branch points.

Table of Theorems

Chapter 1

Motivation

This chapter will be used to motivate why it is worthwhile to write a dissertation on coverings of $\mathbb{P}^1$ with three branch points. Hopefully the reader is convinced, after having read the following brief summary of some topics which have been of interest during the last decade, and in which coverings – in particular those of $\mathbb{P}^1$ which are unbranched outside a set of three points – are a tool of great importance.

Dessins d'Enfant: In 1984, Alexander Grothendieck wrote a manuscript, called *Esquisse d'un Programme*, in which he introduced his *dessins d'enfant*. Roughly, these are connected trees on a topological surface, satisfying certain properties. One of Grothendieck's goals was to obtain a complete description of the structure of the group $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ – a group about which not much is known at the moment –, and his idea was to investigate the action of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ on certain sets of dessins. This very complicated action depends on correspondences between dessins d'enfant, algebraic curves over $\overline{\mathbb{Q}}$, and coverings $X \to \mathbb{P}^1(\mathbb{C})$ which are unbranched outside the set $\{0, 1, \infty\}$ (such coverings are called *Belyi morphisms*; the correspondence between curves over $\overline{\mathbb{Q}}$ and Belyi morphisms is a result of Belyi, 1979). During the nineties, lots of mathematicians have been trying to help carry out Grothendieck's proposed programme, in which coverings of the complex projective line with three branch points are one of the main objects of interest. The interested reader can take a look in [De] for more information.

Inverse Galois Theory: The *inverse Galois problem* over the (arbitrary) field K can be stated as follows: Given a finite group G, does there exist a Galois extension L/K, the Galois group of which is isomorphic to G?
In the case $K = \mathbb{C}(t)$ the answer to this question is quite easily shown to be 'yes', for each finite group G. Namely, a finite group G is isomorphic to a quotient of the group π with presentation $< \sigma_1, \ldots, \sigma_n | \sigma_1 \cdot \ldots \cdot \sigma_n = 1 >$, for some $n \geq 1$ (namely, if G is generated by $g_1, \ldots, g_{n-1}$ then we put $g_n := (g_1 \cdot \ldots \cdot g_{n-1})^{-1}$ and define an epimorphism $\pi \to G : \sigma_i \mapsto g_i$). The group π is the fundamental group of the complement of n points $P_1, \ldots, P_n$ in the sphere $\mathbb{P}^1(\mathbb{C})$ (lemma 2.3.1), and the kernel $H := ker(\pi \to G)$ defines (by theorem 1(a)(i) and propositions 2.1.7 and 2.1.8) a Galois G-covering $f : Z \to \mathbb{P}^* :=$

$\mathbb{P}^1(\mathbb{C})\backslash\{P_1,\ldots,P_n\}$. As we mention in section 2.4, there exists a compact Riemann surface Z_c which contains Z as an open subset, and one can extend f to a surjective holomorphic map $F : Z_c \to \mathbb{P}^1(\mathbb{C})$ with the properties that $Aut(Z_c/\mathbb{P}^1(\mathbb{C})) \cong Aut(Z/\mathbb{P}^*)$ and that the corresponding function field extension $\mathcal{M}(Z_c)/\mathcal{M}(\mathbb{P}^1)$ is Galois. Finally, one can show that the covering $F : Z_c \to \mathbb{P}^1(\mathbb{C})$ satisfies $Gal(\mathcal{M}(Z_c)/\mathcal{M}(\mathbb{P}^1(\mathbb{C}))) \cong Aut(Z_c/\mathbb{P}^1(\mathbb{C}))$ (cf. theorem 6). Thus

$$Gal(\mathcal{M}(Z_c)/\mathcal{M}(\mathbb{P}^1(\mathbb{C}))) \cong Aut(Z_c/\mathbb{P}^1(\mathbb{C})) \cong Aut(Z/\mathbb{P}^*) \cong G,$$

in other words $\mathcal{M}(Z_c)$ is a Galois extension of the field $\mathcal{M}(\mathbb{P}^1(\mathbb{C})) \cong \mathbb{C}(t)$ with group G.

The problem becomes more interesting if one replaces $\mathbb{C}(t)$ by $\mathbb{Q}(t)$ or number fields, in particular $K = \mathbb{Q}$. There are purely group theoretical criteria, so-called *rigidity criteria*, which ensure that certain finite groups G can be realized as Galois group over $K = \mathbb{Q}$. The proofs of these also depend on the study of coverings of the Riemann sphere $\mathbb{P}^1(\mathbb{C})$ which are unbranched outside a given finite set of points, together with *descent-methods*, which allow one to transform results about Galois extensions of $\mathbb{C}(t)$ into statements in inverse Galois theory over $\mathbb{Q}$ (or other interesting fields). So nowadays, coverings are unavoidable in inverse Galois theory. An extensive treatment of this subject can be found in [Vo] or [Ma].

Diophantine Problems: Classical in number theory are *diophantine problems*, that is, the question of finding all rational or integer solutions of polynomial equations. The most famous diophantine equation is the *Fermat equation*

$$x^p + y^p = z^p, \tag{FE}$$

(p a positive integer). In 1995, Andrew Wiles succeeded to complete a proof of Fermat's last theorem, which says that (FE) has no nonzero integer solutions if $p > 2$. Many conjectures have been made on the *generalized Fermat equation*

$$Ax^p + By^q = Cz^r, \tag{GFE}$$

(A, B, C nonzero integers, and p, q, r positive integers), and several of these are now known to be true. For instance, in a 1994 paper of Henri Darmon and Andrew Granville [DG], it is proven that the equation (GFE) has only finitely many *proper* integer solutions (that is, solutions x, y, z with g.c.d.$(x, y, z) = 1$) whenever $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$. Besides famous theorems of Minkowski and Faltings, another important ingredient in this proof is the existence of coverings of $\mathbb{P}^1$ with prescribed ramification indices p, q and r above the points $0, 1$ and ∞ respectively. This illustrates that also in arithmetic, the theory of coverings plays an important role.

In the next chapter we start with an overview of the theory of coverings from the topological viewpoint, which everybody with a little knowledge of topology and group theory can understand.

Chapter 2

Coverings of Topological Spaces

The goal of this chapter is to introduce the notion of coverings, in particular Galois coverings, from the topological point of view, and to give a classification of the connected coverings and Galois coverings of a (sufficiently nice) topological space X in terms of subgroups of the fundamental group $\pi_1(X)$ resp. in terms of ordered tuples of generators of the Galois group. The main result will be the classification of the Galois coverings of the space $\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$. In the final section we give this an interpretation in terms of Riemann surfaces. We will not give proofs, since they involve only annoying and lengthy calculations with paths in topological spaces; good references covering the material in this chapter are [Fo], [Fu], [Ja], [Pu1,2] and [V].

2.1 Definitions and Fundamental Properties of Coverings

In this section we make the reader familiar with the notion of coverings of a topological space. We start with a bunch of definitions, and then state some basic results on Galois coverings and on the relationship between automorphism groups and the fundamental group.

Definition 2.1.1
A *(topological) covering* of a topological space X is a pair (Y, f), where Y is a topological space, and $f : Y \to X$ is a continuous map with the property that each $x \in X$ has an open neighborhood U_x such that $f^{-1}(U_x)$ is the disjoint union of open subsets of Y each of which is mapped homeomorphically onto U_x by f. If we fix a point $x_0 \in X$ (from now on called a *base point* of X) and a point $y_0 \in f^{-1}(x_0) \subset Y$, then we say that (Y, y_0, f) is a *pointed covering* of (X, x_0).

An *isomorphism of coverings* $(Y, f) \cong (Y', f')$ is a homeomorphism $g : Y \to Y'$ with $f = f' \circ g$. We write $(Y, y_0, f) \cong (Y', y_0', f')$ if in addition $g(y_0) = g(y_0')$.

The group of *automorphisms* or *deck transformations* of a covering (Y, f) of X is defined to be $Deck(Y/X)$ or $Aut(Y/X) := \{\text{isomorphisms from } (Y, f) \text{ to itself}\}$.

A covering $u : \Omega \to X$ is said to be the *universal covering* of X if Ω is path-connected and simply connected ■

Remark 2.1.2

(a) The group $Aut(Y/X)$ acts on Y and the orbits under its action are contained in the fibers of f. In particular, $Aut(Y/X)$ acts on each of the fibers of f.

(b) If (Y, f) is a covering of a connected space X, then all fibers of f have the same cardinality, say n. (To see this, fix a point $x \in X$. The set $S := \{y \in X | \ | f^{-1}(y) | = | f^{-1}(x) |\}$ is open in X. By applying this to all points whose fibers have cardinality different from that of $f^{-1}(x)$ we see that S must be closed as well. Since X is connected, it follows that $S = X$.) In this case, the covering is said to be an *n-sheeted covering*, and n is called the *degree* of the covering.

(c) If G is a group of homeomorphisms of X acting evenly [1] on X, then the projection map $X \to X/G$ is a covering map. A covering which is (isomorphic to one) of this form is called a *G-covering*. An *isomorphism of G-coverings* is an isomorphism which respects G-actions ■

The following lemma relates G-coverings and so-called Galois coverings.

Lemma 2.1.3

(a) If (Y, f) is a connected G-covering of a space X, then $G \cong Aut(Y/X)$, for each $x \in X$ we have $| f^{-1}(x) | = | G |$, and the action of G on each fiber of f is faithful and transitive [2].

(b) If (Y, f) is a connected covering of a locally connected space X, then $Aut(Y/X)$ acts evenly on Y. If f has a fiber on which $Aut(Y/X)$ acts transitively then the covering is an $Aut(Y/X)$-covering: There is a homeomorphism $Y/Aut(Y/X) \cong X$ so that f is the composition $Y \to Y/Aut(Y/X) \cong X$.

PROOF: Proposition 11.37;38 [Fu] ■

Definition 2.1.4

Let (X, x_0) be a connected topological space with base point, and suppose that G is a group. If (Y, f) is a connected covering of X with the property that $Aut(Y/X)$ acts transitively on $f^{-1}(x_0)$ and G is isomorphic with $Aut(Y/X)$, then (Y, f) is called a *Galois covering* with *Galois group* G, or simply a *Galois G-covering* [3]. The (isomorphism class of the) Galois group of such a covering will be denoted by $Gal(Y/X)$ ■

[1] If G is a subgroup of the group of homeomorphisms of a topological space X, then G acts on X. We say that this action of G is *even* if each $x \in X$ has a neighborhood U such that for all $g, h \in G$ one has $gU \cap hU \neq \emptyset \Rightarrow g = h$. Notice that an even action is fixed-point-free.

[2] That is, for each $x \in X$ and for all $y, y' \in f^{-1}(x)$ there exists exactly one $g \in G$ such that $gy = y'$.

[3] In the case where X is a Riemann surface or an algebraic curve, this terminology is justified by the fact that the corresponding extension of function fields is Galois, and that G is isomorphic to the Galois group of this function field extension. See for instance [Fo] for the Riemann surface case.

This definition implicitly includes that being Galois is independent of the chosen basepoint x_0. Moreover, the notation *Galois G-covering* suggests that a Galois covering is a G-covering; this is indeed true, as proposition 2.1.7 (b) shows, but only if we make some assumptions about our space X.

In the remainder of this chapter, (X, x_0) will denote a connected, locally path-connected and semilocally simply connected pointed space.

In fact, this is no severe restriction on a connected space X. Only very weird spaces which we will not come across do not satisfy the above condition. The first thing to know is that such a space always possesses a (pointed) universal covering (cf. Theorem 13.20 [Fu]), which we will denote by (Ω, ω_0, u); it is always a Galois covering with Galois group isomorphic with $\pi_1(X, x_0)$. The existence of this universal covering is exactly what makes life so easy, since it has the property that it can be lifted to each pointed connected covering space of (X, x_0). More exactly, we have:

Proposition 2.1.5
If (Y, y_0, f) is a connected pointed covering of (X, x_0) then there exists a unique continuous map $g_{y_0} : (\Omega, \omega_0) \to (Y, y_0)$ of pointed spaces which lifts the universal covering. The map g_{y_0} is a covering map, so $(\Omega, \omega_0, g_{y_0})$ is the universal covering of (Y, y_0).

PROOF: Proposition 13.5 [Fu] or Proposition 2.5 [P1] ■

We can attach an algebraic invariant to a connected pointed covering (Y, y_0, f) of (X, x_0), namely the image $f^*(\pi_1(Y, y_0)) \subset \pi_1(X, x_0)$ of $\pi_1(Y, y_0)$ under the map $f^* : [\sigma] \mapsto [f \circ \sigma]$ [4]. This group $f^*(\pi_1(Y, y_0))$, which we will call the *characteristic subgroup* of (Y, y_0, f) (notation $Char(Y, y)$), is indeed an invariant of connected (pointed) coverings, as the following proposition shows.

Proposition 2.1.6
Between two connected pointed coverings (Y, y, f) and (Y', y', f') of (X, x_0) exists an isomorphism preserving base points if and only if the characteristic subgroups of the pointed coverings are equal. The two pointed coverings are isomorphic if and only if the characteristic subgroups are conjugate in $\pi_1(X, x_0)$.

PROOF: The first statement is the *Eindeutigkeitssatz*, P.176 [Ja]. The second statement follows from the first; it is proven in [Fu], chapter 13 ■

Another consequence of our assumption about the space X is:

Proposition 2.1.7
a) A connected covering $f : (Y, y) \to (X, x_0)$ is Galois if and only if one of the following holds:

[4] The group $f^*(\pi_1(Y, y_0))$ is in fact isomorphic to the group $\{\phi \in Aut(\Omega/X) | g_{y_0} \circ \phi = g_{y_0}\} = Aut(\Omega/Y) \subset Aut(\Omega/X)$.

(i) $Char(Y,y) \lhd \pi_1(X,x_0)$;

(ii) $Aut(Y/X)$ *acts transitively on* $f^{-1}(x_0)$;

(iii) $Aut(Y/X)$ *acts transitively on all fibers of* f.

b) If $f : (Y,y) \to (X,x_0)$ *is a Galois covering then it is a* G*-covering, where* $G = Gal(Y/X)$. *Conversely, each connected* G*-covering of* X *is Galois.*

PROOF: Section 13.4 [Fu] ■

The final result of this section links the fundamental group and the automorphism group of a covering.

Proposition 2.1.8
If $f : (Y,y) \to (X,x_0)$ *is a connected pointed covering, and* N *denotes the normalizer of* $Char(Y,y)$ *in* $\pi_1(X,x_0)$ [5], *then*

$$N/Char(Y,y) \cong Aut(Y/X).$$

PROOF: Theorem 13.11 [Fu] ■

2.2 Classification of Coverings

In this section we present some classifications of coverings, in particular of Galois coverings, modulo isomorphism, and modulo so-called *equivalence*. It is convenient to redefine Galois G-coverings as follows:

Definition 2.2.1
Fix a group G. A *Galois* G*-covering* of the space X is a triple (Y,f,τ), where (Y,f) is a Galois G-covering in the sense of definition 2.1.4, and $\tau : G \to Gal(Y/X)$ is a fixed group isomorphism. The set of Galois G-coverings of X will be denoted by $GalCov(G)$.

Let $\Gamma := (Y,f,\tau)$ and $\Gamma' := (Y',f',\tau')$ be two Galois G-coverings of a space X. We say that Γ and Γ' are *isomorphic* ($\Gamma \cong \Gamma'$) if $(Y,f) \cong (Y',f')$ (see definition 2.1.1(b)). Moreover, Γ and Γ' are said to be *equivalent*[6] ($\Gamma \sim \Gamma'$) if there is an isomorphism $\Phi : \Gamma \cong \Gamma'$ with the property $\Phi \circ \tau(g) = \tau'(g) \circ \Phi$, for all $g \in G$ ■

Theorem 1
[7] *Let* X *be a connected, locally path-connected and semilocally simply connected topological space, with universal covering* (Ω,u). *Fix a base point* $x_0 \in X$ *and a base point* $\omega_0 \in \Omega$ *lying over* x_0. *Denote by* π *the fundamental group* $\pi_1(X,x_0)$ *of* X.

[5] i.e. the largest subgroup of $\pi_1(X,x_0)$ in which $Char(Y,y)$ is normal.
[6] In [Fu], this is called *G-isomorphic*.
[7] Notice the similarity between this theorem and the main theorem of Galois theory for fields.

(a) **(Classification of the connected coverings)**
There are bijections

(i) $\left\{ \begin{array}{c} \text{connected pointed} \\ \text{coverings of } (X, x_0) \end{array} \right\} \Big/ \begin{array}{c} \text{base point preser-} \\ \text{ving isomorphism} \end{array} \overset{1-1}{\longleftrightarrow} \{\text{subgroups of } \pi\};$

(ii) $\{\text{connected coverings of } X\}$ / *isomorphism* $\overset{1-1}{\longleftrightarrow} \{\text{subgroups of } \pi\}$ / $Inn(\pi)$.

(b) **(Classification of the Galois coverings)**
Fix a group G which is isomorphic to the quotient π/H, for some subgroup H of π. The group $Aut(G)$ acts on $Epi(\pi, G)$ by the rule $\alpha(\phi)([\sigma]) := \alpha(\phi([\sigma]))$, with $\alpha \in Aut(G)$ and $\phi \in Epi(\pi, G)$.

(i) There are bijections

$$GalCov(G)/\text{isomorphism} \overset{1-1}{\longleftrightarrow} \{H \lhd \pi \mid \pi/H \cong G\} \overset{1-1}{\longleftrightarrow} Epi(\pi, G)/Aut(G).$$

(ii) Modulo equivalence, the Galois G-coverings are classified by

$$GalCov(G)/\text{equivalence} \overset{1-1}{\longleftrightarrow} Epi(\pi, G)/Inn(G).$$

PROOF: (a) Proposition 2.1.6 shows that (the conjugacy class of) the characteristic subgroup defines an injective map to the right; it can be shown that this map is surjective too.

(b) (i): The first bijection follows from (a)(ii) and the fact that a characteristic subgroup of a Galois cover has no conjugates but itself, since it is normal in π. Furthermore, one easily shows that two maps in $Epi(\pi, G)$ have the same kernel exactly when they differ by an automorphism of G, so the second bijection is given by $\phi \mapsto ker(\phi)$.

(ii): The proof of this part depends on an action of $\pi_1(X, x_0)$ on Y which is described in the proof of Theorem 13.11 [Fu]; We won't go into the details here ■

2.3 Classification of Galois Coverings of $\mathbb{P}^1(\mathbb{C})\setminus\{0,1,\infty\}$

We denote by $\mathbb{P}^*$ the topological space $\mathbb{P}^1(\mathbb{C}) \setminus \{0,1,\infty\}$, the topology being the one induced by the classical topology on $\mathbb{C}$. Since, in the following chapters, we are interested only in the Galois coverings of $\mathbb{P}^*$ with a fixed finite Galois group G, we will now classify these Galois coverings. All we have to do is compute the fundamental group of $\mathbb{P}^*$ (which from now on will be abbreviated by π).

Lemma 2.3.1
The fundamental group π of $\mathbb{P}^*$ has presentation $<a_0, a_1, a_\infty \mid a_0 a_1 a_\infty = 1>$.
In general, if $S = \{P_1, \ldots, P_n\}$ is a finite subset of $\mathbb{P}^1(\mathbb{C})$, then

$$\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus S) =< a_1, \ldots, a_n \mid a_1 \cdot \ldots \cdot a_n = 1 >,$$

where the a_i are nonintersecting loops, based at a fixed point P_0 outside S, winding once around P_i in counterclockwise direction.

PROOF:[8] Identify $\mathbb{P}^*$ with the complement of the north and south pole (N and S) and 1 in the sphere S^2. Choose open discs $D_1 \subsetneq D_2 \subset S^2$ centered at N, not containing 1, and let $x \in D_2 \setminus D_1$ be the base point of S^2. Using stereographic projection to $\mathbb{R}^2$ (in this space fundamental groups are easy to find), it follows that $\pi_1(S^2 \setminus (D_1 \cup \{S, 1\}), x) =<a_1, a_\infty>$ where a_1 and a_∞ are simple loops based at x around 1 and S. If a_0 is a simple loop in $D_2 \setminus D_1$ with winding number 1 around N, then $\pi_1(D_2 \setminus D_1, x) = \pi_1(D_2 \setminus \{N\}, x) =<a_0>$. By reversing some orientations if necessary, we may assume that a_0 has image $(a_1 a_\infty)^{-1}$ in $\pi_1(S^2 \setminus (D_1 \cup \{S, 1\}), x)$, so that Seifert and van Kampen imply

$$\pi_1(\mathbb{P}^*) \cong \pi_1(S^2 \setminus \{N, S, 1\}, x) \cong <a_0> \star_{<a_0>} <a_1, a_\infty> \cong <a_0, a_1, a_\infty \mid a_0 a_1 a_\infty = 1> .$$

This is independent of the base point since $\mathbb{P}^*$ is path-connected. The generalization follows by induction ■

This result, together with the classification theorem of the previous section, leads to a nice classification of the Galois covers of $\mathbb{P}^*$. First, we introduce the notion of *admissible systems of generators* of a group G.

Definition 2.3.2
Let a finite group G and a triple (n_1, n_2, n_3) of positive integers be given. An ordered triple (g_1, g_2, g_3) in $G \times G \times G$ is called *admissible with respect to* (n_1, n_2, n_3) if the g_i generate G, $ord(g_i) = n_i$, and $g_1 g_2 g_3 = 1$. Two such admissible triples (g_1, g_2, g_3) and (h_1, h_2, h_3) are called *equivalent* (resp. *quasi-equivalent*) if there exists an $\alpha \in Inn(G)$ (resp. $\alpha \in Aut(G)$), such that $\alpha(g_i) = h_i$, for $i = 1, 2, 3$. The set of admissible systems of generators of G w.r.t. (n_1, n_2, n_3) will be denoted $Adm(G, (n_1, n_2, n_3))$ ■

Theorem 2
(Classification of the Galois coverings of $\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$)
In the notations of theorem 1, the Galois covers of $\mathbb{P}^*$ with group G are classified as follows:

(i) $GalCov(G)/\cong \overset{1-1}{\longleftrightarrow} \bigcup_{(n_1,n_2,n_3)} (Adm(G, (n_1, n_2, n_3))/quasi\text{-}equivalence)$.

(ii) $GalCov(G)/\sim \overset{1-1}{\longleftrightarrow} \bigcup_{(n_1,n_2,n_3)} (Adm(G, (n_1, n_2, n_3))/equivalence)$.

[8] There are other ways to prove this lemma, see for example Corollary 4.29, P.81 [Vo].

PROOF: Since $\pi =< a_1, a_2, a_3 \mid a_1a_2a_3 >$, the sets $Epi(\pi, G)$ and

$$\{(g_1, g_2, g_3) \in G^3 \mid g_1g_2g_3 = 1 \text{ and } < g_1, g_2 >= G\}$$

can be identified, by sending ϕ to the triple $(\phi(a_1), \phi(a_2), \phi(a_3))$. This identification respects the action of $Aut(G)$, so this theorem is nothing but theorem 1(b) ■

We can of course generalize this theorem by replacing $0, 1, \infty$ by an arbitrary finite number n of points in $\mathbb{P}^1(\mathbb{C})$, and by adjusting the definition of admissible systems of generators.

2.4 Branched Coverings of Riemann Surfaces

One can show that each covering $f^* : X^* \to Y \setminus S$ of a punctured Riemann surface (i.e. the complement of a closed discrete set S of points in a Riemann surface Y) extends to a proper holomorphic map $f : X \to Y$, where X is a Riemann surface containing X^* as an open subset. Such an extension is called a *branched covering* of Y. When Y is taken to be the Riemann sphere, and (X^*, f^*) is Galois, it will turn out that the ramification indices of the holomorphic map f can be read off from the admissible n-tuple of generators corresponding to (X^*, f^*) (theorem 2). References for this section are [Fo], [Fu] and [Vo].

A *Riemann surface* is a connected one-dimensional complex manifold equipped with a complex structure - see [Fo]. We start with some definitions on ramification of analytic maps between Riemann surfaces.

Definition 2.4.1
Let $f : X \to Y$ be an analytic map between Riemann surfaces. Suppose that at $P \in X$ the map f locally has the form $z \mapsto \Sigma_{n=1}^{\infty} a_n z^n$. The *ramification index of f at P* is the number $e_f(P) := min\{n \geq 1 \mid a_n \neq 0\}$, and P is said to be a *ramification point* of f if $e_f(P) > 1$. A point $Q \in Y$ is a *branch point* if the fiber $f^{-1}(Q)$ contains a ramification point ■

The first result of this section is the fact that a connected topological covering of a punctured Riemann surface can be extended to a proper analytic map of Riemann surfaces. First we need to know what a *proper* map is.

Definition 2.4.2
A continuous map $f : X \to Y$ between topological spaces is said to be *proper* if the preimage of each compact set in Y is again a compact set ■

Proposition 2.4.3
Let Y be a Riemann surface, S a closed discrete subset of Y and $Y^* := Y \setminus S$. Suppose that $f^* : X^* \to Y^*$ is a finite-sheeted connected covering. Then there exists a Riemann surface X which contains X^* as an open subset, such that $X \setminus X^*$ is finite, and there exists

a proper analytic mapping $f : X \to Y$ which extends f^*.
The pair (X, f) is unique in the following sense: If (X', f') is another pair with the above properties, then there exists a unique biholomorphic map $\phi : X \to X'$ with $f = f' \circ \phi$.

PROOF: See Satz I.8.4, Satz I.8.5, P.47,48 [Fo] ■

We want the extensions of topological coverings mentioned in the above proposition to be branched coverings, so the following definition is the most natural one:

Definition 2.4.4
A *branched covering* of a Riemann surface Y is a pair (X, f), where X is a Riemann surface and f is a proper surjective holomorphic map from X to Y. We call a branched covering (X, f) of Y, unbranched outside a closed discrete subset $S \subset Y$, *Galois*, if the restriction $(X \setminus f^{-1}(S), f_|)$ is Galois in the topological sense ■

If we take only *compact* Riemann surfaces into consideration, then a branched covering restricts to a connected topological covering of the set of unbranched points, as the next proposition shows:

Proposition 2.4.5
Let $f : X \to Y$ be a nonconstant holomorphic map between compact Riemann surfaces. Denote by $B \subset Y$ and $R := f^{-1}(B) \subset X$ the sets of branch points respectively ramification points of f. Then B and R are finite, and the restriction $f_| : X \setminus R \to Y \setminus B$ is a finite-sheeted connected covering.
If $f_|$ has n sheets then for each $Q \in Y$ we have

$$\Sigma_{P \in f^{-1}(Q)} e_f(P) = n.$$

PROOF: Proposition 19.3, P.266 [Fu] ■

As a consequence, we have the following very nice description of branched coverings of compact Riemann surfaces:

Lemma 2.4.6
Let Y be a compact Riemann surface. A branched cover of Y is the same as a pair (X, f), where X is a compact Riemann surface and $f : X \to Y$ is nonconstant holomorphic.

PROOF: If (X, f) is a branched cover, then X is compact because f is proper. Conversely, if $f : X \to Y$ is a nonconstant holomorphic map between compact Riemann surfaces, then f is surjective by proposition 2.4.5. To show that f is proper, we need two topological facts, namely that a compact subspace of a Hausdorff space is closed, and that a closed subspace of a compact space is compact (see section 1.8 [Ja]). We apply this by using the compactness of X and Hausdorffness of Y: If $V \subset Y$ is compact, then V must be closed, hence $f^{-1}(V)$ is closed and therefore compact as well! ■

In this section we have seen thus far, that a branched covering of a compact Riemann surface Y can be defined as a pair (X, f) where X is a compact Riemann surface, and $f : X \to Y$ is a nonconstant holomorphic map. Each such branched covering, which has branch locus $S \subset Y$, restricts to a connected topological covering of $Y \setminus S$, and each connected topological covering of $Y \setminus S$ extends to a branched covering of Y which is determined up to biholomorphic equivalence. In the sequel, we call branched coverings simply *coverings* or *covers*.

To conclude this chapter, we take a look at the extensions of the topological Galois coverings of $\mathbb{P}^* = \mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$, and we show how the orders of the elements of an admissible triple are related to the ramification indices of the corresponding branched covering map.

Proposition 2.4.7
Let $f : X \to \mathbb{P}^1(\mathbb{C})$ be a Galois cover, which is unbranched outside the set $S := \{0, 1, \infty\}$. Let (g_0, g_1, g_∞) be an admissible triple corresponding to the restriction $f_| : X^* := X \setminus f^{-1}(S) \to \mathbb{P}^*$.

a) *The ramification index $e_f(Q)$ is constant on the fibers of f (this follows from the Galois property). Therefore we will simply speak of the ramification index of f at a point $P \in \mathbb{P}^1(\mathbb{C})$, and denote it by $e_f(P) := e_f(Q)$, where $Q \in f^{-1}(P) \subset X$;*

b) *We have $e_f(P) = ord(g_P)$, for $P = 0, 1, \infty$ (this is well-defined, since the order function is constant on quasi-equivalence classes of admissible triples);*

c) *Each element ϕ^* of $Aut(X^*/\mathbb{P}^*)$ extends uniquely to an* analytic automorphism *ϕ of $f : X \to \mathbb{P}^1(\mathbb{C})$, i.e. a biholomorphic map $\phi : X \to X$ with $f \circ \phi = f$. Conversely, each analytic automorphism of $f : X \to \mathbb{P}^1(\mathbb{C})$ arises in this way. The group of analytic automorphisms of $f : X \to \mathbb{P}^1(\mathbb{C})$ will be denoted by $Aut_{an}(X/\mathbb{P}^1(\mathbb{C}))$; it is of course isomorphic with $Aut(X^*/\mathbb{P}^*)$.*

PROOF: See for example Chapter 5 [Vo] ■

One can show that the quotient of X by $Aut_{an}(X/\mathbb{P}^1(\mathbb{C})$ has a unique structure of Riemann surface for which the quotient map π is analytic. Furthermore, there is a biholomorphic map $\Phi : X/Aut_{an}(X/\mathbb{P}^1(\mathbb{C})) \to \mathbb{P}^1(\mathbb{C})$ such that $f = \Phi \circ \pi$. So a Galois covering of $\mathbb{P}^1(\mathbb{C})$ which restricts to an unbranched cover of $\mathbb{P}^*$ is nothing but a quotient by a finite subgroup G of the group of analytic isomorphisms of X, and to such a covering corresponds a unique (quasi-)equivalence class of admissible triples of G; the orders of such a class of triples describe exactly the ramification indices of this branched covering map.

We have thus given theorem 2 an interpretation in terms of branched coverings of Riemann surfaces, and related the order function to the ramification index. In the next chapter we will generalize some of these ideas to projective algebraic curves over arbitrary fields, instead of just over $\mathbb{C}$.

Chapter 3

Coverings of Algebraic Curves

It is well-known that complex projective curves and compact Riemann surfaces are essentially one and the same thing. Therefore we can ask ourselves the question if the theory of coverings of Riemann surfaces has an analogue in terms of algebraic geometry (where the base field need no longer be the field of complex numbers!). In this chapter we will give an answer to this question. We fix an algebraically closed field $K = \bar{K}$ throughout. All varieties are assumed to be irreducible algebraic varieties over K (notation: V/K), and all curves are, in addition, assumed to be nonsingular.

3.1 Translation to Algebraic Curves

We will define coverings of algebraic curves, and recall some properties of algebraic curves. For proofs, we refer to Chapter 2 [Si]. The next theorem is part of J-P. Serre's paper GAGA (Géométrie algébrique et géométrie analitique, 1956).

Theorem 3
There is a functor an, from the category of complex projective curves and algebraic morphisms to the category of compact Riemann surfaces and analytic maps, which is an equivalence of categories ■

For a discussion, see Section 3.6 [P2]. By this result and lemma 2.4.6, the following definition makes sense:

Definition 3.1.1
An (algebraic) *covering* of a projective curve C_2/K is a pair (C_1, f) consisting of a projective curve C_1/K and a nonconstant morphism $f : C_1 \to C_2$ ■

The map f is automatically surjective, and it induces an injection of function fields

$$f^\sharp : K(C_2) \hookrightarrow K(C_1) : g \mapsto g \circ f,$$

which is of finite degree. This degree is called the *degree* of f.

Definition 3.1.2
A *Galois G-covering* (or simply *Galois covering*) of the curve C_2/K is a triple (C_1, f, τ), where (C_1, f) is a covering of C_2 with the property that the extension $K(C_1)/K(C_2)$ is Galois, and τ is an isomorphism from the group $Aut(C_1/C_2) := \{\text{isomorphisms } \Phi : C_1 \to C_1 \text{ with } f \circ \Phi = f\}$ onto the group G ■

We will see in theorem 6 that G is isomorphic to $Gal(K(C_1)/K(C_2))$.

Definition 3.1.3
In analogy with definition 2.1.1, we define two covers (C_1, f) and (C_1', f') to be *isomorphic* (notation $\cong$), if there is an isomorphism of curves $\Phi : C_1 \to C_1'$ with $f = f' \circ \Phi$. Two Galois G-covers (C_1, f, τ) and (C_1', f', τ') are *equivalent* [1] (notation $\sim$), if there is an isomorphism $\Phi : (C_1, f) \to (C_1', f')$ with $\Phi \circ \tau^{-1}(g) = (\tau')^{-1}(g) \circ \Phi$, for all $g \in G$ ■

Fix a projective curve C. Recall that, by the hypothesis of nonsingularity, for each $P \in C$, the local ring $K[C]_P$ is a discrete valuation ring (DVR) (i.e. a local PID). A *local parameter* at P is a generator t_P of the maximal ideal $\mathfrak{m}_P$ of $K[C]_P$. The *order function* $v_P : K(C)^* \to \mathbb{Z}$ defined by $g \mapsto max\{k \in \mathbb{Z} \mid g \in K[C]_P \cdot t_P^k\}$ does not depend on t_P, and defines a discrete valuation on the function field $K(C)$. One can generalize the notion of ramification of maps of Riemann surfaces to algebraic curves, as follows:

Definition 3.1.4
Let $f : C_1 \to C_2$ be a nonconstant morphism of projective curves over K, and let $P \in C_1$. The *ramification index* of f at P is the positive integer

$$e_f(P) := v_P(f^\sharp(t_{f(P)})).$$

We say that f is *tamely ramified* at P if either $char(K) = 0$, or $e_f(P)$ and $char(K)$ are relatively prime. Otherwise the ramification is called *wild* ■

One can show that, in the case that $K = \mathbb{C}$, all the definitions made in this section are in harmony with the corresponding definitions for Riemann surfaces. For example, the function field $\mathbb{C}(C)$ of a complex projective curve C is isomorphic to the field $\mathcal{M}(C_{an})$ of meromorphic functions on the corresponding Riemann surface C_{an}, and the algebraic and analytic definition of ramification index agree, etc.

Furthermore, the classification theorem 2 of topological Galois coverings of $\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$ has the following algebraic analogue:

Theorem 4
The set of Galois G-covers of the algebraic curve $\mathbb{P}^1(\mathbb{C})$ *which are unbranched outside* $0, 1$ *and* ∞, *modulo equivalence, is in bijection with the set*

$$\bigcup_{(n_1,n_2,n_3),n_i \geq 1} (Adm(G, (n_1, n_2, n_3))/equivalence).$$

[1] In [Sh], this is called C_2-*isomorphic*.

If (C_1, f, τ) mod $\sim$ *corresponds to the triple* (g_1, g_2, g_3) mod $\sim$, *the ramification index* $e_f(P)$ *at* $P = 0$ *(resp.* $P = 1, \infty$*) equals* $ord(g_1) = n_1$ *(resp.* $ord(g_2) = n_2$, $ord(g_3) = n_3$*).*

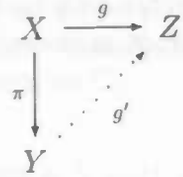
PROOF: P.117 [Sh] ■

3.2 Quotients of Curves by Finite Groups of Automorphisms

In section 2.4 we have already encountered the fact, that a Galois covering $f : X \to \mathbb{P}^1(\mathbb{C})$ with Galois group G identifies $\mathbb{P}^1(\mathbb{C})$ with the orbits of G on X. Here we will show that something more general holds: Each Galois covering of a projective curve Y is a quotient of a projective curve X by a finite subgroup G of $Aut(X)$. By a quotient we mean the following:

Definition 3.2.1
Let X be an variety, and suppose that $G \subset Aut(X)$ is a finite subgroup. A *quotient of* X *by* G is a pair (Y, π), where Y is a variety, and $\pi : X \to Y$ is a surjective morphism which identifies the points of Y with the G-orbits on X (i.e. $\forall\, x \in X$ we have $\pi^{-1}(\pi(x)) = \{g(x) \mid g \in G\}$), such that the following universal mapping property is satisfied:

(UMP Quotient) For each variety Z and morphism $g : X \to Z$, there is a morphism $g' : Y \to Z$ with $g = g' \circ \pi$, exactly when g is constant on the G-orbits.



It is clear how one defines isomorphy of quotients ■

Notice that if we speak of a quotient of a variety V by a finite group G, an action of G on V (i.e. an embedding $G \hookrightarrow Aut(V)$) must be specified. Thus distinct actions of a finite group G on V may define non-isomorphic quotients of V.

We have defined quotients for varieties in general, since the standard proof of the following result is no more difficult than for the special case of projective curves.

Theorem 5
The quotient of a projective variety X *by a finite subgroup* $G \subset Aut(X)$ *always exists. It is again projective, and it is unique up to isomorphism; we denote it by* X/G.

PROOF: Chapter 10 [Harr] ■

We continue with a lemma which allows us to convert questions about curves into questions about function fields, which are usually easier to solve because of the presence of the classical Galois theory.

Lemma 3.2.2

a) *There is a functor $\mathcal{F}$ from the category of smooth projective curves over k and surjective morphisms to the category of one-dimensional function fields over k and k-injections, which is an arrow-reversing equivalence of categories.*

b) *Similarly, there is an equivalence from the category of curves over k and nonconstant rational maps, to the same category of one-dimensional function fields over k.*

c) *A rational map from a curve to an arbitrary variety is defined at each smooth point. In particular, rational maps from a smooth curve to a variety are morphisms.*

PROOF: a) The functor $\mathcal{F}$ maps a curve C to $\mathcal{F}(C) := k(C)/k$; And a morphism $g : C \to D$ is mapped to the comorphism $\mathcal{F}(g) := g^\sharp : k(D) \hookrightarrow k(C) : \phi \mapsto \phi \circ g$. Corollary I.6.12 [Hart] shows that $\mathcal{F}$ is an equivalence of categories.
b) See Corollary I.6.12 [Hart].
c) See Proposition II.2.1 [Si] ■

The algebraic analogue of corollary 2 of proposition 2.1.8 now sounds as follows:

Theorem 6

a) *Let (C_1, f) be a Galois covering of the projective curve C_2/k (the isomorphism to the Galois group is of no importance here). Denote by K_i the function field $k(C_i)/k$, for $i = 1, 2$, and set $G := Gal(K_1/K_2)$. Then $Aut(C_1/C_2) \cong G$, and the covering $f : C_1 \twoheadrightarrow C_2$ equals the quotient $\pi : C_1 \twoheadrightarrow C_1/Aut(C_1/C_2)$.*[2]

b) *Conversely, for any smooth irreducible projective curve C_1/k and for each finite subgroup $G \leq Aut(C_1)$, the quotient C_1/G is again a smooth irreducible projective curve, and $\pi : C_1 \to C_1/G$ is a Galois covering.*

PROOF: a) An immediate consequence of lemma 3.2.2 (a) is that the groups of maps in the top rows of the following two diagrams, making these diagrams commute, are isomorphic:

$$\begin{array}{ccc} C_1 & \overset{\phi}{\cdots\!\!\twoheadrightarrow} & C_1 \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ C_2 & \xrightarrow[id]{} & C_2 \end{array} \qquad \overset{\mathcal{F}}{\rightsquigarrow} \qquad \begin{array}{ccc} K_1 & \overset{\phi^\sharp}{\twoheadleftarrow\!\!\cdots} & K_1 \\ {\scriptstyle f^\sharp}\uparrow & & \uparrow{\scriptstyle f^\sharp} \\ K_2 & \xleftarrow[id]{} & K_2. \end{array}$$

In other words, $Aut(C_1/C_2) \cong G$. In the sequel we identify these two groups. Notice that we have hereby shown that $f : C_1 \to C_2$ is a Galois G-covering, $G = Gal(K_1/K_2)$.

We need to show that C_2 satisfies the universal mapping property of the quotient of C_1 by G. The first task is to show that the fibers of f coincide with the G-orbits on C_1. To this end, we include the following short digression on DVRs.

[2] More precisely, there is an isomorphism $\Phi : C_1/G \to C_2$ with $\Phi \circ \pi = f$.

For the moment, we let C, C_1, C_2 denote arbitrary (nonsingular projective) curves over k. Recall that a subring $R \subset k(C)$ is a DVR (or *place ring*) of the function field $k(C)/k$ if and only if $k \subsetneq R \subsetneq k(C)$, and $x \notin R \Rightarrow x^{-1} \in R$, for all $x \in k(C)$. The set of DVRs of a function field K/k will be denoted by $\mathbb{P}_{K/k}$, or $\mathbb{P}_K$ (do not confuse this with the projective line $\mathbb{P}^1(K)$ over K). Since we consider nonsingular curves, the map $\mathcal{G} : C \to \mathbb{P}_{k(C)} : P \mapsto R_P := k[C]_P$ (local ring at P) is a bijection. Further, the maps $C \mapsto k(C)$ and $[f : C_1 \to C_2] \mapsto [restrict : \mathbb{P}_{k(C_1)} \to \mathbb{P}_{k(C_2)}]$ (where $k(C_2)$ is identified with a subfield of $k(C_1)$ via the comorphism $f^\sharp : g \mapsto g \circ f$, and $restrict(R) := R \cap k(C_2)$) define an equivalence from the category of (nonsing. projective) algebraic curves over k to the category of *abstract curves over* k (section I.6 [Hart]). We denote this functor also by $\mathcal{G}$.

A finite subgroup H of $Aut_k(C)$ and its image $L := \mathcal{F}(H) \subset Aut(k(C)/k)$ naturally define actions on C resp. $\mathbb{P}_{k(C)}$. Indeed, if $R \subset k(C)$ is a place ring, and $\psi \in L$, then

$$x \notin \psi(R) \Rightarrow \psi^{-1}(x) \notin R \Rightarrow (\psi^{-1}(x))^{-1} \in R \Rightarrow x^{-1} = \psi((\psi^{-1}(x))^{-1}) \in \psi(R)$$

shows that $\psi(R)$ is a place ring of $k(C)/k$ as well. Notice that

$$\text{for all } \phi \in H \text{ and } P \in C \text{ we have: } \mathcal{F}(\phi)(R_P) = R_{\phi(P)}. \tag{3.1}$$

Also, for a nonconstant morphism of curves $f : C_1 \to C_2$ we have

$$\mathcal{G} \circ f = restrict \circ \mathcal{G} : C_1 \to \mathbb{P}_{k(C_2)}, \tag{3.2}$$

because for all $P \in C_1$, there holds $R_{f(P)} = R_P \cap k(C_2)$.

We return to our Galois G-cover $f : C_1 \to C_2$. Recall that we have identified $Aut(C_1/C_2)$ with $G = Gal(K_1/K_2)$. The following list of equivalent conditions shows that indeed the fibers of f coincide with the G-orbits on C_1. Let P and Q be two points on C_1.

$$\begin{aligned}
f(P) = f(Q) &\overset{\mathcal{G} \text{ bijective}}{\Leftrightarrow} \mathcal{G}(f(P)) = \mathcal{G}(f(Q)) \\
&\overset{(3.2)}{\Leftrightarrow} restrict(R_P) = restrict(R_Q) \\
&\overset{(\star)}{\Leftrightarrow} \exists\, g \in G \text{ with } g(R_P) = R_Q \\
&\overset{(3.1)}{\Leftrightarrow} \exists\, g \in G \text{ with } R_{g(P)} = R_Q \\
&\overset{\mathcal{G} \text{ bijective}}{\Leftrightarrow} \exists\, g \in G \text{ with } g(P) = Q.
\end{aligned}$$

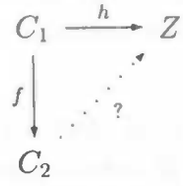
It only remains to verify $(\star)$. This follows from the assumption that K_1/K_2 is Galois: On the one hand, if $R \in \mathbb{P}_{K_1}$ and $g \in G$, then R and $g(R)$ lie over the same place ring in $\mathbb{P}_{K_2}$, since

$$g(R) \cap K_2 = g(R \cap K_2) = R \cap K_2.$$

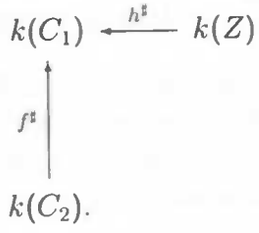
The converse direction is equivalent with saying that G acts transitively on the set of extensions in K_1 of a place ring S, for each $S \in \mathbb{P}_{K_2}$. The latter is shown in Theorem III.7.1 [St] [3]. We conclude that the fibers of f are exactly the G-orbits on C_1.

[3] As follows: Suppose that R and R' restrict to the same DVR S, but $\phi(R) \neq R'$ for all $\phi \in G$. Denote by N the norm map $N_{K_1/K_2} : K_1 \to K_2$. By the approximation theorem, there exists $z \in K_1$ with $v_{R'}(z) > 0$, and $v_Q(z) = 0$ for all $Q \neq R'$ lying over S. A computation shows that this z has the property $v_R(N(z)) = 0 < v_{R'}(N(z))$, contradicting the equivalence $v_R(x) = 0 \Leftrightarrow v_S(x) = 0 \Leftrightarrow v_{R'}(x) = 0$, which holds for all $x \in K_2$.

To complete the proof of a), we must show that the following diagram of k-morphisms of curves



can be completed to a commutative triangle, whenever h is G-invariant. The equivalent picture in the function field category is



Notice that by assumption C_1 and C_2 are irreducible projective smooth curves, but about Z (which at first sight should denote an arbitrary variety!) we do not know much. We can replace Z by the image of h, so that h becomes surjective, and Z becomes an irreducible (and even complete) curve. But Z need not be smooth projective.

We assume however, that $f : C_1 \to C_2$ is Galois, i.e. $k(C_1)/k(C_2)$ is Galois, in other words $k(C_2) = k(C_1)^G$. Because of G-invariance of h, we obtain $h \circ g = h \ \forall g \in G \Rightarrow g \circ h^\sharp = h^\sharp \ \forall g \in G \Rightarrow g \circ h^\sharp(\phi) = h^\sharp(\phi) \ \forall g \in G$. So $k(Z)$ can be identified with a subfield of the subfield of G-invariants of $k(C_1)$, i.e. $k(Z)$ can be injected into $k(C_2)$. Lemma 3.2.2 (b) shows that this inclusion induces a nonconstant rational map r from C_2 to Z. Lemma 3.2.2 (c) shows that r is necessarily a morphism.

b) As before, the problem can be translated to the category of function fields over k. We define L to be the subfield $K(C_1)^G$, and C_2 the smooth projective curve corresponding to the function field L. The inclusion $L \hookrightarrow K(C_1)$ determines a surjective morphism $f : C_1 \to C_2$, and by Artin's theorem (Theorem 11.3 [Ga]) the extension $K(C_1)/L$ is Galois with group G. So $f : C_1 \to C_2$ is a Galois G-covering. Now we just apply a), and conclude that this Galois G-covering is in fact the quotient of C_1 by G we started with ■

In sum, for smooth irreducible projective curves, quotients by finite groups of automorphisms and Galois coverings are one and the same thing. The quotient $C_1 \to C_1/G$, with $G \leq Aut(C_1)$, has the property $G = Aut(C_1/(C_1/G)) \cong Gal(K(C_1)/K(C_1/G))$.

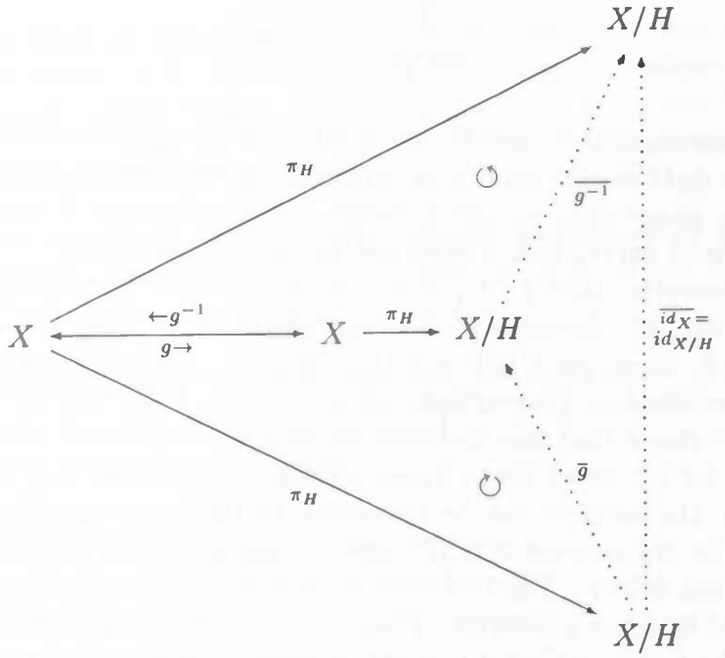
Just like we defined topological G-coverings (remark 2.1.2(c)), we will from now on refer to Galois G-covers, or quotients of an algebraic curve by group G, as a *G-covering.*

Finally we will need the following result, which in essence says that the quotient of a variety by a finite group G, which has a normal series $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n =$

G, can be viewed as the composition of certain quotient maps by the factor groups $G_n/G_{n-1}, \ldots, G_2/G_1, G_1/G_0 = G_1$. Thus, together with the previous result, this gives us a way of obtaining Galois covers out of one or more successive quotients by finite groups [4]. We give explicit examples of this idea in section 5.4.

Proposition 3.2.3
Let X be a projective variety, and let $G \subseteq Aut(X)$ be a finite subgroup. Suppose that $H \lhd G$ is a normal subgroup. Then G/H acts naturally as a group of automorphisms on X/H, and the quotients $(X/H)/(G/H)$ and X/G are isomorphic.

PROOF: The proof is quite straightforward, and follows from the mapping property of quotients. For example, the following diagram, which is a triple application of the mapping property of the quotient of X by H, shows how an automorphism $g \in G \subseteq Aut(X)$ induces an automorphism $\bar{g}$ of X/H:



Thus one defines $\bar{g}(P \mod H) := g(P) \mod H$. (Here one uses normality of H in G, since the H-invariance of, for instance, the map $\pi_H \circ g$, is ensured only if $(\pi_H \circ g)(h(P)) = \pi_H \circ (g \circ h)(P) = \pi_H \circ (h \circ g)(P) = (\pi_H \circ h)(g(P)) = \pi_H(g(P))$, i.e. if $g \circ h = h \circ g$.) It is clear that the subgroup $\{\bar{g} \mid g \in G\} \subseteq Aut(X/H)$ so obtained carries the same group structure as the abstract group G/H. The rest of the proof can be treated with similar commutative diagrams, and isn't difficult either ■

[4] Roughly this says that we know what a G-covering looks like, as soon as the quotients by the composition factors of G are known; In other words, we have reduced the problem of finding Galois covers with a finite group to the problem of finding the quotient by a finite simple group.

Chapter 4

Admissible Triples of $SL(2,q)$

In the previous chapters we have found several classifications of coverings. The main results were theorems 1 (b), 2 and 4. We have seen in the case of topological spaces, as well as in the case of algebraic curves, that the Galois G-coverings are exactly the connected G-coverings, i.e. the quotient by a group of automorphisms which is isomorphic to G.

The aim of the current chapter is to classify the $SL(2,q)$-coverings of the algebraic curve $\mathbb{P}^1(\mathbb{C})$, which are branched only above $0, 1$ and ∞, modulo equivalence. With theorem 4 (or theorem 2 (ii) in the case of topological covers), we reduced this problem to a pure group-theoretical one: Determine the set $\bigcup_{(n_1,n_2,n_3)} (Adm(G,(n_1,n_2,n_3))/\text{equivalence})$. From now on, this last set will be abbreviated by $Adm(G)/\sim$. Notice that an admissible triple (g_1,g_2,g_3) is determined by the pair (g_1,g_2), since $g_3 = (g_1g_2)^{-1}$. We will call the induced action of $SL(2,q)$ on these pairs *simultaneous conjugation* (thus: $(g_1,g_2)^h = (h^{-1}g_1h, h^{-1}g_2h)$). So the following problem is central in this chapter:

Determine the set of ordered pairs of generators of $SL(2,q)$ modulo simultaneous conjugation [1].

We start with summing up some basic properties of $SL(2,q)$, and determining the conjugacy classes of $SL(2,q)$ and the stabilizers of its elements under $SL(2,q)$-conjugation. Then, using Dickson's lemma A.3.2, we prove the existence of certain admissible triples of $SL(2,q)$ for general odd q, and we present an algorithm which computes the set $Adm(G)/\sim$ for general, but fixed, odd q.

[1] I don't know if it is possible to give a nice classification of these pairs for general q. In this chapter, we will just try to say as much as possible about this set.

4.1 First Properties of the Groups $SL(2,q)$

Most of the notations on groups can be found in appendix A.1. The group of 2×2 matrices with determinant 1 and entries in the finite field $\mathbb{F}_q$ is denoted by $SL(2,q)$. We fix a group $SL(2,q)$ and an algebraic closure F of $\mathbb{F}_q$ throughout; $p \geq 2$ denotes the characteristic of F (so $q = p^r$ for some $r \geq 1$). For $\lambda \in F^*$ and $\alpha \in F$ we introduce the abbreviations $d_\lambda := \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$ and $t_\alpha := \left(\begin{smallmatrix} 1 & 0 \\ \alpha & 1 \end{smallmatrix}\right)$. The matrices t_α and their conjugates are called *transvections*.

The characteristic polynomial of an element $x \in SL(2,q)$ equals $T^2 - trace(x)T + 1$. It will be denoted by $f_x(T)$. Recall that the theorem of Cayley and Hamilton says that $f_x(x) = 0$.

Lemma 4.1.1

(a) *If $p = 2$ then $Z(SL(2,q)) = \{I\}$. If $p > 2$ then the only element of order 2 in $SL(2,q)$ is $-I$ and $Z(SL(2,q)) = \{\pm I\}$.*

(b) *If $q > 3$ then $SL(2,q)$ has no nontrivial normal subgroups, except for the center $Z(SL(2,q))$ in case $p \neq 2$. Therefore $PSL(2,q)$ is simple whenever $q > 3$. The exceptional groups satisfy $PSL(2,2) = SL(2,2) \cong S_3 \cong D_{2\times 3}$, and $PSL(2,3) \cong A_4$.*

(c) *$SL(2,q)$ has size $(q+1)q(q-1) = q^3 - q$.*

(d) *In $SL(2,F)$, each element of $SL(2,q)$ is conjugate to some d_λ or $\pm t_\alpha$. If $p = 2$ the elements of $SL(2,q)$ have order $1, 2$ or a divisor of $q \pm 1$. If $p > 2$, the elements of $SL(2,q)$ have order $1, 2, p, 2p$ or a divisor of $q \pm 1$.*

(e) *Noncentral elements with the same trace have the same order. In some cases the converse also holds* [2]*. For all $x \in SL(2,q) \setminus Z(SL(2,q))$ we have:*

$p = 2$	$ord(x) = 2$	$\Leftrightarrow trace(x) = 0$
	$ord(x) = 3$	$\Leftrightarrow trace(x) = 1$
$p > 2$	$ord(x) = 3$	$\Leftrightarrow trace(x) = -1$
	$ord(x) = 4$	$\Leftrightarrow trace(x) = 0$
	$ord(x) = 6$	$\Leftrightarrow trace(x) = 1$
	$ord(x) = p$	$\Leftrightarrow trace(x) = 2$
	$ord(x) = 2p$	$\Leftrightarrow trace(x) = -2$

(f) *$SL(2,q)$ is generated by its transvections.*

[2] Not always: An example of two elements of order 5 in $SL(2,3^4)$ having distinct traces is the following: The splitting field of $X^5 - 1$ over $\mathbb{F}_3$ is the field $\Omega^f_{\mathbb{F}_3} \cong \mathbb{F}_{3^4} \cong \mathbb{F}_3[\overline{X}]$, which is the splitting field of $f(X) := X^4 + \ldots + X + 1$ over $\mathbb{F}_3$. Here $\overline{X}$ denotes the zero $X + (f)$ of $f(X)$ in the extension field $\mathbb{F}_3[X]/(f)$. The other roots of f are $\overline{X}^3, \overline{X}^{3^2} = \overline{X}^4$ and $\overline{X}^{3^3} = \overline{X}^2$. Since $\overline{X}^5 = \overline{1}$ we have $\overline{X}^{-1} = \overline{X}^4$ and $(\overline{X}^2)^{-1} = \overline{X}^3$. The matrices $diag(\overline{X}, \overline{X}^4)$ and $diag(\overline{X}^2, \overline{X}^3) \in SL(2,3^4)$ have order 5 but their traces, $\overline{-X^3 - X^2 - 1}$ and $\overline{X^3 + X^2}$ respectively, are distinct.

Proof: For (a) - (c) and (f) I refer to P.73-P.78 [Rob] and P.393-P.394 [Suz].

(d) The order of x will be denoted by $|x|$. If the characteristic polynomial $f_x(T) = (T-\lambda)^2$ then $\lambda = \pm 1$ is a double eigenvalue of x, so x has a normal form $\pm t_\alpha$ for some $\alpha \in F$. If $\alpha = 0$ then x is central. For other α we have

$$|x| = \begin{cases} |t_\alpha| = |-t_\alpha| = 2, & \text{if } p = 2 \\ |t_\alpha| = p \text{ or } |-t_\alpha| = 2p, & \text{if } p > 3. \end{cases}$$

Suppose now that $f_x(T) = (T-\lambda)(T-\lambda^{-1})$ has no double root. If $f_x(T)$ is reducible, i.e. $\lambda \in \mathbb{F}_q$, then $\lambda \in \mathbb{F}_q^*$, so $|x| = |\lambda|$ divides $q-1$. In the remaining situation, $f_x(T)$ is irreducible in $\mathbb{F}_q[T]$. The set of roots of a degree-d irreducible polynomial over a finite field of q elements is of the form $a, a^q, \ldots, a^{q^{d-1}}$. So $\lambda^q = \lambda^{-1}$, and $|x| = |\lambda|$ divides $q+1$.

(e) We know that the trace of $x \in SL(2,q)$ determines $f_x(T)$. So noncentral elements with the same trace have the same normal form under conjugation in $SL(2,q)$, hence the same order. The Cayley-Hamilton-theorem and lemma A.1.4 (c) prove the last assertion: For all $x \in SL(2,q)$ we have $x^2 - tr(x)x + 1 = 0$. This implies

$$tr(x) = 0 \Leftrightarrow x^2 + 1 = 0 \Rightarrow \qquad |x| = \begin{cases} 2 & \text{if } p = 2; \\ 4 & \text{if } p = 4; \end{cases}$$

$$tr(x) = \pm 1 \Leftrightarrow x^2 \mp x + 1 = 0 \Rightarrow$$

$$x^3 \pm 1 = (x \pm 1)(x^2 \mp x + 1) = 0 \Rightarrow |x| = \begin{cases} 6 & \text{if } p \geq 3 \text{ and } tr(x) = 1; \\ 3 & \text{otherwise,} \end{cases}$$

and, finally, if $p \geq 3$ and $tr(x) = \pm 2$, the (double) eigenvalue of x is ± 1, so the normal form of x is $\pm t_\alpha$ and $|x| = p$ (if $tr(x) = 2$) or $2p$ (if $tr(x) = -2$).

The only-if-part of the assertion follows from lemma A.1.4 (c). For example, if $p \geq 3$ and $|x| = 6$, then x is conjugate to $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$, for a primitive 6-th root of unity (we assume here $p > 3$). The lemma shows $0 = \sum_{i=1}^{6} (\lambda^4)^i = 2(\lambda^2 - \lambda + 1)$, i.e. $tr(x) = \lambda + \lambda^{-1} = 1$. Other cases are treated in the same way ■

4.2 The Conjugacy Classes of $SL(2,q)$

The conjugacy class of $x \in SL(2,q)$ will be denoted by $\mathfrak{Cl}(x)$, and the stabilizer (w.r.t. conjugation in $SL(2,q)$) of x by $Stab_{SL(2,q)}(x)$, or $\mathfrak{S}(x)$. In this section we determine both these sets and their sizes, for each x.

Since conjugate matrices have the same trace, elements in one and the same conjugacy class have the same characteristic polynomial. Moreover, for each $t \in \mathbb{F}_q$ the polynomial $T^2 - tT + 1$ occurs as a characteristic polynomial of some $x \in SL(2,q)$ (namely, of $x = \left(\begin{smallmatrix} 0 & -1 \\ 1 & t \end{smallmatrix}\right)$, for instance). For each $t \in \mathbb{F}_q$, we will find the conjugacy classes corresponding to the polynomial $T^2 - tT + 1$, and we will find their sizes. We denote by ζ a generator of $\mathbb{F}_q^*$, and write $f(T) = (T-\lambda)(T-\lambda^{-1}) = T^2 - tT + 1$.

Case 1: $f(T)$ has a double zero

In this case $\lambda = \lambda^{-1} = \pm 1$. Suppose that $M \in SL(2,q)$ has eigenvalue polynomial $f_M(T) = f(T)$, with $\lambda = 1$. Choose an eigenvector $v_1 \in \mathbb{F}_q \times \mathbb{F}_q$, and let v_2 be independent of v_1. Denote by $(v_1 \mid v_2)$ the matrix with first column v_1 and second column v_2. If this matrix has determinant d, then $Q := (v_1 \mid d^{-1}v_2)$ has determinant 1, and $Q^{-1}MQ = \left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right)$ for some $\alpha \in \mathbb{F}_q$. For $\alpha = 0$ we find the identity matrix. Therefore choose $\alpha, \beta \neq 0$. Then $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & \beta \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \Leftrightarrow C = 0$ and $\alpha D = \beta A$, that is $\alpha = \beta A^2$. So $\left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right)$ are conjugate if and only if α and β differ by a square in $\mathbb{F}_q$. Since all finite fields are perfect, this holds for all $\alpha, \beta \in \mathbb{F}_q^*$ if $p = 2$; if $p \geq 3$, this gives rise to two conjugacy classes. In the same way, if $p \geq 3$ and $\lambda = -1$, we obtain two classes as well.

The stabilizer of any of the four matrices $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & \zeta \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -1 & \zeta \\ 0 & -1 \end{smallmatrix}\right)$ is easily shown to be $\{\pm I + \left(\begin{smallmatrix} 0 & B \\ 0 & 0 \end{smallmatrix}\right) \mid B \in \mathbb{F}_q\}$. According as $p = 2$ or $p \geq 3$, this has size q or $2q$, so by the orbit-stabilizer-lemma, the corresponding conjugacy classes have size $q^2 - 1$ resp. $(q^2 - 1)/2$.

Case 2: $f(T)$ has two distinct zeros in $\mathbb{F}_q$

We assume that $f(T) = (T - \lambda)(T - \lambda^{-1})$ with $\lambda \neq \lambda^{-1} \in \mathbb{F}_q^*$. Suppose that M is a matrix having trace $t = \lambda + \lambda^{-1}$. Choose eigenvectors v_1 and v_2 in $\mathbb{F}_q \times \mathbb{F}_q$ corresponding to λ and λ^{-1}. If $det\,(v_1 \mid v_2) = d$, define $Q := (v_1 \mid d^{-1}v_2)$. Then $Q^{-1}MQ = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$, so M is conjugate to the diagonal form inside $SL(2,q)$. The matrices $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} \tilde{\lambda} & 0 \\ 0 & \tilde{\lambda}^{-1} \end{smallmatrix}\right)$ are conjugate if and only if $\tilde{\lambda} = \lambda^{\pm 1}$. We conclude that each the polynomial $f(T)$ corresponds to exactly one conjugacy class, namely the one which is represented by $d_\lambda = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$.
Since the stabilizer of $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$ in $SL(2,q)$ is the cyclic group $\left\langle \left(\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{smallmatrix}\right) \right\rangle$ (where ζ denotes a generator of $\mathbb{F}_q^*$), the orbit-stabilizer lemma shows that in case 2, each $\mathfrak{Cl}\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$ contains $|SL(2,q)|/(q-1) = q(q+1)$ elements.
Finally, we remark that there are exactly $(q-2)/2$ (if $p = 2$) or $(q-3)/2$ (if $p \geq 3$) polynomials $f(T) = T^2 - tT + 1$ ($t \in \mathbb{F}_q$) which have two distinct roots in $\mathbb{F}_q$ (namely, each of the pairs $\{\lambda, \lambda^{-1}\}$ with $\lambda \in \mathbb{F}_q^* \setminus \{\pm 1\}$ defines one), so in case 2 we obtain exactly as many conjugacy classes.

Case 3: $f(T)$ has two distinct zeros in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$

According as $p = 2$ or $p \geq 3$, case 1 showed that there are 1 or 2 characteristic polynomials with double root $\lambda = \lambda^{-1}$, and case 2 showed that there are $\frac{q-2}{2}$ or $\frac{q-3}{2}$ polynomials with roots $\lambda \neq \lambda^{-1} \in \mathbb{F}_q^*$. So we end up with $\frac{q}{2}$ (if $p = 2$) or $\frac{q-1}{2}$ (if $q \geq 3$) irreducible characteristic polynomials, having distinct roots which lie not in $\mathbb{F}_q$.

Lemma 4.2.1
Suppose that $x \in SL(2,q)$ has an irreducible eigenvalue polynomial $f_x(T) = T^2 - tT + 1$. Then x is conjugate to $\left(\begin{smallmatrix} 0 & 1 \\ -1 & t \end{smallmatrix}\right)$ in $SL(2,q)$, and $\mathfrak{S}(x)$ is cyclic of order $q+1$.

PROOF: Suppose that the lemma holds for all $x = \left(\begin{smallmatrix} 0 & 1 \\ -1 & t \end{smallmatrix}\right)$ with T^2-tT+1 irreducible. The orbit-stabilizer-lemma then tells us that the conjugacy class of x contains $q(q^2-1)/(q+1) = q(q-1)$ elements. According as $p = 2$ or $p > 2$, there are exactly $q/2$ resp. $(q-1)/2$ different t with the property that $T^2 - tT + 1$ is irreducible, so we find $q^2(q-1)/2$ resp. $q(q-1)^2/2$ elements in $SL(2,q)$ which are conjugate to some x of the above form. Adding these to the elements which have a reducible eigenvalue polynomial, we obtain exactly $q(q^2-1)$ elements, that is, the whole of $SL(2,q)$.

It remains to show that for $x = \left(\begin{smallmatrix} 0 & 1 \\ -1 & t \end{smallmatrix}\right)$, the lemma is valid. Fix such an x. By the Cayley-Hamilton-theorem, we have $x^2-tx+1 = 0$, and since x isn't diagonal, the eigenvalue polynomial is also the minimal polynomial $f_x(T)$ of x over $\mathbb{F}_q$. So $\mathbb{F}_q[x] \cong \mathbb{F}_q[T]/(f_x(T)) \cong \mathbb{F}_{q^2}$. One easily sees that $C(x) := \{y \in Mat(2,q) \mid yx = xy\} = \left\{\left(\begin{smallmatrix} a & b \\ -b & a+bt \end{smallmatrix}\right) \middle| a,b \in \mathbb{F}_q\right\} = \mathbb{F}_q I + \mathbb{F}_q x = \mathbb{F}_q[x]$ (where $Mat(2,q)$ denotes the set of all 2×2 matrices over $\mathbb{F}_q$), so $\mathfrak{S}(x) = \{y \in SL(2,q) \mid yx = xy\} = \{y \in C(x) \mid det(y) = 1\} = \{y \in \mathbb{F}_q[x] \mid det(y) = 1\}$. Therefore, to complete the proof, it is sufficient to show that $(det_{|\mathbb{F}_q[x]})^{-1}(1)$ is a cyclic group of order $q+1$. One can use the norm to do this.

Recall that the norm $N := N_{\mathbb{F}_{q^2}/\mathbb{F}_q} : \mathbb{F}_{q^2} \to \mathbb{F}_q$ is defined by $\alpha \mapsto det(m_\alpha)$, where m_α denotes a matrix representing multiplication by α. An easy calculation shows that $N(\alpha) = \alpha^2$, for all α. The restriction $N_{|\mathbb{F}_{q^2}^*} : \mathbb{F}_{q^2}^* \to \mathbb{F}_q^*$ is a group homomorphism. In general, in a cyclic group $C_m =< x >$, and for $n \mid m$, the elements $g \in C_m$ with the property $g^n = 1$ form a subgroup $< x^{m/n} >$. Therefore $ker(N_|) = \{\alpha \in \mathbb{F}_{q^2} \mid \alpha^{q+1} = 1\}$ is cyclic of order $q+1$.

Finally we show that the norm and determinant on $\mathbb{F}_q[x]$ are one and the same function; if this is true, then it follows that $\mathfrak{S}(x) = (det_{|\mathbb{F}_q[x]})^{-1}(1) = ker(N_|)$, a cyclic group of order $q+1$. Each element y in $\mathbb{F}_q[x]$ can be written as $ax+b$. On the one hand we have $det(ax+b) = a^2 + b^2 + abt$, on the other hand we have $N(a+bx) = (ax+b)(ax+b)^q = (ax+b)(ax^q+b) = a^2x^{q+1} + b^2 + ab(x+x^q) = a^2 + b^2 + abt$. So indeed $N = det$, and the proof is complete ■

We summarize the information from this section in the following table:

	The conjugacy classes of $SL(2,q)$ for $p = 2$:			
Class Rep. x	$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 0 & -1 \\ 1 & t \end{smallmatrix}\right)$
Char. Pol. $f_x(T)$	$(T+1)^2$	$(T+1)^2$	$(T-\lambda)(T-\lambda^{-1})$ $\lambda \in \mathbb{F}_q^* \setminus \{1\}$	$T^2 - tT + 1$ irr. in $\mathbb{F}_q[T]$
# Classes	1	1	$\frac{1}{2}(q-2)$	$\frac{1}{2}q$
$\lvert\mathfrak{Cl}(x)\rvert$	1	q^2-1	$q(q+1)$	$q(q-1)$
$\mathfrak{S}(x)$	$SL(2,q)$	$\{I + \left(\begin{smallmatrix} 0 & B \\ 0 & 0 \end{smallmatrix}\right) \mid B \in \mathbb{F}_q\}$	$\left\langle \left(\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{smallmatrix}\right) \right\rangle$	$\cong C_{q+1}$
Remark	center	elts. of order 2	elts. of order $\neq 1$ but dividing $q-1$	elts. of order $\neq 1$ but dividing $q+1$

	The conjugacy classes of $SL(2,q)$ for $p \geq 3$:			
Class Rep. x	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$; $\left(\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$; $\left(\begin{smallmatrix}1&\zeta\\0&1\end{smallmatrix}\right)$; $\left(\begin{smallmatrix}-1&1\\0&-1\end{smallmatrix}\right)$; $\left(\begin{smallmatrix}-1&\zeta\\0&-1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}\lambda&0\\0&\lambda^{-1}\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&-1\\1&t\end{smallmatrix}\right)$
Char. Pol. $f_x(T)$	$(T+1)^2$; $(T-1)^2$	$(T+1)^2$ and $(T-1)^2$	$(T-\lambda)(T-\lambda^{-1})$ $\lambda \in \mathbb{F}_q^* \setminus \{\pm 1\}$	$T^2 - tT + 1$ irr. in $\mathbb{F}_q[T]$
# Classes	1; 1	1; 1; 1; 1	$\frac{1}{2}(q-3)$	$\frac{1}{2}(q-1)$
$\lvert\mathfrak{Cl}(x)\rvert$	1; 1	$\frac{1}{2}(q^2-1)$	$q(q+1)$	$q(q-1)$
$\mathfrak{S}(x)$	$SL(2,q)$	$\{\pm I + \left(\begin{smallmatrix}0&B\\0&0\end{smallmatrix}\right) \mid B \in \mathbb{F}_q\}$	$\left\langle \left(\begin{smallmatrix}\zeta&0\\0&\zeta^{-1}\end{smallmatrix}\right) \right\rangle$	$\cong C_{q+1}$
Remark	center	elts. of order p and $2p$	elts. of order $\neq 1,2$ but dividing $q-1$	elts. of order $\neq 1,2$ but dividing $q+1$

Recall that ζ is a generator of $\mathbb{F}_q^*$, and that $\mathfrak{Cl}(x)$ and $\mathfrak{S}(x)$ denote the conjugacy class and the stabilizer of x in $SL(2,q)$, respectively.

4.3 A Few Existence Results

Definition 4.3.1
Let $f : C \to \mathbb{P}^1(\mathbb{C})$ be an $SL(2,q)$-cover which is unbranched outside $\{0,1,\infty\}$, and denote by (g_1,g_2,g_3) the corresponding (equivalence class of) admissible triple(s) of $SL(2,q)$. The triple $(|g_1|,|g_2|,|g_3|)$ will be called the *branch type* of the cover (C,f). For simplicity each triple (n_1,n_2,n_3) of positive numbers will be called a branch type of the group $SL(2,q)$, or we say $SL(2,q)$ has branch type (n_1,n_2,n_3), if there exists an $SL(2,q)$-cover unbranched outside $\{0,1,\infty\}$, which has branch type (n_1,n_2,n_3) (or equivalently, if $SL(2,q)$ has generators x,y which satisfy $(|x|,|y|,|xy|) = (n_1,n_2,n_3)$) ■

Of course, if (n_1,n_2,n_3) is a branch type, then $(n_{\sigma(1)},n_{\sigma(2)},n_{\sigma(3)})$ is also a branch type for any permutation σ of $\{1,2,3\}$ (the geometrical proof of this statement is just the 3-transitivity of $PGL(2,\mathbb{C}) = Aut(\mathbb{P}^1(\mathbb{C}))$: One can compose the covering map f with an automorphism of $\mathbb{P}^1$ which permutes the set $\{0,1,\infty\}$ in the appropriate way). Therefore in this section, we are interested only in unordered branch types.

The classification theorem 7 and Dickson's lemma, which can be found in appendix A, can be used to prove some results on the existence of certain branch types of $SL(2,q)$.

Example 4.3.2
In the proof of Dickson's lemma, it is shown that $SL(2,5)$ can be generated by two elements x,y of order 3, the product of which has order 10. In other words, $SL(2,5)$ has branch type $\{3,3,10\}$.

Explicitly, one can take $x = \left(\begin{smallmatrix}0&-1\\1&-1\end{smallmatrix}\right)$ and $y = \left(\begin{smallmatrix}0&1\\-1&-1\end{smallmatrix}\right)$. Namely, in the previous section it was shown that up to conjugation, the only element of order 3 in $SL(2,5)$ is $x := \left(\begin{smallmatrix}0&-1\\1&-1\end{smallmatrix}\right)$. By lemma 4.1.1 (e), we have $|y| = 3 \Leftrightarrow tr(y) = -1$ and $|xy| = 10 \Leftrightarrow tr(xy) = -2$. Solving these equations for $y \in SL(2,5)$ yields only six possibilities, one of which is $y := \left(\begin{smallmatrix}0&1\\-1&-1\end{smallmatrix}\right)$. This y satisfies in addition $|(xy)^2x| = 4$. So $|\langle x,y\rangle|$ is divisible by $|x| = 3, |xy| = 10$

and $|(xy)^2x| = 4$, thus $60||< x, y >|$. Since $< x, y >$ is cannot be normal in $SL(2,5)$, and therefore not be of index 2, it follows that $< x, y >= SL(2,5)$ ■

Proposition 4.3.3
*Let $p \geq 3$ be prime and assume that q is a power of p. Then $SL(2,q)$ does not posses any of the branch types $\{2,*,*\}$, $\{p,p,p\}$ and $\{p,2p,2p\}$ (where * denotes an arbitrary number).*

PROOF: Since $p \neq 2$, the only element of order 2 is the central element $-I$. Because no $SL(2,q)$ is Abelian, but $< -I, x >$ is Abelian for each $x \in SL(2,q)$, there cannot be branch types containing 2. Suppose $< x, y >= SL(2,q)$ and $|x| = |y| = p$. Then x and y fix a line in $\mathbb{P}^1_{\mathbb{F}_q}$, say $\mathbb{F}_q(a_1 : a_2)$ and $\mathbb{F}_q(b_1 : b_2)$, respectively. These lines are distinct, since otherwise x and y could be conjugated simultaneously to the form $\left(\begin{smallmatrix} 1 & 0 \\ * & 1 \end{smallmatrix}\right)$. This would mean that $< x, y >$ consists only of elements of order $1, 2, p$ or $2p$, a contradiction. So $\{(a_1, a_2), (b_1, b_2)\}$ is a basis for $\mathbb{F}_q \times \mathbb{F}_q$, and on this basis x and y have the form $\left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ \beta & 1 \end{smallmatrix}\right)$, respectively. Therefore $tr(xy) = 2 + \alpha\beta$, so by lemma 4.1.1(e), xy has order p exactly if $\alpha\beta = 0$. This would mean that either x or y is the identity, contradicting $|x| = |y| = p$. The case $\{p, 2p, 2p\}$ is treated in the same way ■

Proposition 4.3.4
Let $p \geq 3$ be prime. For each $k = 3, 4, 6, p, 2p$, the group $SL(2,p)$ has branch types $b = \{p,p,k\}$, $\{p,2p,k\}$ and $\{2p,2p,k\}$ [3], unless $b = \{p,p,p\}$ or $b = \{p,2p,2p\}$.

PROOF: The "unless"-statement is just a special case of proposition 4.3.3. We now show the existence of branch type $\{p,p,k\}$. Define $x = t_1$ and $y = \left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right)$, where α is an indeterminate, algebraic over $\mathbb{F}_p$. Then $xy = \left(\begin{smallmatrix} 1 & \alpha \\ 1 & 1+\alpha \end{smallmatrix}\right)$ has trace $2+\alpha$. Lemma 4.1.1(e) shows that xy has order $3, 4, 6, p$ or $2p$ exactly if $\alpha = -3, -2, -1, 0$ or -4 respectively. For each of these α we have $\alpha^2 \neq -1$ if $p = 3$, so by Dickson's lemma we find that whenever $\alpha \neq 0$, we have $< x, y >= SL(2,p)$. This shows the existence of branch types $\{p,p,k\}$, $k = 3, 4, 6, 2p$ unless $k = p = 3$.

We turn to $\{p,2p,k\}$: Define $x = t_1$ and $y = \left(\begin{smallmatrix} -1 & \alpha \\ 0 & -1 \end{smallmatrix}\right)$, then $tr(xy) = \alpha - 2$ so $|xy| = 3, 4, 6, p$ or $2p$ exactly if $\alpha = 1, 2, 3, 4$ or 0, respectively. Dickson's lemma says that $< x, y^{p-1} >= \langle \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & -\alpha \\ 0 & 1 \end{smallmatrix}\right) \rangle = SL(2,p)$ unless $\alpha = 0$ or $p = 3$ and $\alpha = 3 (= 0)$. In all the other cases we obtain $SL(2,p) =< x, y^{p-1} >\leq< x, y >\leq SL(2,p)$, so x and y generate $SL(2,p)$. Thus all $\{p,2p,k\}$, $k = 3, 4, 6, p$ are branch types of $SL(2,p)$, unless $p = 3$ and $k = 6$.

The final case $\{2p,2p,k\}$ can be treated as the previous one: We consider the matrices $x = -t_{-1}$ and $y = \left(\begin{smallmatrix} -1 & \alpha \\ 0 & -1 \end{smallmatrix}\right)$. The trace of their product becomes $2 - \alpha$, and now Dickson's lemma says that $< x^{p-1}, y^{p-1} >= SL(2,p)$, unless $p = k = 3$. The result follows ■

[3] Notice that since $p > 2$ indeed always $3, 4$ and 6 divide either $q \pm 1$ or $2p$.

Proposition 4.3.5
Let $p \geq 3$ be prime, $n \geq 1$ and $q = p^n \neq 3, 9$. Suppose that $r > 2$ is a divisor of $q-1$ or $q+1$, and define N to be the order of p in the group $(\mathbb{Z}/r\mathbb{Z})^*$. If either

(i) $N = n$ is odd, or

(ii) $N = 2n$ and $r \mid q+1$,

then $\{p,p,r\}$, $\{p,2p,r\}$ and $\{2p,2p,r\}$ are branch types of $SL(2,q)$.

PROOF: We will only prove that $\{p,p,r\}$ is a branch type of $SL(2,q)$; the cases $\{p,2p,r\}$ and $\{2p,2p,r\}$ are treated similarly (as in proposition 4.3.4). Define $x = t_1$ and $y = \left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right)$, where α is an unknown. Then xy has trace $2+\alpha$. If xy has order r relatively prime to p, then xy is conjugate to d_ζ for some primitive r-th root of unity ζ in $\mathbb{F}_{q^2}$. Since the trace is invariant under conjugation, we find $\alpha = \omega - 2$, with $\omega := \zeta + \zeta^{-1}$. Thus we fix an $\alpha := \zeta + \zeta^{-1} - 2$, for some r-th root of unity ζ.

Dickson's lemma A.3.2 ensures that $< x, y >= SL(2, \mathbb{F}_p(\alpha))$ only if $(p, \alpha^2) \neq (3, -1)$. In this case however, we have $\alpha \in \mathbb{F}_9$. For this reason we have restricted to $q \neq 3, 9$; then we can never have $(p, \alpha^2) = (3, -1)$ and $\mathbb{F}_p(\alpha) = \mathbb{F}_q$ at the same time. We may thus assume, that Dickson's lemma holds without exception!

First, suppose that $r \mid q-1$. We have $< x, y >= SL(2,q)$ if and only if $\mathbb{F}_p(\omega) = \mathbb{F}_p(\alpha) = \mathbb{F}_q = \mathbb{F}_{p^n}$. So we have to find conditions on r and N under which $\mathbb{F}_p(\omega) = \mathbb{F}_{p^n}$. Lemma A.3.1 helps us out. Namely, it says that

$$\mathbb{F}_p(\omega) = \begin{cases} \mathbb{F}_{p^{N/2}}, & \text{if } N \text{ is even and } r \mid p^{N/2}+1; \ (1) \\ \mathbb{F}_{p^N}, & \text{if } N \text{ is odd. } (2) \end{cases}$$

Situation (1) gives us no information. For in that case, if $\mathbb{F}_p(\omega) = \mathbb{F}_{p^n}$, then $N = 2n$ and $r \mid p^{N/2}+1 = p^n+1$, contradicting the assumption $2 < r \mid p^n - 1$. Situation (2) however shows, if $N = n$ is odd, then $\mathbb{F}_p(\alpha) = \mathbb{F}_p(\omega) = \mathbb{F}_{p^n}$, and therefore $< x, y >= SL(2, p^n) = SL(2,q)$.

Finally, if on the other hand $r \mid q+1$, the same argument shows that $\mathbb{F}_p(\alpha) = \mathbb{F}_p(\omega) = \mathbb{F}_{p^n}$ if either $N = 2n$, or $N = n$ is odd. This completes the proof ■

The above propositions show the existence of certain branch types $\{n_1, n_2, n_3\}$ in $SL(2,q)$. The next proposition shows something stronger: For certain triples $\{n_1, n_2, n_3\}$ of integers $n_i \geq 3$ (depending on q), we know that $\{n_1, n_2, n_3\}$ is a branch type of $SL(2,q)$, and that in addition every two elements $x, y \in SL(2,q)$ with $\{|x|, |y|, |xy|\} = \{n_1, n_2, n_3\}$ *necessarily generate* $SL(2,q)$.

Proposition 4.3.6
Let $p \geq 3$ be a prime, and let $q > 3$ be a power of p. Define the set

$$\Sigma(q) := \left\{ \{q-1, r_+, p\}, \{q-1, r_+, 2p\} \mid 2 < r_+ \mid q+1 \right\} \cup \left\{ \{q+1, r_-, p\}, \{q+1, r_-, 2p\} \mid 2 < r_- \mid q-1 \right\}.$$

a) For all $x, y \in SL(2,q)$ *we have*

$$\{|x|,|y|,|xy|\} \in \Sigma(q) \Rightarrow < x,y >= SL(2,q),$$

unless

$$p = 3,\ q = 3^2 = 9,\ |x| = 4,\ |y| = 10,\ \text{and } |xy| = 3 \text{ or } 6. \tag{4.1}$$

b) For each $\{n_1,n_2,n_3\} \in \Sigma(q)$ *there exist* $x, y \in SL(2,q)$ *with* $\{|x|,|y|,|xy|\} = \{n_1,n_2,n_3\}$. *Therefore each element in* $\Sigma(q)$, *different from* $\{4, 10, 3 \text{ or } 6\}$ *in case* $q = 9$, *is a branch type of* $SL(2,q)$.

c) In the exceptional case (4.1), x *and* y *generate either the whole group* $SL(2,q)$, *or a group isomorphic to* $SL(2,5)$ *(the group of type (viii) in theorem 7).*

PROOF: Choose two elements $x, y \in SL(2,q)$ with $2 < |x| | q-1$ and $2 < |y| | q+1$. By section 4.2 we may assume $x = d_\lambda$ for some $\lambda \in \mathbb{F}_q \setminus \{\pm 1\}$. Let $y = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ have trace t. By lemma 4.1.1(e), we have $|xy| = p \Leftrightarrow \left[tr\left(\begin{smallmatrix} \lambda a & \lambda b \\ \lambda^{-1}c & \lambda^{-1}d \end{smallmatrix}\right) = 2 \text{ and } \lambda b \neq 0 \text{ or } \lambda^{-1}c \neq 0\right] \Leftrightarrow \left[a = \frac{2\lambda - t}{\lambda^2 - 1} \text{ and } b \neq 0 \text{ or } c \neq 0\right]$. So we can define $y = \left(\begin{smallmatrix} a & 1 \\ det=1 & t-a \end{smallmatrix}\right)$ with a as above, and conclude that for any two divisors $2 < r_+, r_-$ of $q \pm 1$ there exist elements $x, y \in SL(2,q)$ with $(|x|,|y|,|xy|) = (r_+, r_-, p)$. If we replace 2λ in the definition of a by -2λ, we find in the same way existence of x, y with $(|x|,|y|,|xy|) = (r_+, r_-, 2p)$. This shows that the first statement in (b) holds, thus (b) follows if we have proven (a).

To prove (a), we choose arbitrary elements x and y in $SL(2,q)$ with $2 < |x| | q-1$ and $2 < |y| | q+1$ and $|xy| = p$ or $2p$, and we want to find conditions on x, y under which $< x,y >= SL(2,q)$. Since $< x >$ and $< y >$ are contained in non-conjugate maximal Abelian subgroups of $< x,y >$ which have size relatively prime to p (namely in cyclic subgroups of order $q-1$ and $q+1$, respectively), we find (in the terminology of section A.2) $s + t \geq 2$. Scanning the table in theorem 7, we see that $G :=< x,y >$ must be a group of type (viii) (i.e. isomorphic with $SL(2,5)$; this can only happen if $p = 3$), (ix) (i.e. $G \cong SL(2,q')$ for some $q' \leq q$), or (x) (i.e. $G \cong < SL(2,q'), d_\lambda >$ for some $q' < q$ and $\lambda \in \mathbb{F}_q$ with $< \lambda^2 >= \mathbb{F}_{q'}^*$). We consider the two cases, in which $< x >$ resp. $< y >$ are themselves maximal Abelian subgroups of $SL(2,q)$:

$|x| = q-1$: If G were of type (viii), then in fact $q = 9$ (since $SL(2,5) \not\subset SL(2,3)$, and for $q > 9$ the element x would have order $\geq 3^3 - 1 = 26$, whereas $SL(2,5)$ doesn't contain elements of such high order). But if $q = 9$ then $|x| = 8$, which is also not the order of an element of $SL(2,5)$. Thus G must be of type (ix) or (x).

Suppose that G is of type (x), that is, there is $q' \leq \sqrt{q}$ with $\mathbb{F}_{q'} < \mathbb{F}_q$, and some $d_\lambda \in SL(2,(q')^2)$ such that $G \cong < SL(2,q'), d_\lambda >$. This last group has only maximal Abelian subgroups of size $2(q' \pm 1)$ and $2q'$ (this is proven in the appendix, case $(s,t) = (0,2)$). For $q > 9$ we always have

$$2(q'+1) \leq 2(\sqrt{q}+1) < q - 1 = |x|,$$

which is in contradiction with the size of the maximal Abelian subgroups. Since $q' \geq p \geq 3$ and $q \geq (q')^2$, we must have $q = 9$. But that means $|G| = 2|SL(2,3)| = 2^4 \cdot 3$, contradicting our assumption that $y \in G$ has order 5 or 10.

We conclude that G is necessarily a group of type (ix). If $G \cong SL(2,q')$ with $q' \leq \sqrt{q}$, then G contains elements of order $p, 2p$, or a divisor of $q' \pm 1$. But these numbers are all distinct from $|x| = q - 1$, so we may indeed conclude that $q' = q$, and therefore $G =< x, y >= SL(2,q)$.

$|y| = q + 1$: We may assume $|x| \neq q - 1$. As above, if G is of type (viii) then, as above, $p = 3$, and now $x, y \in SL(2,9)$ satisfy $|x| = 4, |y| = 10$ and $|xy| = 3$ or 6. These orders divide the size of $SL(2,5)$, so in the situation (4.1), it is indeed possible that $G \cong SL(2,5)$. The groups of type (ix) and (x) are treated just like we did it before, in the case $|x| = q - 1$. Thus we have proven (a) and (c) as well ■

4.4 Computing Admissible Triples of $SL(2,q)$

In theorem 4 we have given the set $Adm(SL(2,q))/\sim$ a geometric interpretation: It is in bijection with the set of $SL(2,q)$-covers of $\mathbb{P}^1(\mathbb{C})$ which are branched at $0, 1$ and ∞ only, modulo equivalence. In this section we will show how one can compute the set $Adm(SL(2,q))/\sim$, or equivalently, the set of ordered pairs of generators of $SL(2,q)$ modulo simultaneous conjugation. For the sake of simplicity we will restrict to odd q.

Convention 4.4.1
Recall that the conjugacy class of x in $SL(2,q)$ is denoted by $\mathfrak{Cl}(x)$, and the stabilizer $Stab_{SL(2,q)}(x)$ by $\mathfrak{S}(x)$. The set of conjugacy class representatives of $SL(2,q)$ that was found in section 4.2 will be abbreviated by $Rep(q)$. For an element $x \in SL(2,q)$, by an $\mathfrak{S}(x)$-class we mean a subset of $SL(2,q)$ which is of the form $y^{\mathfrak{S}(x)} := \{z^{-1}yz \mid z \in \mathfrak{S}(x)\}$, for some $y \in SL(2,q)$ (so if x is central, the $\mathfrak{S}(x)$-classes are exactly the conjugacy classes of $SL(2,q)$) ■

Lemma 4.4.2
The set

$$\bigcup_{x \in Rep(q)} \{(x,y) \mid y \text{ runs through a set of } \mathfrak{S}(x)\text{-class representatives}\}$$

is in bijection with $(SL(2,q) \times SL(2,q)) \mod SL(2,q)$, *the set of pairs of elements in* $SL(2,q)$ *modulo simultaneous conjugation.*

PROOF: The obvious map $(x,y) \mapsto (x,y) \mod SL(2,q)$ defines a bijection between the two sets in the lemma ■

Our main problem, as formulated on page 19, can therefore be restated as follows:

Determine those pairs in the set

$$\bigcup_{x \in Rep(q)} \{(x,y) \mid y \text{ runs through a set of } \mathfrak{S}(x)\text{-class representatives}\},$$

which generate $SL(2,q)$.

We will try to do this now. To begin, we make two observations: If x is noncentral, and $y \in \mathfrak{S}(x)$, then $< x,y > \subset \mathfrak{S}(x) \lneq SL(2,q)$. Moreover, $SL(2,q)$ is never Abelian, so if (x,y) generates $SL(2,q)$, both x and y are noncentral elements. So we consider only pairs (x,y) with $x,y \in SL(2,q)$ noncentral, and such that $y \notin \mathfrak{S}(x)$.

The first conjugacy class representatives that we consider are $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}-1 & 1\\ 0 & -1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}1 & \zeta\\ 0 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}-1 & \zeta\\ 0 & -1\end{smallmatrix}\right)$ (recall that we assumed $p > 2$). Let x be one of these. We have $\mathfrak{S}(x) = \{\pm\left(\begin{smallmatrix}1 & \alpha\\ 0 & 1\end{smallmatrix}\right) \mid \alpha \in \mathbb{F}_q\}$. Conjugation of an arbitrary element in $SL(2,q)$ by an element of $\mathfrak{S}(x)$ looks like

$$\begin{pmatrix}1 & -\alpha\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}1 & \alpha\\ 0 & 1\end{pmatrix} = \begin{pmatrix}a-\alpha c & \alpha a + b - \alpha^2 c - \alpha d\\ c & \alpha c + d\end{pmatrix}$$

(up to some signs, we find the same if there are -1 on the diagonal). In particular, the element c remains constant under $\mathfrak{S}(x)$-conjugation. If (x,y) generates $SL(2,q)$, then y cannot be an upper-diagonal matrix, for otherwise $< x,y >$ generates a subgroup of upper diagonal matrices. Thus we write $y := \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$, with $c \neq 0$. If we define $\alpha := -c^{-1}(d' - d)$, then conjugation of y by $\left(\begin{smallmatrix}1 & \alpha\\ 0 & 1\end{smallmatrix}\right)$ shows that y is conjugate to a matrix having bottom row (c,d'), for any $d' \in \mathbb{F}_q$. We take $d' := t := trace(y)$, and conclude that y can be conjugated to $\left(\begin{smallmatrix}0 & -c^{-1}\\ c & t\end{smallmatrix}\right)$ by an element of $\mathfrak{S}(x)$. We end up with the following potential pairs of generators of $SL(2,q)$ (with x one of the above four matrices):

$$\left\{(x,y) \mid y = \left(\begin{smallmatrix}0 & -c^{-1}\\ c & t\end{smallmatrix}\right), \text{with } c \in \mathbb{F}_q^* \text{ and } t \in \mathbb{F}_q\right\}. \tag{4.2}$$

The next type of conjugacy class representatives to consider, are the noncentral diagonal matrices $\left(\begin{smallmatrix}\lambda & 0\\ 0 & \lambda^{-1}\end{smallmatrix}\right)$, where $\lambda \in \mathbb{F}_q^* \setminus \{\pm 1\}$. If x equals one of these matrices, we have $\mathfrak{S}(x) = \left\{d_\alpha = \left(\begin{smallmatrix}\alpha & 0\\ 0 & \alpha^{-1}\end{smallmatrix}\right) \mid \alpha \in \mathbb{F}_q^*\right\}$. Again, if (x,y) generates $SL(2,q)$ and $y = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$, then neither b nor c are allowed to equal zero, since otherwise $< x,y >$ is a group of lower resp. upper diagonal matrices. Conjugating y by an element of $\mathfrak{S}(x)$ looks like

$$\begin{pmatrix}\alpha^{-1} & 0\\ 0 & \alpha\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}\alpha & 0\\ 0 & \alpha^{-1}\end{pmatrix} = \begin{pmatrix}a & \alpha^{-2}b\\ \alpha^2 c & d\end{pmatrix}.$$

So the diagonal of y remains unchanged under $\mathfrak{S}(x)$-conjugation. If t denotes the trace of y, then $d^2 - td + 1 = (d-t)d + 1 = -ad + 1 = bc \neq 0$. We will see what this means for the different possibilities of t.

- $t = 2$: In this case $d^2 - td + 1 = (d-1)^2$ so we can choose $d \in \mathbb{F}_q \setminus \{1\}$. For such a fixed d we have $a = t - d$. After $\mathfrak{S}(x)$-conjugation we can achieve that c is either 1 or ζ (where ζ denotes, as usual, a generator of the group $\mathbb{F}_q^*$, which is a non-square). Then b is determined by the identity $ad - bc = 1$.

- $t = -2$: This case is similar to the previous one. The diagonal can be anything of the form $(-2-d, d)$ with $d \neq -1$, and c can be chosen from $\{1, \zeta\}$; then b is again determined by $det(y) = 1$.
- $T^2 - tT + 1$ reducible but $t \neq \pm 2$: There are $(q-3)/2$ such $t \in \mathbb{F}_q$. For each of these t there are $q-2$ ways to choose $d \in \mathbb{F}_q$ such that $d^2 - td + 1 \neq 0$, since $T^2 - tT + 1$ has two distinct roots in $\mathbb{F}_q$. For each of these d we can again choose $c \in \{1, \zeta\}$, and b has no freedom anymore.
- $T^2 - tT + 1$ irreducible: There are $(q-1)/2$ such $t \in \mathbb{F}_q$. For each of these t, each $d \in \mathbb{F}_q$ satisfies $d^2 - td + 1 \neq 0$. For a fixed d, the coordinate c can again be realized as being either 1 or ζ, and b is determined by the condition $det(y) = 1$.

We have obtained the following potential pairs (x, y) of generators of $SL(2,q)$ (where x is a noncentral diagonal matrix):

$$\left\{(x,y) \mid y = \left(\begin{smallmatrix} 2-d & det=1 \\ c & d \end{smallmatrix}\right), \text{with } d \in \mathbb{F}_q \setminus \{1\}, \text{ and } c = 1 \text{ or } \zeta\right\} \tag{4.3}$$

$$\left\{(x,y) \mid y = \left(\begin{smallmatrix} -2-d & det=1 \\ c & d \end{smallmatrix}\right), \text{with } d \in \mathbb{F}_q \setminus \{-1\}, \text{ and } c = 1 \text{ or } \zeta\right\} \tag{4.4}$$

$$\left\{(x,y) \mid y = \left(\begin{smallmatrix} t-d & det=1 \\ c & d \end{smallmatrix}\right), \text{with } t \in \mathbb{F}_q \setminus \{\pm 2\} \text{ such that } T^2 - tT + 1 \text{ is reducible,} \right.$$
$$\left. d \in \mathbb{F}_q \text{ such that } d^2 - td + 1 \neq 0, \text{ and } c = 1 \text{ or } \zeta\right\} \tag{4.5}$$

$$\left\{(x,y) \mid y = \left(\begin{smallmatrix} t-d & det=1 \\ c & d \end{smallmatrix}\right), \text{with } t \in \mathbb{F}_q \text{ such that } T^2 - tT + 1 \text{ is irreducible,} \right.$$
$$\left. d \in \mathbb{F}_q, \text{ and } c = 1 \text{ or } \zeta\right\} \tag{4.6}$$

It remains to investigate the pairs (x, y), where $x = \left(\begin{smallmatrix} 0 & -1 \\ 1 & t \end{smallmatrix}\right)$ has an irreducible eigenvalue polynomial $T^2 - tT + 1$, and y runs through the set of $\mathfrak{S}(x)$-class representatives. For such x however, it turns out to be very difficult to write down the representatives y explicitly. The stabilizer of x can however be computed quite easily.

We fix a representative $x = \left(\begin{smallmatrix} 0 & -1 \\ 1 & t \end{smallmatrix}\right)$, where $t = \lambda + \lambda^{-1}$ and $\lambda \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. In $SL(2,q^2)$, we can conjugate x to d_λ. Namely, the matrix

$$M := \begin{pmatrix} \frac{\lambda}{1-\lambda^2} & \frac{\lambda^2}{1-\lambda^2} \\ 1 & \frac{1}{\lambda} \end{pmatrix} \in SL(2,q^2)$$

has the property $M^{-1} d_\lambda M = x$. Since $Stab_{SL(2,q^2)}(d_\lambda) = \{d_\mu \mid \mu \in \mathbb{F}_{q^2}^*\}$, we find that

$$\begin{aligned} \mathfrak{S}(x) = Stab_{SL(2,q)}(x) &= SL(2,q) \cap Stab_{SL(2,q^2)}(x) \\ &= SL(2,q) \cap Stab_{SL(2,q^2)}(M^{-1} d_\lambda M) \\ &= SL(2,q) \cap M^{-1} Stab_{SL(2,q^2)}(d_\lambda) M \\ &= SL(2,q) \cap M^{-1} \left\langle d_{\zeta_{q^2-1}} \right\rangle M, \end{aligned}$$

where ζ_{q^2-1} is a fixed generator of the group $\mathbb{F}_{q^2}^*$. On the other hand, recall that by lemma 4.2.1, $\mathfrak{S}(x)$ is cyclic of order $q+1$. But a cyclic group of order q^2-1 has a unique subgroup of order $q+1$; in our case, we find

$$\mathfrak{S}(x) = M^{-1} \left\langle d_{\zeta_{q^2-1}}^{q-1} \right\rangle M. \tag{4.7}$$

We will denote the generator of $\mathfrak{S}(x)$ by γ_x. Thus $\gamma_x = M^{-1} d_{\zeta_{q^2-1}}^{q-1} M$. Conjugating an element of $SL(2,q)$ by γ_x looks however quite complicated in general, and we won't be able to write down, for arbitrary q, an explicit set of $\mathfrak{S}(x)$-class representatives.

Remark 4.4.3
A very inefficient and straightforward method for computing a set of $\mathfrak{S}(x)$-class representatives, in a fixed group $SL(2,q)$, is the following: Let *dom* := $SL(2,q)$ as a set, and define *reps* := $\emptyset$. Now pick an element in *dom*, add it to *reps*, and remove the set $y^{\mathfrak{S}(x)} = \{z^{-1}yz \mid z \in \mathfrak{S}(x)\}$ from *dom*. Repeat this process until *dom* is empty; then *reps* is a set of $\mathfrak{S}(x)$-class representatives. This method applies of course to any element x, in an arbitrary finite group G ■

Let us finally mention a criterion which ensures that two elements x, y in $SL(2,q)$ do not generate $SL(2,q)$. Notice that the pairs (x,y) in equations (4.2)-(4.6) have the property that x, y and I are linearly independent over $\mathbb{F}_q$. The same holds for pairs (x,y) if x has an eigenvalue polynomial which is irreducible over $\mathbb{F}_q$, and if $y \notin \mathfrak{S}(x)$ (indeed, the proof of lemma 4.2.1 shows that $\mathfrak{S}(x) = \{aI + bx \mid a,b \in \mathbb{F}_q \text{ and } det(aI+bx) = 1\}$. This means that $y \in SL(2,q)$ depends on I and x if and only if $y \in \mathfrak{S}(x)$). Thus for all potential pairs (x,y) of generators of $SL(2,q)$, the matrices x, y and I are linearly independent over $\mathbb{F}_q$.

Lemma 4.4.4
For the above constructed potential pairs (x,y) of generators of $SL(2,q)$, we have:

a) *If both xy and yx depend linearly on x, y and I over $\mathbb{F}_q$, then $< x,y > \lneqq SL(2,q)$;*

b) *If the field generated by the entries of the matrices x and y is strictly smaller than $\mathbb{F}_q$, then $< x,y > \lneqq SL(2,q)$.*

PROOF: a) We denote by $< x,y >_R$ the smallest unitary ring containing all the elements of $< x,y >$ (the *group* generated by x and y under multiplication; notice that $< x,y > \subset < x,y >_R$), and by $< x,y >_{\mathbb{F}_q}$ the vector space over $\mathbb{F}_q$ spanned by the elements of $< x,y >_R$. By the Cayley-Hamilton theorem, there are relations $x^{-1} = trace(x) - x$; $y^{-1} = trace(y) - y$; $x^2 = trace(x)x - I$; and $y^2 = trace(y)y - I$. Now, if also xy and yx depend on x, y and I over $\mathbb{F}_q$, it follows that all the elements of $< x,y >$ are contained in $\mathbb{F}_q x \oplus \mathbb{F}_q y \oplus \mathbb{F}_q I$, and therefore $< x,y >_R$, which consists of all the finite sums of elements of $< x,y >$, is contained in $\mathbb{F}_q x \oplus \mathbb{F}_q y \oplus \mathbb{F}_q I$ as well. Thus $< x,y >_{\mathbb{F}_q} = \mathbb{F}_q x \oplus \mathbb{F}_q y \oplus \mathbb{F}_q I$ is three-dimensional.

Therefore it is sufficient to show that if x and y generate $SL(2,q)$, then $< x,y >_{\mathbb{F}_q}$ is four-dimensional. Suppose $< x,y >= SL(2,q)$. Then $\left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ \lambda & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ -1 & \lambda \end{smallmatrix}\right), \left(\begin{smallmatrix} \lambda & 1 \\ -1 & 0 \end{smallmatrix}\right), I$ and

$-I$ are all contained in $< x,y >_R$ (where λ denotes a generator of $\mathbb{F}_q^*$). Therefore also $\left(\begin{smallmatrix}\alpha & 0\\ 0 & 0\end{smallmatrix}\right), \left(\begin{smallmatrix}0 & \alpha\\ 0 & 0\end{smallmatrix}\right), \left(\begin{smallmatrix}0 & 0\\ \alpha & 0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0 & 0\\ 0 & \alpha\end{smallmatrix}\right) \in < x,y >_R$ for all $\alpha \in \mathbb{F}_q$. It follows that $Mat(2,\mathbb{F}_q) = < x,y >_R \subset < x,y >_{\mathbb{F}_q} \subset Mat(2,\mathbb{F}_q)$, hence $dim_{\mathbb{F}_q}(< x,y >_{\mathbb{F}_q}) = 4$.

b) This is clear ■

This section can be summarized in the form of an algorithm, which is displayed on page 33. The function **generators** is Boolean valued, and returns *true* iff x and y generate $SL(2,q)$. It checks if one of the conditions a) and b) in lemma 4.4.4 holds [4]. If none of both holds, it checks with brute force if x and y generate $SL(2,q)$ (in GAP for instance, the answer to this question is given by `Group(x,y) = SL(2,q)`).

One can of course adapt the algorithm easily to characteristic 2, because besides the choice of the conjugacy class representatives x, no use has been made of the odd characteristic.

4.5 Lists of Admissible Triples for Small Odd q

We have implemented algorithm 1 in GAP [GAP]. Given an odd prime p, and q a p-power, let us define sets $\mathtt{p} := \{p, 2p\}$, $\mathtt{q}_- := \{n > 2 \text{ dividing } q-1\}$ and $\mathtt{q}_+ := \{n > 2 \text{ dividing } q+1\}$. For each pair (x,y) generated by the algorithm (thus $< x,y >= SL(2,q)$), we have computed the triple $\{|x|,|y|,|xy|\}$, and ordered it in such a way, that multiples of p precede divisors of $q-1$, and divisors of $q-1$ precede divisors of $q+1$. For each such ordered triple t, we have finally counted the number of (x,y) in the output of the algorithm, which have the property $\{|x|,|y|,|xy|\} = t$ (so this number equals the number of distinct Galois $SL(2,q)$-covers which are unbranched outside $\{0,1,\infty\}$ and have unordered branch type t, up to equivalence; it is listed in the column #). In the tables below, we have listed for the six smallest odd q these ordered triples together with the number of their occurrences. The tables should be understood as follows: The column under ordered triple (set_1, set_2, set_3) contains all the admissible triples (g_1,g_2,g_3) of $SL(2,q)$, ordered in the above explained way, with the property $g_i \in set_i$ for $i = 1,2,3$.

It follows from the Hurwitz genus formula that if $f : C \to \mathbb{P}^1$ is a covering with Galois group $SL(2,q)$ and branch type (e_0,e_1,e_∞), then the genus

$$g(e_0,e_1,e_\infty) := g(C) = \frac{q^3-q}{2}\left(1 - \frac{1}{e_0} - \frac{1}{e_1} - \frac{1}{e_\infty}\right) + 1.$$

For $q = 3$ and 5 we have added this genus g to the table, to illustrate how large the genera of $SL(2,q)$-coverings can become, even for the smallest q. For example, the genus g of an $SL(2,13)$-covering satisfies $209 = g(3,3,7) \le g \le g(26,26,26) = 967$.

[4] One easily checks if a) holds: Associate to a 2×2 matrix $M = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$ the vector $v_M := (a,b,c,d)$. Four 2×2 matrices $M_1, \ldots, M_4$ over $\mathbb{F}_q$ are linearly dependent if and only if the 4×4 matrix, the columns of which are the $v_{M_i}^T$, has zero determinant.

INPUT: an odd prime power $q = p^n \geq 3$.
STEP 0: (initialization)
ζ is a fixed generator of $\mathbb{F}_q^*$;
μ is a fixed generator of $\mathbb{F}_{q^2}^*$;
adm_pairs := $\emptyset$; % will contain those pairs in lemma 4.4.2, which generate $SL(2,q)$.
adm_triples := $\emptyset$; % will be a set of representatives of $Adm(SL(2,q))/\sim$.
STEP 1: (first type of conjugacy class representatives x)
for x *in* $\{\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&\zeta\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1&1\\0&-1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1&\zeta\\0&-1\end{smallmatrix}\right)\}$ **do**
  for c *in* $\mathbb{F}_q^*$ **do**
    for t *in* $\mathbb{F}_q$ **do**
      $y := \left(\begin{smallmatrix}0&-c^{-1}\\c&t\end{smallmatrix}\right)$; % thus (x,y) runs through the pairs in (4.2)
      if generators $(x,y,q) = true$ **then**
        add (x,y) to the set *adm_pairs* ;
      endif;
    endfor;
  endfor;
endfor;
STEP 2: (second type of conjugacy class representatives x)
for each unordered pair $\{\lambda, \lambda^{-1}\}$, with $\lambda \in \mathbb{F}_q^* \setminus \{\pm 1\}$ **do**
  $x := \left(\begin{smallmatrix}\lambda&0\\0&\lambda^{-1}\end{smallmatrix}\right)$;
  for y as in (4.3)-(4.6) **do**
    if generators $(x,y,q) = true$ **then**
      add (x,y) to the set *adm_pairs* ;
    endif;
  endfor;
endfor;
STEP 3: (third type of conjugacy class representatives)
for $t = \lambda + \lambda^{-1}$ *in* $\mathbb{F}_q$ with $T^2 - tT + 1$ irreducible in $\mathbb{F}_q[T]$ **do**
  $x := \left(\begin{smallmatrix}0&-1\\1&t\end{smallmatrix}\right)$;
  use the brute-force-method (remark 4.4.3) to compute a set Σ of $\mathfrak{S}(x)$-class representatives in $SL(2,q) \setminus \mathfrak{S}(x)$ (the generator of $\mathfrak{S}(x)$ is given by (4.7); its entries can be expressed in μ and λ);
  for y *in* Σ **do**
    if generators $(x,y,q) = true$ **then**
      add (x,y) to the set *adm_pairs* ;
    endif;
  endfor;
endfor;
STEP 4: (computing the admissible triples modulo equivalence)
adm_triples := $\{(x,y,xy) \mid (x,y) \in$ *adm_pairs* $\}$;
OUTPUT: *adm_triples* is a set of representatives of $Adm(SL(2,q))/\sim$,
that is, it represents the set of $SL(2,q)$-covers of $\mathbb{P}^1(\mathbb{C})$
which are unbranched outside $\{0,1,\infty\}$, modulo equivalence.

Algorithm 1: Computing admissible triples in $SL(2,q)$ modulo equivalence, for odd q.

$q = 3$: $\mathfrak{q}_- = \emptyset$, $\mathfrak{q}_+ = \{4\}$.

$(\mathfrak{p},\mathfrak{p},\mathfrak{p})$	g	#	$(\mathfrak{p},\mathfrak{p},+)$	g	#
(3,3,6)	3	6	(3,3,4)	2	6
(6,6,6)	7	2	(3,6,4)	4	12
			(6,6,4)	6	6

$q = 5$: $\mathfrak{q}_- = \{4\}$, $\mathfrak{q}_+ = \{3,6\}$.

$(\mathfrak{p},\mathfrak{p},\mathfrak{p})$	g	#	$(\mathfrak{p},\mathfrak{p},-)$	g	#	$(\mathfrak{p},\mathfrak{p},+)$	g	#	$(\mathfrak{p},-,+)$	g	#	$(\mathfrak{p},+,+)$	g	#
(5,5,10)	31	6	(5,5,4)	22	6	(5,5,3)	17	6	(5,4,3)	14	12	(5,3,6)	19	12
(10,10,10)	43	2	(5,10,4)	28	12	(5,5,6)	27	6	(5,4,6)	24	12	(10,3,3)	15	6
			(10,10,4)	34	6	(5,10,3)	23	12	(10,4,3)	20	12	(10,6,6)	35	6
						(5,10,6)	33	12	(10,4,6)	30	12			
						(10,10,3)	29	6						
						(10,10,6)	39	6						

$q = 7$: $\mathfrak{q}_- = \{3,6\}$, $\mathfrak{q}_+ = \{4,8\}$.

$(\mathfrak{p},\mathfrak{p},\mathfrak{p})$	#	$(\mathfrak{p},\mathfrak{p},-)$	#	$(\mathfrak{p},\mathfrak{p},+)$	#	$(\mathfrak{p},-,-)$	#	$(\mathfrak{p},-,+)$	#
(7,7,14)	6	(7,7,3)	6	(7,7,4)	6	(7,3,6)	12	(7,3,4)	12
(14,14,14)	2	(7,7,6)	6	(7,7,8)	12	(14,3,3)	6	(7,3,8)	24
		(7,14,3)	12	(7,14,4)	12	(14,6,6)	6	(7,6,4)	12
		(7,14,6)	12	(7,14,8)	24			(7,6,8)	24
		(14,14,3)	6	(14,14,4)	6			(14,3,4)	12
		(14,14,6)	6	(14,14,8)	12			(14,3,8)	24
								(14,6,4)	12
								(14,6,8)	24

$(\mathfrak{p},+,+)$	#	$(-,-,-)$	#	$(-,-,+)$	#	$(-,+,+)$	#	$(+,+,+)$	#
(7,4,8)	24			(3,3,8)	12	(3,8,8)	12	(8,8,8)	16
(7,8,8)	12			(3,6,8)	24	(6,8,8)	12		
(14,4,8)	24			(6,6,8)	12				
(14,8,8)	12								

$q = 3^2$: $\mathfrak{q}_- = \{4,8\}$, $\mathfrak{q}_+ = \{5,10\}$.

$(\mathfrak{p},\mathfrak{p},\mathfrak{p})$	#	$(\mathfrak{p},\mathfrak{p},-)$	#	$(\mathfrak{p},\mathfrak{p},+)$	#	$(\mathfrak{p},-,-)$	#	$(\mathfrak{p},-,+)$	#
		(3,3,8)	12	(3,3,5)	12			(3,8,5)	48
		(3,6,8)	24	(3,6,10)	24			(3,8,10)	48
		(6,6,8)	12	(6,6,5)	12			(6,8,5)	48
								(6,8,10)	48

$(\mathfrak{p},+,+)$	#	$(-,-,-)$	#	$(-,-,+)$	#	$(-,+,+)$	#	$(+,+,+)$	#
(3,5,10)	24	(8,8,8)	16	(4,8,5)	48	(4,5,5)	12	(5,5,5)	4
(6,5,5)	12			(4,8,10)	48	(4,5,10)	24	(5,5,10)	36
(6,10,10)	12			(8,8,5)	48	(4,10,10)	12	(5,10,10)	12
				(8,8,10)	48	(8,5,5)	48	(10,10,10)	12
						(8,5,10)	96		
						(8,10,10)	48		

$q = 11$: $\mathfrak{q}_- = \{5,10\}$, $\mathfrak{q}_+ = \{3,4,6,12\}$.

$(\mathfrak{p},\mathfrak{p},\mathfrak{p})$	#	$(\mathfrak{p},\mathfrak{p},-)$	#	$(\mathfrak{p},\mathfrak{p},+)$	#	$(\mathfrak{p},-,-)$	#	$(\mathfrak{p},-,+)$	#
(11,11,22)	6	(11,11,5)	12	(11,11,3)	6	(11,5,5)	12	(11,5,3)	24
(22,22,22)	2	(11,11,10)	12	(11,11,4)	6	(11,5,10)	48	(11,5,4)	24
		(11,22,5)	24	(11,11,6)	6	(11,10,10)	12	(11,5,6)	24
		(11,22,10)	24	(11,11,12)	12	(22,5,5)	24	(11,5,12)	48
		(22,22,5)	12	(11,22,3)	12	(22,5,10)	24	(11,10,3)	24
		(22,22,10)	12	(11,22,4)	12	(22,10,10)	24	(11,10,4)	24

continued on next page...

...continued from previous page

$(\mathfrak{p},+,+)$	#	$(-,-,-)$	#	$(-,-,+)$	#	$(-,+,+)$	#	$(+,+,+)$	#
				(11, 22, 6)	12			(11, 10, 6)	24
				(11, 22, 12)	24			(11, 10, 12)	48
				(22, 22, 3)	6			(22, 5, 3)	24
				(22, 22, 4)	6			(22, 5, 4)	24
				(22, 22, 6)	6			(22, 5, 6)	24
				(22, 22, 12)	12			(22, 5, 12)	48
								(22, 10, 3)	24
								(22, 10, 4)	24
								(22, 10, 6)	24
								(22, 10, 12)	48

$(\mathfrak{p},+,+)$	#	$(-,-,-)$	#	$(-,-,+)$	#	$(-,+,+)$	#	$(+,+,+)$	#
(11, 3, 4)	12	(5, 5, 5)	4	(5, 5, 3)	12	(5, 3, 3)	12	(3, 3, 12)	12
(11, 3, 6)	12	(5, 5, 10)	36	(5, 5, 4)	12	(5, 3, 12)	48	(3, 6, 12)	24
(11, 3, 12)	24	(5, 10, 10)	12	(5, 5, 6)	12	(5, 4, 12)	48	(3, 12, 12)	12
(11, 4, 6)	12	(10, 10, 10)	12	(5, 5, 12)	48	(5, 6, 6)	12	(4, 12, 12)	24
(11, 4, 12)	24			(5, 10, 3)	24	(5, 6, 12)	48	(6, 6, 12)	12
(11, 6, 12)	24			(5, 10, 4)	24	(5, 12, 12)	48	(6, 12, 12)	12
(11, 12, 12)	12			(5, 10, 6)	24	(10, 3, 6)	24	(12, 12, 12)	16
(22, 3, 3)	6			(5, 10, 12)	96	(10, 3, 12)	48		
(22, 3, 4)	12			(10, 10, 3)	12	(10, 4, 12)	48		
(22, 3, 12)	24			(10, 10, 4)	12	(10, 6, 12)	48		
(22, 4, 6)	12			(10, 10, 6)	12	(10, 12, 12)	48		
(22, 4, 12)	24			(10, 10, 12)	48				
(22, 6, 6)	6								
(22, 6, 12)	24								
(22, 12, 12)	12								

$q = 13$: $\mathfrak{q}_- = \{3, 4, 6, 12\}$, $\mathfrak{q}_+ = \{7, 14\}$.

$(\mathfrak{p},\mathfrak{p},\mathfrak{p})$	#	$(\mathfrak{p},\mathfrak{p},-)$	#	$(\mathfrak{p},\mathfrak{p},+)$	#	$(\mathfrak{p},-,-)$	#	$(\mathfrak{p},-,+)$	#
(13, 13, 26)	6	(13, 13, 3)	6	(13, 13, 7)	18	(13, 3, 4)	12	(13, 3, 7)	36
(26, 26, 26)	2	(13, 13, 4)	6	(13, 13, 14)	18	(13, 3, 6)	12	(13, 3, 14)	36
		(13, 13, 6)	6	(13, 26, 7)	36	(13, 3, 12)	24	(13, 4, 7)	36
		(13, 13, 12)	12	(13, 26, 14)	36	(13, 4, 6)	12	(13, 4, 14)	36
		(13, 26, 3)	12	(26, 26, 7)	18	(13, 4, 12)	24	(13, 6, 7)	36
		(13, 26, 4)	12	(26, 26, 14)	18	(13, 6, 12)	24	(13, 6, 14)	36
		(13, 26, 6)	12			(13, 12, 12)	12	(13, 12, 7)	72
		(13, 26, 12)	24			(26, 3, 3)	6	(13, 12, 14)	72
		(26, 26, 3)	6			(26, 3, 4)	12	(26, 3, 7)	36
		(26, 26, 4)	6			(26, 3, 12)	24	(26, 3, 14)	36
		(26, 26, 6)	6			(26, 4, 6)	12	(26, 4, 7)	36
		(26, 26, 12)	12			(26, 4, 12)	24	(26, 4, 14)	36
						(26, 6, 6)	6	(26, 6, 7)	36
						(26, 6, 12)	24	(26, 6, 14)	36
						(26, 12, 12)	12	(26, 12, 7)	72
								(26, 12, 14)	72

$(\mathfrak{p},+,+)$	#	$(-,-,-)$	#	$(-,-,+)$	#	$(-,+,+)$	#	$(+,+,+)$	#
(13, 7, 7)	36	(3, 3, 12)	12	(3, 3, 7)	18	(3, 7, 7)	54	(7, 7, 7)	24
(13, 7, 14)	108	(3, 6, 12)	24	(3, 3, 14)	18	(3, 7, 14)	108	(7, 7, 14)	162
(13, 14, 14)	36	(3, 12, 12)	12	(3, 4, 7)	36	(3, 14, 14)	54	(7, 14, 14)	72
(26, 7, 7)	54	(4, 12, 12)	24	(3, 4, 14)	36	(4, 7, 7)	54	(14, 14, 14)	54
(26, 7, 14)	72	(6, 6, 12)	12	(3, 6, 7)	36	(4, 7, 14)	108		
(26, 14, 14)	54	(6, 12, 12)	12	(3, 6, 14)	36	(4, 14, 14)	54		

continued on next page...

...continued from previous page

(p,+,+)	#	(−,−,−)	#	(−,−,+)	#	(−,+,+)	#	(+,+,+)	#
		(12,12,12)	16	(3,12,7)	72	(6,7,7)	54		
				(3,12,14)	72	(6,7,14)	108		
				(4,6,7)	36	(6,14,14)	54		
				(4,6,14)	36	(12,7,7)	108		
				(4,12,7)	72	(12,7,14)	216		
				(4,12,14)	72	(12,14,14)	108		
				(6,6,7)	18				
				(6,6,14)	18				
				(6,12,7)	72				
				(6,12,14)	72				
				(12,12,7)	72				
				(12,12,14)	72				

Finally, for $p = 2$ and $q = 2, 4, 8$ a computation yielded the following tables of branch types of the groups $SL(2,q)$:

$q = 2$: $\mathfrak{q}_- = \emptyset$, $\mathfrak{q}_+ = \{3\}$.

(p,p,+)	g	#
(2,2,3)	0	3

$q = 4$: $\mathfrak{q}_- = \{3\}$, $\mathfrak{q}_+ = \{5\}$.

(p,−,+)	g	#	(p,+,+)	g	#	(−,−,+)	g	#	(−,+,+)	g	#	(+,+,+)	g	#
(2,3,5)	0	12	(2,5,5)	4	6	(3,3,5)	5	6	(3,5,5)	9	12	(5,5,5)	13	2

$q = 8$: $\mathfrak{q}_- = \{7\}$, $\mathfrak{q}_+ = \{3,9\}$.

(p,p,p)	g	#	(p,p,−)	g	#	(p,p,+)	g	#	(p,−,−)	g	#	(p,−,+)	g	#
									(2,7,7)	55	18	(2,7,3)	7	18
												(2,7,9)	63	54

(p,+,+)	g	#	(−,−,−)	g	#	(−,−,+)	g	#	(−,+,+)	g	#	(+,+,+)	g	#
(2,3,9)	15	18	(7,7,7)	145	12	(7,7,3)	97	27	(7,3,9)	105	54	(3,3,9)	57	9
(2,9,9)	71	18				(7,7,9)	153	81	(7,9,9)	161	81	(3,9,9)	113	9
												(9,9,9)	169	18

The tables in this section show that for the prime powers q up to 13 the only branch types corresponding to a rational (i.e. genus zero) or elliptic (genus one) $SL(2,q)$-covering branched above three points are the triples $(2,2,3)$ if $q = 2$ and $(2,3,5)$ if $q = 4$, both of which correspond to genus zero. In the next chapter we show that *the only* $SL(2,q)$-*coverings* of $\mathbb{P}^1(\mathbb{C})$ unbranched outside $\{0,1,\infty\}$ of *genus at most one* are in fact the rational $SL(2,2)$-covers of type $(2,2,3)$ and the rational $SL(2,4)$-covers of type $(2,3,5)$.

Chapter 5

$SL(2,q)$-Covers of Genus 0 and 1

As we have said in the introduction, we are mainly interested in Galois coverings of $\mathbb{P}^1$ with group $SL(2,q)$ and branch points above $0, 1$ and ∞ only. In this chapter we will find all the rational and elliptic Galois $SL(2,q)$-covers of $\mathbb{P}^1$. Actually, it turns out that there are almost no such. Theorem 6 tells us that $f : C_1 \to C_2$ is a Galois G-cover if and only if it is the quotient of C_1 by the group $Aut(C_1/C_2)$, with $G \cong Aut(C_1/C_2)$. Thus our first task is to determine all the finite subgroups of $Aut(C_1)$, in the case where C_1 is a curve of genus 0 or 1, and to find out which of them are isomorphic to some $SL(2,q)$.

5.1 Investigation of the Finite Subgroups of $Aut(\mathbb{P}^1)$

In this section, K denotes an algebraically closed field of arbitrary characteristic $p := char(K) \geq 0$. We will find all the prime-powers q (not necessarily of the prime p), for which $SL(2,q)$ can be embedded in $Aut(\mathbb{P}^1)$. It is known that $Aut(\mathbb{P}^1(K)) \cong PGL(2,K)$ (see Exercise I.6.6 and Example II.7.1 [Hart], or Lecture 18 [Harr]), and the first proposition of this chapter gives a complete list of the finite subgroups of $PGL(2,K)$:

Proposition 5.1.1
The finite subgroups G of $PGL(2,K)$ are:

	$G \cong$	$char(K) =$
1	$Q_m := \underbrace{\mathbb{Z}_p \times \ldots \times \mathbb{Z}_p}_{m \text{ factors}}$ for $m \geq 1$	$p \geq 2$
2	C_n for $n \geq 1$, and $g.c.d.(n,p) = 1$ if $p \geq 2$	$p \geq 0$
3	$D_{2\times m}$ for $m \geq 2$, and $g.c.d.(m,p) = 1$ if $p \geq 2$	$p \geq 0$
4	A_4 and A_5	$p \geq 0$
5	S_4	$p \neq 2$
6	$Q_m \rtimes C_n$ for $m \geq 1$ and $n \mid p^m - 1$	$p \geq 2$
7	$PSL(2,p^m)$ and $PGL(2,p^m)$ for $m \geq 1$	$p \geq 2$

PROOF: For the nonzero characteristic case, see [VM]. The finite subgroups of $PGL(2,\mathbb{C})$ can be found in a book of Weber [We]. Finally, as Serre [Se] notices, one can use the *Lefschetz principle* to generalize from $\mathbb{C}$ to arbitrary fields of characteristic zero: Let F be an arbitrary field of characteristic zero, and let $G = \left\{ \left(\begin{smallmatrix} a_1 & b_1 \\ c_1 & d_1 \end{smallmatrix}\right), \left(\begin{smallmatrix} a_2 & b_2 \\ c_2 & d_2 \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} a_n & b_n \\ c_n & d_n \end{smallmatrix}\right) \right\} \subset Aut(\mathbb{P}^1(F))$ be a finite subgroup (where $a_i, b_i, c_i, d_i \in F$). Define the subfield $E := \mathbb{Q}(a_1, b_1, c_1, d_1, a_2, \ldots, d_n) \subset F$. We can embed E in $\mathbb{C}$, so we have $G \subset PGL(2,E) \subset PGL(2,\mathbb{C})$. Thus G is a finite subgroup of $Aut(\mathbb{P}^1(\mathbb{C}))$, and can be found in Weber's list. (Notice that this doesn't prove that each group in the list indeed occurs as subgroup of $PGL(2,F)$!) ■

In each of the above seven classes of groups, we check which groups are isomorphic to some $SL(2,q)$. The groups in 1. and 2. are Abelian and therefore not special linear. So we start with case 3. As before, we denote by $p \geq 0$ the characteristic of K, and we suppose that q is a power of the prime $p' \geq 2$. We will use in the remainder of this chapter the properties of $SL(2,q)$ from chapter 4 and appendix A.

3) Each dihedral group $D_{2\times n}$ has an element of order n, which generates a subgroup of index 2, which therefore is normal. But for $q > 3$, the only normal subgroup of $SL(2,q)$ is the center $\{\pm I\}$. So only if $q = 2, 3$ we possibly have $D_{2\times n} \cong SL(2,q)$ (in which case n equals 3 resp. 12). However, D_{24} contains an element of order 12, whereas elements in $SL(2,3)$ have order at most 6. The remaining group D_6 has a presentation $< a, b \mid a^3 = b^2 = baba = 1 >$, and $SL(2,2)$ contains the two matrices $A := \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and $B := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, which generate $SL(2,2)$ and satisfy the relations for D_6. We conclude that the only dihedral group which is isomorphic to some $SL(2,q)$ is $D_6 \cong SL(2,2)$. Notice that this group is *not* contained in $PGL(2,K)$ if $p = 3$.

4) The size of A_4 is 12, not the size of a special linear group. We will however show that A_5 is isomorphic to $SL(2,4)$. Both these groups have order 60, and are simple, so it suffices to show that, up to isomorphism, there exists only one simple group of order 60. The next lemma will be used in showing that every simple group of order 60 can be embedded in S_5.

Lemma 5.1.2
Let H be a subgroup of a group G, and denote by R the set of right cosets of H in G. The map $\rho : G \to Sym(R)$, defined by $\rho(g) : Hx \mapsto Hxg$, is a transitive permutation representation, with kernel the core H_G (i.e. the largest normal subgroup of G which is contained in H).

PROOF: Proposition 1.6.6 [R] ■

Suppose that we are given a simple group G of order $60 = 2^2 \times 3 \times 5$. Denote by n_p the number of Sylow p-subgroups of G. By Sylow's theorem we have $n_2 = 3, 5$ or 15; $n_3 = 4$ or 10; and $n_5 = 6$. Since distinct Sylow 3-subgroups have no nontrivial

elements in common, we count at least $4(3-1) = 8$ elements of order 3 in G. Similarly, there are $6(5-1) = 24$ elements of order 5 in G. Two distinct Sylow 2-subgroups of G cannot have more than 2 elements in common. It follows that if $n_2 = 15$, the group G contains at least $1 + 8 + 24 + 15(4-2) = 63$ elements, which is absurd.

Suppose that $n_2 = 3$. This means that G contains a subgroup of index 3 (namely the normalizer of a Sylow 2-subgroup). Since G is simple, by lemma 5.1.2 there is an injection $G \hookrightarrow S_3$, which is impossible.

It follows that $n_2 = 5$. Again by the lemma, we obtain an injection $G \hookrightarrow S_5$. So G is a normal subgroup of index 2 in S_5. By simplicity of A_5, and since $G \cap A_5 \lhd A_5$, we either have $G \cap A_5 = \{(1)\}$ (which is impossible, since then $|G \cdot A_5| = |G| \cdot |A_5| > |S_5|$), or $G \cap A_5 = A_5$ (i.e. $G = A_5$). As a consequence, $A_5 \cong SL(2,4)$.

5) The symmetric group S_4, which satisfies $|S_4| = |SL(2,3)| = 24$, can be seen not to be isomorphic with $SL(2,3)$, by noting that $SL(2,3)$ has only one involution, though S_4 has many.

6) Suppose that $SL(2,q) \cong Q_m \rtimes C_n$. We must have $p' \neq 2$, since otherwise $SL(2,q)$ has no nontrivial normal subgroups, although Q_m is normal. For $p' \neq 2$ the only nontrivial normal subgroup is $\{\pm 1\}$, hence $Q_m = C_2$, with $m = 1$ and $p = 2$. Since $n \mid p^m - 1 = 1$, we see that $Q_m \rtimes C_n$ was just the cyclic group C_2.

7) Of course, $PSL(2,p^m)$ equals $SL(2,p^m)$ if $p = 2$. In general, for $p^m \geq 4$ the group $PSL(2,p^m)$ is simple, so not isomorphic with any $SL(2,q)$, $p' \neq 2$. Also, $PSL(2,3) \cong A_4$ is not special linear, as we mentioned earlier. We may conclude that the only $PSL(2,p^m)$ which are at the same time special linear, are these with $p = 2$; they occur only if $char(K) = 2$.

$PGL(2,p^m)$ has order $(p^m)^3 - p^m = |SL(2,p^m)|$. For natural numbers r and s, one has $r^3 - r = s^3 - s$ if and only if $r = s$. So if $PGL(2,p^m)$ is special linear, it must be isomorphic with $SL(2,p^m)$. However, $PGL(2,p^m)$ contains the subgroup $PSL(2,p^m)$. For $p \geq 3$ this subgroup has index 2, so is normal. Since $SL(2,q)$ has no normal subgroup of index 2 for $q \geq 3$, it follows that $PGL(2,p^m)$ is *not* isomorphic with $SL(2,p^m)$, whenever $p \neq 2$. On the other hand, if $p = 2$, we have $PGL(2,p^m) = PSL(2,p^m) = SL(2,p^m)$.

We have proven the following proposition:

Proposition 5.1.3
Let K be an algebraically closed field of characteristic $p \geq 0$. If G is a finite subgroup of $Aut(\mathbb{P}^1(K))$, which is isomorphic with some $SL(2,q)$, then we are in one of the following three situations:

i) $q = 2$ *and* $p \neq 3$;

ii) $q = 4$ *and* $p \geq 0$;

iii) $q = 2^m$, $m \geq 3$ *and* $p = 2$ ■

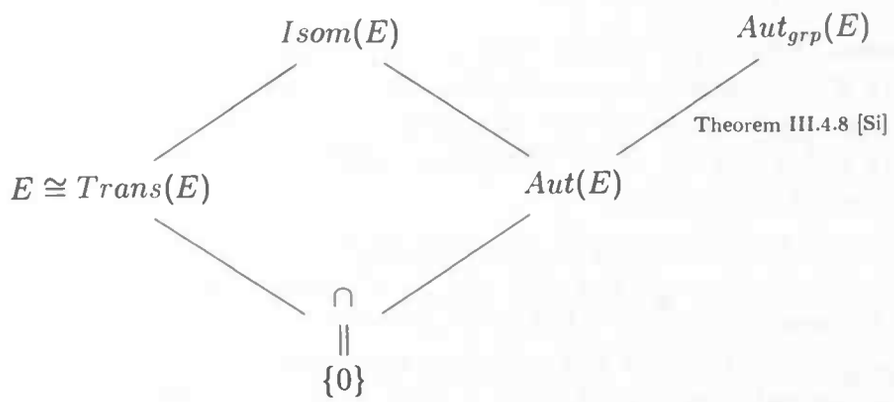
5.2 Investigation of the Isomorphism Group of an Elliptic Curve

We let the genus increase by one, and try to find out what kind of elliptic covers of $\mathbb{P}^1$ with Galois group $SL(2,q)$ exist. As in the rational case, this comes down to finding all the finite subgroups of the form $SL(2,q)$ of the automorphism group of an elliptic curve. In the present section, we follow the terminology in [Si]; in particular, we have to adapt our notations concerning automorphism groups. Thus, if E is an elliptic curve with identity element $0 \in E$, we write

$$Aut(E) := \{\text{invertible isogenies } \phi : E \to E\};$$
$$Isom(E) := \{\text{isomorphisms of the } \textit{variety } E\};$$

in this new terminology, we are interested in the finite subgroups of $Isom(E)$. Furthermore, we will denote the group of automorphisms of the underlying group of E by $Aut_{grp}(E)$. In this section, the group law in both $Aut(E)$ and $Aut_{grp}(E)$ will be denoted by $\phi\psi := \phi \circ \psi$.

The group $Trans(E)$ of translations τ_P of E will be identified with E. We have the following diagram of group inclusions:



Throughout this section, K is assumed to have characteristic zero, since in that case the groups E and $Aut(E)$ are particularly nice to work with.

Definition 5.2.1
Let two groups H and N be given, with a group homomorphism $\alpha : H \to Aut(N)$. For $h \in H$ and $n \in N$, we write $n^h := \alpha(h)(n)$. We define the *product* $N \rtimes^{\alpha} H$ *of* N *and* H *twisted by the homomorphism* α to be the set $N \times H$ together with the group law $(n_1, h_1)(n_2, h_2) := (n_1 n_2^{h_1}, h_1 h_2)$ ■

The next lemma describes the groups E and $Aut(E)$, and expresses $Isom(E)$ as a twisted product of the two former groups.

Lemma 5.2.2
Let $(E,0)$ be an elliptic curve over an algebraically closed field K of characteristic 0, with j-invariant $j := j(E)$. Denote by $E \rtimes Aut(E)$ the product of E and $Aut(E)$ twisted by the injection $Aut(E) \hookrightarrow Aut_{grp}(E)$.

(a) The map $(P,\alpha) \mapsto \tau_P \circ \alpha$ defines an isomorphism $E \rtimes Aut(E) \cong Isom(E)$.

(b) If $K = \mathbb{C}$, as a group $E \cong \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$. In general, the subgroup $E[m] \leq E$ (i.e. the torsion elements of order dividing m) is isomorphic to $C_m \times C_m$.

(c) The automorphism group of E is finite, and is described in the following table:

j	$Aut(E)$
$\neq 0, 1728$	C_2
$1728 = 2^6 3^3$	C_4
0	C_6

PROOF: (a) Proposition X.5.1 [Si].
(b) Corollary III.6.4 [Si] and Theorem IV.4.16 [Hart].
(c) Theorem III.10.1 [Si] ■

In the sequel we identify $Isom(E)$ with the twisted product in (a), and we identify E and $Aut(E)$ with the subgroups $\{(P,id) \mid P \in E\}$ resp. $\{(0,\alpha) \mid \alpha \in Aut(E)\}$ of $Isom(E)$.

It is shown in the third chapter of [Si], that an elliptic curve over a field K of characteristic $\neq 2,3$ is isomorphic to one given by an equation $Y^2 = X^3 + AX + B$, with $A, B \in K$. This allows us to assume, from now on, that our elliptic curves are of the form

$$E : Y^2 = X^3 + AX + B.$$

If the unique point at infinity is defined to be the identity $0 \in E$, then the *Group Law Algorithm* 2.3, P.58 [Si], gives us explicit formulas for the group operation on E: The inverse of a point $(x,y) \in E$ is $(x,-y)$, and the sum of two points (x_1,y_1) and $(x_2,y_2) \neq (x_1,-y_1)$ equals $(\lambda^2 - x_1 - x_2, -\lambda(\lambda^2 - x_1 - x_2) - \nu)$, where λ and ν are defined by

$$\lambda := \begin{cases} \frac{y_2-y_1}{x_2-x_1} & \text{if } x_1 \neq x_2, \\ \frac{3x_1^2+A}{2y_1} & \text{if } x_1 = x_2, \end{cases} \quad \text{and} \quad \nu := \begin{cases} \frac{y_1x_2-y_2x_1}{x_2-x_1} & \text{if } x_1 \neq x_2, \\ \frac{-x_1^3+Ax_1+2B}{2y_1} & \text{if } x_1 = x_2. \end{cases}$$

The proof of lemma 5.2.2(c) shows that the cyclic isomorphism group $Aut(E) \cong C_n$ of order n, of an elliptic curve E of the above normal form, is generated by the isogeny $\phi_n : E \to E : (x,y) \mapsto (\zeta^2 x, \zeta^3 y)$, where ζ denotes a fixed primitive n-th root of unity in $K = \bar{K}$. For $n = 2,4,6$ we have $\phi_n^{n/2} = [-1]$, the "multiplication by -1 map" (i.e. inversion in the *group* E). With this information, we can immediately compute the order of an element $(P,\phi) \in Isom(E)$.

An inductive argument shows that $(P,\phi)^m = (\Sigma_{i=0}^{m-1}\phi^i(P), \phi^m)$. Thus for all $(P,\phi) \in Isom(E)$ we have $ord(\phi) \mid ord(P,\phi)$. On the other hand, if $\phi \in Aut(E)$ is an element of order $k \neq 1,3$ (so $ord(\phi) = 2,4$ or 6), then there holds for all $P \in E$:

$$\sum_{i=0}^{k-1} \phi^i(P) = \sum_{i=0}^{(k/2)-1} (\phi^i(P) + \phi^i \circ [-1](P)) = 0.$$

If $\phi = id$ then of course $ord(P,\phi) = ord(P)$ for all $P \in E$. So it remains to find the order of elements (P,ϕ), where $\phi := \phi_6^2$, an isogeny of order 3. Recall that if such a ϕ exists, necessarily $j = 0$ (since $Aut(E) \cong C_6$) and $E : Y^2 = X^3 + 1$. In this remaining case we will use the formulas for addition in E (with $A = 0$ and $B = 1$), to show that $\sum_{i=0}^{3-1} \phi^i(P) = 0$. Denote the primitive third root of 1 which defines ϕ by ζ. This means that, for arbitrary $P = (x,y) \in E$, we must show that $(x,y) + (\zeta^2 x, y) + (\zeta x, y) = 0$. Suppose $x = 0$, in which case $y = 1$ or -1, and $\phi(P) = P$. Thus $\lambda = 0$ and $\nu = -1/y = -y$, and hence $P + \phi(P) = P + P = (x,y) + (x,y) = (x,-y) = -P = -\phi^2(P)$, in other words $ord(P,\phi) = 3$. Finally, assume that $x \neq 0$. Then $P + \phi(P) = (x,y) + (\zeta^2 x, y)$. The λ and ν defining the coordinates of this sum are $\lambda = 0$ and $\nu = (\zeta^2 xy - xy)/(\zeta^2 x - x) = y$. So it follows that again $P + \phi(P) = (-x - \zeta^2 x, -y) = (\zeta x, -y) = -(\zeta x, y) = -\phi^2(P)$ (since $1 + \zeta + \zeta^2 = 0$), and again $ord(P,\phi) = 3$.

This all is summarized in a lemma:

Lemma 5.2.3
Let E be an elliptic curve over a field of characteristic 0. The order of an arbitrary isomorphism $(P,\phi) \in Isom(E)$ is given by

$$ord(P,\phi) = \begin{cases} ord(P) & \text{if } \phi = id, \\ ord(\phi) & \text{if } \phi \neq id \end{cases} \quad \blacksquare$$

We can now easily derive that $Isom(E)$ contains only very few finite subgroups isomorphic to $SL(2,q)$. A calculation shows that E is normal in $Isom(E)$. Therefore, by the isomorphism theorem, if G is a subgroup of $Isom(E)$, we have $E \cap G \lhd G$. So G contains an Abelian normal subgroup, namely the subgroup of all translations in G.

Recall that for $q > 3$, the group $SL(2,q)$ has no other Abelian normal subgroups than $\{1\}$ and $Z(SL(2,q)) = \{\pm 1\}$. On the other hand, $SL(2,4)$ and $SL(2,5)$ contain elements of order 5, and for $q \geq 7$ the group $SL(2,q)$ contains an element of order $q+1 > 6$. Since $Aut(E)$ is cyclic of order 2, 4 or 6, no automorphism $\phi \in Aut(E)$ can have order 5 or order > 6. It follows from lemma 5.2.3 that if $G \cong SL(2,q)$ were a subgroup of $Isom(E)$, for some $q > 3$, then $E \cap G$ would contain an element of order at least 5. This would mean that the Abelian normal subgroup $E \cap G$ of G has size at least 5, which is impossible.

It remains to find out if $SL(2,2)$ and $SL(2,3)$ can be subgroups of $Isom(E)$. In the previous section we saw that $SL(2,2) \cong D_{2\times 3} \cong < a,b \mid a^3 = b^2 = baba = 1 >$. By

lemma 5.2.2(b), E contains an element P_0 of order 3. Also, the group $Aut(E)$ always contains the inversion map $[-1]$. The two elements (P_0, id) and $(0, [-1]) \in Isom(E)$ now generate a subgroup of $Isom(E)$ which is isomorphic to $SL(2,2)$. Thus, for each elliptic curve E over a field of characteristic zero, $Isom(E)$ contains a subgroup isomorphic to $SL(2,2)$.

Finally suppose that $SL(2,3) \leq Isom(E)$. The group $SL(2,3)$ consists of ± 1, eight elements of order 3, eight elements of order 6 and six elements of order 4 (this can be read off from the conjugacy class tables in chapter 4). Suppose that $j(E) \neq 0$. Then $Aut(E) \leq C_4$, so by lemma 5.2.3 all elements of order 3 and 6 are contained in E. But there are 16 such elements, so $E \cap SL(2,3)$ has more than 16 elements. Since $|SL(2,3)| = 24$, this shows that $SL(2,3) \leq E$, contradicting the non-Abelianity of $SL(2,3)$. Therefore we may assume that $j(E) = 0$, so $Aut(E) \cong C_6$.

We use Dickson's lemma A.3.2 to show that $SL(2,3)$ is *not* contained in $Isom(E)$. By the result of Dickson, $SL(2,3)$ is generated by the matrices $X := \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ and $Y := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. These matrices have order 3, and their products XY and YX are *distinct* elements of order 4. Since $4 \nmid |Aut(E)| = 6$, by lemma 5.2.3, XY and YX are both contained in the Abelian group E. But a calculation shows that $(XY)(YX) = \left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right) \neq \left(\begin{smallmatrix} 0 & 1 \\ 2 & 0 \end{smallmatrix}\right) = (YX)(XY)$. This contradicts the existence of the two generators given by Dickson.

Hereby we have achieved the goal of this section:

Proposition 5.2.4
Let E be an arbitrary elliptic curve over an algebraically closed field of characteristic zero. The group $Isom(E)$ contains an isomorphic copy of $SL(2,q)$ if, and only if, $q = 2$ ■

5.3 Preliminaries

Before we actually construct explicit $SL(2,q)$-covers of $\mathbb{P}^1$, we spend a section on summarizing the necessary results from algebraic geometry. We refer to [Si] for details.

First of all, recall the *Hurwitz genus formula*: Suppose that $f : C_1 \to C_2$ is a nonconstant separable morphism [1] of smooth curves over K, which is nowhere wildly ramified [2]. Denote the genera of C_1 and C_2 by g_1 and g_2. Then

$$2g_1 - 2 = deg(f)(2g_2 - 2) + \Sigma_{P \in C_1}(e_f(P) - 1).$$

An immediate consequence is that if $f : C_1 \to C_2$ is a nonconstant separable morphism of smooth curves, $g_1 \geq g_2$. Indeed, if we denote the sum of the $e_f(P) - 1$ on the right by c, the inequality $g_1 \geq g_2$ is equivalent with $deg(f)(2g_2 - 2) + c \geq 2g_2 - 2$, where $c \geq 0$ and $deg(f) \geq 1$. In particular, the quotient of a curve of genus zero (equivalently, a curve which is isomorphic to $\mathbb{P}^1$ - such a curve is called a *rational* curve) has again genus zero;

[1] i.e. the corresponding extension of function fields is separable.
[2] This is of course always satisfied in case $char(K) = 0$.

and the quotient of an elliptic curve (a curve of genus one) is of genus zero, or of genus one. In fact, it can be shown that the quotient of an elliptic curve is rational if and only if the quotient map is ramified.

Some other elementary properties of the ramification index are the following.

Lemma 5.3.1
Let $f : C_1 \to C_2$ be a Galois covering.

a) $\sum_{P \in f^{-1}(Q)} e_f(P) = deg(f)$, *for all* $Q \in C_2$.

b) $e_f(P) = e_f(P')$ *whenever* $f(P) = f(P')$.

c) *If $g : C_2 \to C_3$ is another nonconstant map of smooth curves, then* $e_{g \circ f}(P) = e_g(f(P))e_f(P)$, *for all* $P \in C_1$.

PROOF: a) Proposition II.2.6 (a) [Si].
b) Corollary III.7.2 (a) [St]. (Stichtenoth assumes that the ground field is perfect. In our case K is algebraically closed, thus perfect.)
c) Proposition II.2.6 (c) [Si] ■

If a finite subgroup $G \subset Aut(C)$ is given, the ramification points of the quotient map $\pi : C \twoheadrightarrow C/G$ are exactly the fixed points of G (that is, the points on C that are fixed by at least one non-identity element in G), as the second lemma shows:

Lemma 5.3.2
Let C be a smooth curve, and let G be a finite subgroup of its isomorphism group. Denote by $\pi : C \to C/G$ the quotient of C by G. For all $P \in C$, we have

$$e_\pi(P) = \#\{g \in G \mid g(P) = P\}.$$

PROOF: This is Exercise 3.13 [Si] ■

The group of elements in G fixing the point $P \in C$ is called the *inertia group* at P. It is always a cyclic subgroup of G. In this terminology, the fixed points of π are the points having a non-trivial inertia group.

5.4 Construction of some Rational and Elliptic Galois Coverings

Throughout this section, the ground field k is assumed to be algebraically closed and of characteristic 0, for example $k = \mathbb{C}$. We have now gathered enough information needed to construct some of the most elementary $SL(2,q)$-coverings of $\mathbb{P}^1(k)$: By propositions 5.1.3 and 5.2.4, rational and elliptic $SL(2,q)$ covers exist only if $q = 2, 4$ resp. $q = 2$; theorem 6

shows that a Galois G-cover is just a quotient by the group G; proposition 3.2.3 tells us how certain quotients by the composition factors of a group G fit together to form the quotient by G itself; and finally, in the previous section it was shown how the ramification of a quotient map by group G can be described in terms of fixed points of G.

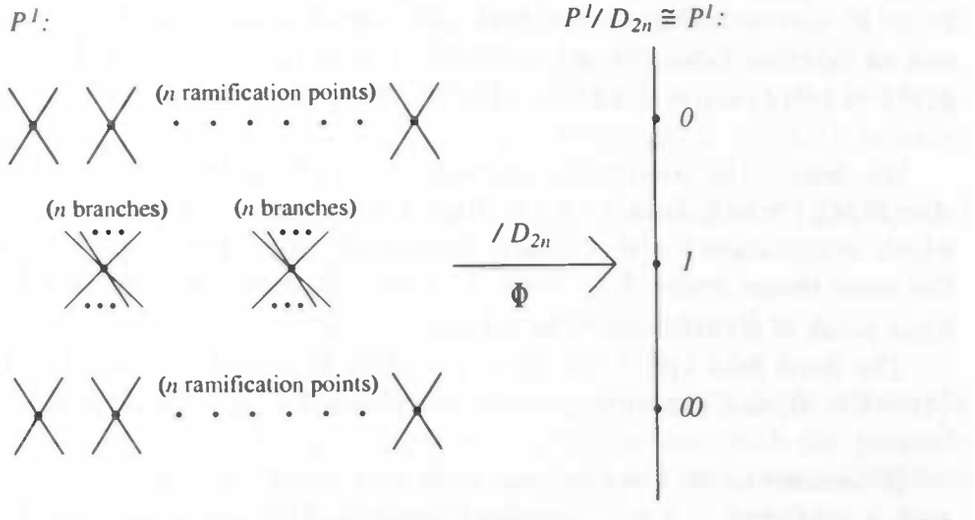
5.4.1 Rational $SL(2,2)$-Covers

The group $SL(2,2)$ is isomorphic to the dihedral group with 6 elements, $D_6 = D_{2\times 3}$. We will explain how, for general $n \geq 2$, one can construct the quotient of $\mathbb{P}^1$ by a subgroup $D_{2\times n} \cong G \subset Aut(\mathbb{P}^1) = PGL(2)$, which is ramified only above the points $0, 1$ and ∞.

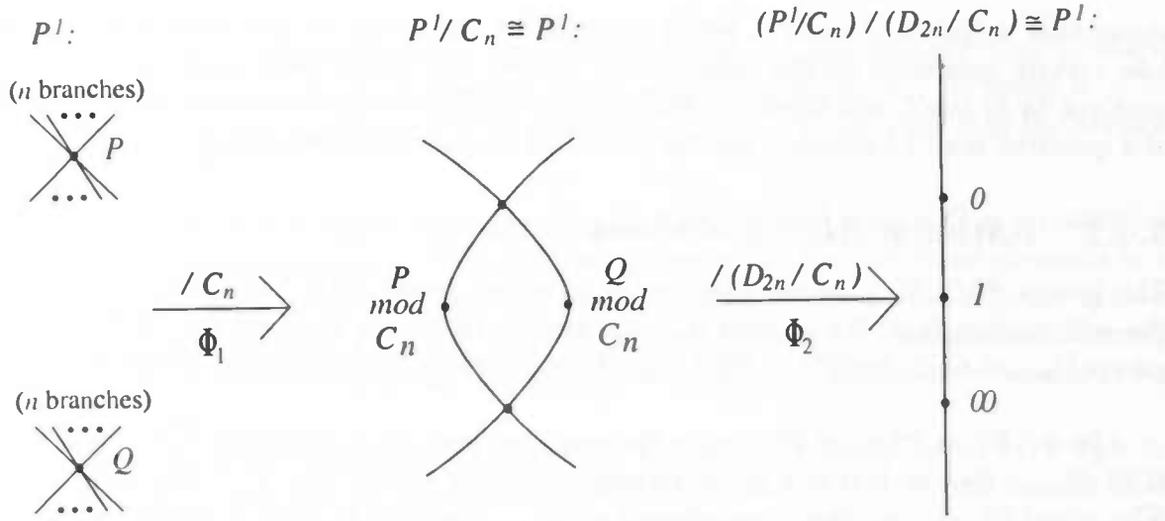
Let $\Phi : \mathbb{P}^1 \to \mathbb{P}^1/G \cong \mathbb{P}^1$ denote the quotient map by a subgroup $G \subset Aut(\mathbb{P}^1)$ with $G \cong D_{2\times n}$. By the Hurwitz genus formula we know that $2 \cdot 0 - 2 = |D_{2\times n}|(2 \cdot 0 - 2) + \sum_{P\in\mathbb{P}^1}(e_\Phi(P) - 1)$, in other words $4n - 2 = \sum_{P\in\mathbb{P}^1}(e_\Phi(P) - 1)$. One possibility (in fact the only possibility, in the case $n = 3$) is that Φ has two fibers of each n ramification points of index 2, and one fiber containing two ramification points of index n (see the picture below). Since $D_{2\times n} = C_n \rtimes C_2$, the quotient by $D_{2\times n}$ is of the form

$$\mathbb{P}^1 \xrightarrow{\Phi_1} \mathbb{P}^1/C_n \xrightarrow{\Phi_2} (\mathbb{P}^1/C_n)/(D_{2\times n}/C_n).$$

The ramification of index n finds place at Φ_1, and the $2n$ ramification points of index 2 are a result of two ramification points of index 2 of the map Φ_2. Since $PGL(2)$ is 3-transitive, we can compose the quotient map $\mathbb{P}^1 \to \mathbb{P}^1/D_{2\times n}$ with an automorphism of $\mathbb{P}^1/D_{2\times n} \cong \mathbb{P}^1$, so that ramification finds place only above $0, 1$ and $\infty \in \mathbb{P}^1/D_{2\times n}$. We can even assume that 0 and ∞ are branch points of index 2, and that 1 is a branch point of index n. These preparations can be visualized by the following pictures. The first picture shows what the ramification is of the map $\Phi : \mathbb{P}^1 \to \mathbb{P}^1/D_6$:



and the second picture shows how Φ can be seen as the composition of two quotients by cyclic groups :



We write $G =< g, h >$ where g is a generator of C_n and $ord(h) = 2$. The quotient by C_n has two ramification points, so g must have two fixed points in $\mathbb{P}^1$. We may assume that these are 0 and ∞ (after a conjugation of the group G in $PGL(2,\overline{k})$; i.e. w.r.t. an appropriate coordinate function). Since g is of the form $z \mapsto \frac{az+b}{cz+d}$, it follows that g must look like

$$g : z \mapsto \zeta_n z,$$

where ζ_n is a primitive n-th root of unity.

The quotient of $\mathbb{P}^1$ by $< g >=< z \mapsto \zeta_n z > \cong C_n$ can be represented, in the category of function fields, by the Galois extension $k(z)/k(z)^{<g>}$. The field of invariants of $k(z)$ under $< g >$ is known, namely $k(z)^{<g>} = k(z^n)$. Furthermore, the morphism from $\mathbb{P}^1$ to $\mathbb{P}^1$ corresponding to the field extension $k(z)/k(z^n)$ is $\phi : z \mapsto z^n$ (since the injection of function fields defined by $k(z^n) \hookrightarrow k(z) : z^n \mapsto z^n$ indeed equals the comorphism $f(z^n) \mapsto (\phi^*(f))(z) = f \circ \phi(z) = f(z^n)$). So we have found $\Phi_1 : \mathbb{P}^1 \to \mathbb{P}^1 : z \mapsto z^n$.

We denote the coordinate function z^n on $\mathbb{P}^1/C_n$ from now on by t. Pick an $\overline{h}(t) \in Aut(\mathbb{P}^1/C_n)$ which fixes 1 (so we have chosen 1 to be a ramification point of Φ_2), and which interchanges 0 and ∞ (since these points aren't ramification points, but should have the same image under Φ_2). Since $\overline{h} : t \mapsto \frac{at+b}{ct+d}$, it follows that now $\overline{h}(t) = \frac{1}{t}$; the second fixed point of $\overline{h}$ turns out to be -1.

The fixed field $k(t)^{<\overline{h}>}$ is $k(t + \frac{1}{t})$ (which is indeed of index 2 in $k(t)$, since $t^2 - (t + \frac{1}{t})t - 1 = 0$), and the corresponding morphism $\Phi_2 : \mathbb{P}^1 \to \mathbb{P}^1$ is just $t \mapsto t + \frac{1}{t}$.

It remains to lift the automorphism $\overline{h}$ of $Aut(\mathbb{P}^1/C_n)$ to an automorphism h of $\mathbb{P}^1$, in such a way that $< g, h >$ is indeed dihedral. Obviously, the map $h : z \mapsto \frac{1}{z}$ induces $\overline{h}$ w.r.t. the quotient $\Phi_1 : \mathbb{P}^1 \to \mathbb{P}^1/C_n$. The group generated by g and h has at least $2n$ elements, and h and g are easily shown to satisfy the relations for the dihedral group $D_{2\times n}$.

So $< g, h > \cong D_{2\times n}$.

To get the ramification above the right points, we finally have to compose with an automorphism of $\mathbb{P}^1/D_{2\times n}$. The map $\Phi_2 \circ \Phi_1 : z \mapsto z^n + \frac{1}{z^n}$ is ramified above ∞ (at 0 and ∞) and above the points 2 and -2 (at the points $\sqrt[n]{1}$ resp. $\sqrt[n]{-1}$). We can compose $\Phi_2 \circ \Phi_1$ with the automorphism $\alpha : w \mapsto \frac{w+2}{w-2}$ to obtain our definitive quotient map $\Phi := \alpha \circ \Phi_2 \circ \Phi_1$:

$$\mathbb{P}^1 \xrightarrow{/D_{2\times n}} \mathbb{P}^1 : z \mapsto 1 + \frac{4z^n}{z^{2n} - 2z^n + 1},$$

a map which is ramified above 0, 1 and ∞, at the points $\sqrt[n]{-1}$, $\{0, \infty\}$ and $\sqrt[n]{1}$, respectively.

5.4.2 Rational $SL(2,4)$-Covers

The group $SL(2,4)$ has 60 elements and is simple, so obviously the quotient of $\mathbb{P}^1$ by $SL(2,2)$ cannot be constructed as the composition of several small quotients like we did in the case $SL(2,2)$. But there are other ways in which one can describe the quotient $\mathbb{P}^1/SL(2,4)$.

First of all, it follows from Hurwitz' genus formula that if the quotient is ramified above only three points (say above $0, 1$ and ∞), then the branch type of this map must be either $(2,2,30)$ or $(2,3,5)$.

The group $SL(2,4)$ does not contain an element of order 30, so coverings of type $(2,2,30)$ do not exist. It is, however, not difficult to show that a $(2,3,5)$ covering does exist. In section 5.1 (item 4)) it is shown that $SL(2,4)$ is isomorphic to the simple group $PSL(2,5)$; and in section 4.5 one can find that $(5,4,3)$ is a branch type of $SL(2,5)$, say $< x, y >= SL(2,5)$ with $|x| = 4$, $|y| = 3$ and $|xy| = 5$. From section 4.2 we know that up to conjugation, $x = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$ for a generator λ of $\mathbb{F}_5^*$. Now, look at the image of x, y and xy under π in the sequence $Z(SL(2,5)) \hookrightarrow SL(2,5) \xrightarrow{\pi} PSL(2,5)$. Since $x^2 = \lambda^2 Id$, we have $|\pi(x)| = 2$; and since y and xy are not a multiple of Id and have prime order, it follows that $|\pi(y)| = 3$ and $|\pi(xy)| = 5$. Hence $< \pi(x), \pi(y) >= PSL(2,5) \cong SL(2,4)$, in other words, $(2,3,5)$ is a branch type of $SL(2,4)$.

We conclude that over $\mathbb{C}$, there exist a rational $SL(2,4)$-coverings of $\mathbb{P}^1$ unbranched outside $\{0, 1, \infty\}$, and each such covering has branch type $(2,3,5)$.

We will now show how one can describe the quotient of $\mathbb{P}^1$ by $SL(2,4) \cong A_5$.

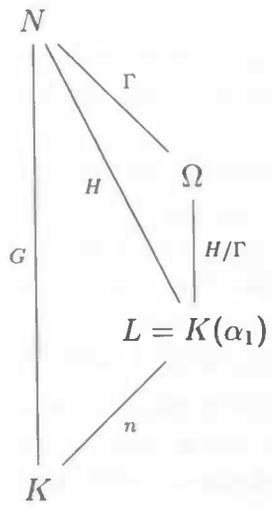
(1) We consider the analogue of the problem in the category of function fields: Given the rational function field $\mathbb{C}(t)$, find a Galois extension N of genus zero with the property $Gal(N/\mathbb{C}(t)) = A_5$. If we write $N = \mathbb{C}(z)$, and if we can express t as a rational function $t(z) \in \mathbb{C}(z)$, then the injection $t \mapsto t(z)$ induces a morphism $\mathbb{P}^1 \to \mathbb{P}^1 : z \mapsto t(z)$.

Now, we won't write down an explicit formula for this morphism, but we will describe the field N as the normal closure of some smaller field. The following lemma helps us out.

Lemma 5.4.1
Let N/K be a finite Galois extension with Galois group G, and suppose that G maps isomorphically onto a transitive subgroup of the symmetric group S_n, for some $n \geq 2$. Then there is an intermediate field $K \subset L \subset N$ with $[L : K] = n$ and such that the normal closure of L/K is N.

PROOF: (The Galois theory used here can be found in [Ga].) View G as a transitive permutation group on n elements. Then, the stabilizer in G of one of these elements is a subgroup of index n. So there exists a subgroup of G of index n, say $[G : H] = n$. Galois theory tells us that the field $L := N^H$ has the properties that N/L is Galois with group H, and L/K is a separable extension of degree n. Thus there is a primitive element α for L/K, i.e. $L = K(\alpha)$.

Let f be the minimal polynomial for α over K. We know that $deg(f) = [K(\alpha) : K] = n$, that f splits in N, and that all the roots $\alpha_1 := \alpha, \alpha_2, \ldots, \alpha_n$ of f in N are distinct. Let $\Omega := \Omega_K^f = K(\alpha_1, \ldots, \alpha_n)$ be the splitting field inside N for f over K. This is the normal closure of L/K, so we are done if we can show that $N = \Omega$. Notice that the extensions N/Ω and Ω/L are both Galois. We denote $\Gamma := Gal(N/\Omega)$, thus $Gal(\Omega/L) \cong H/\Gamma$.



Since f is irreducible, its Galois group (i.e. $Gal(\Omega/K)$) acts transitively on the set of roots $\{\alpha_1, \ldots, \alpha_n\}$. Also, since N/Ω is separable, each automorphism of Ω can be extended to an automorphism of N. Thus we find that $Gal(N/K)_{|\Omega} = Gal(\Omega/K)$ (where $Gal(N/K)_{|\Omega}$ denotes the group $\{g_{|\Omega} \mid g \in Gal(N/K)\}$). Therefore also $G = Gal(N/K)$ acts transitively on the set of roots of f. Now, $Gal(\Omega/K)$ and G are equal, since they define the same permutation group on $\alpha_1, \ldots, \alpha_n$. So $\Omega = N$ ■

Thus we know that there exists a Galois extension $N/\mathbb{C}(t)$ with group A_5 which is ramified above $0, 1, \infty$ of type $(2, 3, 5)$, and we know that it factors as $\mathbb{C}(t) \hookrightarrow L \hookrightarrow N$ for a field L of degree 5 over $\mathbb{C}(t)$. Let us denote the corresponding coverings of curves by $C_N \overset{\Phi_1}{\twoheadrightarrow} C_L \overset{\Phi_2}{\twoheadrightarrow} \mathbb{P}^1(\mathbb{C})$. Since A_5 has no normal subgroup of index 5, the morphism

$\Phi_2 : C_L \twoheadrightarrow \mathbb{P}^1$ is not Galois. We will determine the ramification of the maps Φ_1 and Φ_2:

Since Φ_1 is Galois and $deg(\Phi_1) = 12$, the map Φ_1 cannot have ramification of index 5. Therefore Φ_1 has only ramification of index $2, 3$. Let Φ_1 be ramified above m points $\in C_L$ of index 2 and above n points $\in C_L$ of index 3. Then the Hurwitz formula applied to Φ_1 yields $-2 = 12(-2) + m \cdot \frac{12}{2}(2-1) + n \cdot \frac{12}{3}(3-1)$, or simply $3m + 4n = 11$. The only solution of this is $(m, n) = (1, 2)$.

The map Φ_2 must be totally ramified (i.e. ramified of index $= deg(\Phi_2) = 5$) at a unique point above ∞. Now let k and l denote the number of ramification points $\in C_L$ of index 2 resp. 3, now w.r.t. the map Φ_2. An application of the Hurwitz formula to Φ_2 yields $-2 = 5(-2)+k(2-1)+l(3-1)+(5-1)$, i.e. $k+2l = 4$. The solutions (k, l) are $(4, 0), (2, 1)$ and $(0, 2)$. However, $(k, l) = (4, 0)$ cannot happen since ramification of index 2 finds place only above one point, namely 0; The existence of four ramification points in $\Phi_2^{-1}(0)$ and one in $\Phi^{-1}(0)$ would imply $deg(\Phi_2) \geq 9$, contradicting $deg(\Phi_2) = 5$. For the same reason, $(k, l) = (0, 2)$ is not a valid solution. It follows that $(k, l) = (2, 1)$.

In fact, we could have known in advance that neither k nor l equals 0, because of the following general principle:

Lemma 5.4.2
Let $\Phi_1 : C_N \to C_L$ and $\Phi_2 : C_L \to C_K$ be coverings corresponding to extensions of function fields $K \subset L \subset N$ of characteristic zero, in which N is the normal closure of L/K. Let $\Phi := \Phi_2 \circ \Phi_1$. Then, if Φ_2 is unramified above the point $P \in C_K$, the map Φ is also unramified above P.

PROOF: This is the analogue of a result for number fields (see chapter 4 [Mar]): If L/K is an extension of number fields, and P is a prime in K which is unramified in L, then P is also unramified in the normal closure of L/K. In fact, this statement holds for the normal closure of field extensions in general ■

A method to write down the morphism $\Phi_2 : C_L \to \mathbb{P}^1$ is the following: By choosing an appropriate coordinate u on $C_L \cong \mathbb{P}^1$ and t on $\mathbb{P}^1$, we may assume that (i) the branch points on $\mathbb{P}^1$ of index $2, 3, 5$ are $0, 1$ and ∞ resp.; and (ii) ∞ and $0 \in L \cong \mathbb{P}^1$ are ramification points of index 5 and 3, resp. The morphism $\Phi_2 : C_L \to \mathbb{P}^1 : u \mapsto t(u) = \phi(u)/\psi(u)$ (with $\phi, \psi \in \mathbb{C}[u]$) then satisfies $\Phi_2^{-1}(\infty) = \{\infty\}$, in other words $\Phi_2 = \phi$ is a polynomial in u, of degree 5.

Now, saying that $u_0 \in C_L \setminus \{\infty\}$ is a ramification point of index n of Φ_2 is equivalent with saying that u_0 is an n-fold zero of the polynomial $\Phi_2(u) - \Phi_2(u_0)$. Thus the above ramification data for Φ_2, under conditions (i) and (ii), show us that $\Phi_2 = \phi$ must satisfy

$$\begin{aligned} \phi(u) &= (u-d)^2(u-e)^2(u-f); \\ \phi(u) - 1 &= (u-0)^3(u-b)(u-c). \end{aligned}$$

Mathematica could solve this system, and gave as solution the polynomial $\phi(u) = u^5 + a_4u^4 + \ldots + a_0$, where $a_2 = a_1 = 0$, $a_0 = 1$ and

$$a_4 = 10\frac{(19+5\sqrt{-5})^{1/5}}{12(432)^{1/5}}(-1-\sqrt{-5}),$$
$$a_3 = 10\frac{(19+5\sqrt{-5})^{2/5}}{27(24)^{1/5}}(-2+\sqrt{-5}).$$

Thus the injection $\mathbb{C}(t) \hookrightarrow \mathbb{C}(u) : t \mapsto \phi(u)$, with ϕ as above, describes our covering $C_L \to \mathbb{P}^1$, and the function field of the Galois A_5-covering of $\mathbb{P}^1$ is the normal closure of $\mathbb{C}(u)$.

(2) In the article [BD] there is given a formula for the quotient of $\mathbb{P}^1$ by A_5, namely (from projective to affine coordinates):

$$(X:Y) \mapsto \frac{Q_i(X,Y)^{e_i}}{Q_j(X,Y)^{e_j}},$$

where Q_i and Q_j denote any two of the following three homogeneous polynomials:

$$\begin{aligned} Q_1(X,Y) &= XY(X^{10}+11X^5Y^5-Y^{10}); \\ Q_2(X,Y) &= -(X^{20}+Y^{20})+228(X^{15}Y^5-X^5Y^{15})-494X^{10}Y^{10}; \\ Q_3(X,Y) &= X^{30}+Y^{30}+522(X^{25}Y^5-X^5Y^{25})-10005(X^{20}Y^{10}-X^{10}Y^{20}), \end{aligned}$$

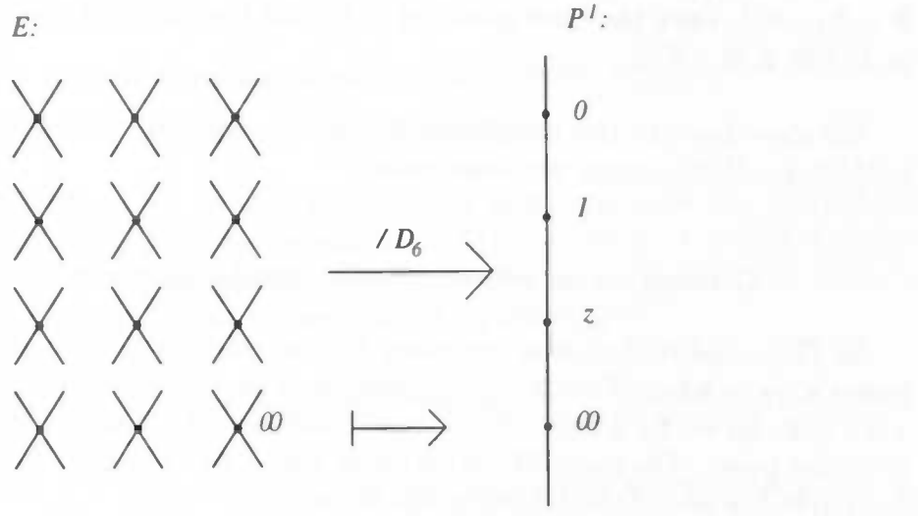
and $e_1 = 5$, $e_2 = 3$ and $e_3 = 2$. This formula for the quotient of $\mathbb{P}^1(\mathbb{C})$ by A_5 is in fact a classical result; it was written down by H.A. Schwarz more than a century ago.

5.4.3 Elliptic $SL(2,2)$-Covers

If $\Phi : E \to E/G \cong \mathbb{P}^1$ is the quotient of an elliptic curve E by a subgroup $D_6 \cong G \subset Isom(E)$, the Hurwitz genus formula tells us that $2\cdot 1-2 = |D_6|(2\cdot 0-2)+\sum_{P\in E}(e_\Phi(P)-1)$, in other words, $\sum_{P\in E}(e_\Phi(P)-1) = 12$. The ramification index of Φ at a ramified point is either 2 or 3. Moreover, lemma 5.3.1 shows that a branch point $Q \in \mathbb{P}^1$ of index e gives a contribution $(6/e)\cdot(e-1)$ to the above sum ($|D_6|/e$ ramification points of index e above Q, each of which gives a contribution of $e-1$). Thus for $e=2$ we obtain 3, and for $e=3$ we obtain 4. It follows that Φ cannot have ramification of index both 2 and 3. So we have either 12 ramification points of index 2 (three ramified points per fiber), or 6 ramification points of index 3 (two per fiber).

A D_6-covering with ramification of index 3 does not exist, since the existence of 3 branch points of index 3 is (cf. theorem 4) equivalent with $(3,3,3)$ being an admissible triple of D_6. Indeed, $(3,3,3)$ is not an admissible triple of D_6, because D_6 has only two elements of order 3, so $\{|x|,|y|,|xy|\} = \{3,3,3\}$ is possible only if $x = y$, in which case $< x,y >=< x > \neq D_6$.

We conclude that each elliptic D_6-covering of $\mathbb{P}^1$ has 12 ramification points of index 2, three above each of the four branch points on $\mathbb{P}^1$. Since $Aut(\mathbb{P}^1) = PGL(2)$ is 3-transitive, composition of the quotient map with an appropriate isomorphism of $\mathbb{P}^1$ allows us to assume that $0, 1$ and ∞ are among the branch points. On the other hand, if $P \in E$ is a ramification point above $\infty \in \mathbb{P}^1$ of the quotient $E \xrightarrow{\Phi} E/G = \mathbb{P}^1$ (where $G \cong D_6$), then the composition $E \xrightarrow{\tau_P} E \xrightarrow{\Phi} \mathbb{P}^1$ has Galois group $\tau_P^{-1} G \tau_P$ and is ramified at ∞. We conclude that up to conjugation of the Galois group in $Isom(E)$, each quotient of an elliptic curve E by a group D_6 is of the following form:



Although there are no elliptic $SL(2,q)$-covers with 3 branch points, we will - as an illustration - show in detail how to construct the elliptic D_6-cover of $\mathbb{P}^1$ having *four* branch points of index 2. This construction makes use of the equivalence of the categories of curves resp. function fields, mentioned in lemma 3.2.2.

Claim: Under the above circumstances, the Galois group $G \cong D_6$ of $\Phi : E \twoheadrightarrow \mathbb{P}^1$ is given by $G =< \tau_P, [-1] >$, for some $P \in E[3]$.

Proof: By lemma 5.3.2, the hypothesis $e_\Phi(\infty) = 2$ is equivalent with $|\{g \in G | g(\infty) = \infty\}| = |G \cap Aut(E)| = 2$. Therefore $[-1] \in G$. The remaining four non-trivial elements in G do not fix ∞, so we can pick $\beta \in G$ and put $P := \beta(\infty) \neq \infty$. There exists $\sigma \in Aut(E)$ with $\tau_{-P} \circ \beta = \sigma$, that is $\beta = \tau_P \circ \sigma$. The order of β is now given by lemma 5.2.3: If $|\sigma| = 6$, then $\beta = 6$ as well, but $G \cong D_6$ does not contain such an element; also, if $|\sigma| = 3$, then $\tau_P \circ (\sigma \circ [-1]) = \beta \circ [-1] \in G$ has order $|\sigma \circ [-1]| = 6$, which is again an absurdity. Therefore $\sigma \in \{id_E, [-1]\}$, and for both choices of σ the group $< \tau_P, [-1] >$ is easily seen to be contained in G, and it is isomorphic to D_6 exactly when $P \in E[3]$ ■ (claim)

There is a normal subgroup $< \tau_P > \lhd G$ to which we may apply proposition 3.2.3: The quotient $\Phi : E \to E/G$ is isomorphic to the composition $E \xrightarrow{\Phi_1} E/ < \tau_P > \xrightarrow{\Phi_2}$

$(E/ < \tau_P >) / (G/ < \tau_P >)$. The map Φ_1 is unramified, by lemma 5.3.2, since translation has no fixed points. Therefore $E/ < \tau_P >$ is again an elliptic curve, which we denote by $\tilde{E}$. We can choose the identity ∞ of the group $\tilde{E}$ in such a way, that $\Phi_1(\infty) = \infty$ (by an appropriate coordinate transformation). We denote the inversion on E and $\tilde{E}$ with a subscript, thus $[-1]_E$ and $[-1]_{\tilde{E}}$, respectively. Now, in the proof of proposition 3.2.3 it is shown that the automorphism $\overline{[-1]_E} := [-1]_E \mod < \tau_P >$ of $\tilde{E}$ has order 2 and fixes $\infty \in \tilde{E}$. The only element of order 2 in $Aut(\tilde{E})$ is $[-1]_{\tilde{E}}$, so we conclude that $\overline{[-1]_E} = [-1]_{\tilde{E}}$, in other words the map $\Phi_2 : \tilde{E} \to \tilde{E}/(G/ < \tau_P >)$ is just division of $\tilde{E}$ by the map $[-1]_{\tilde{E}}$.

The map Φ_2 indeed has four ramification points (resulting in 12 ramification points of $\Phi = \Phi_2 \circ \Phi_1$), since the fixed points of $[-1]_{\tilde{E}}$ are the points of order 1 or 2, i.e. the points in $\tilde{E}[2] \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.

We show how the two morphisms Φ_1 and Φ_2, describing division by τ_P and division by $[-1]$ on an elliptic curve, are constructed.

Dividing out an elliptic curve by translation over a 3-torsion point:

In [To], explicit formulas are given for the quotient map of an elliptic curve E by a group $< \tau_T >$ when $|T| = 3$. [3] A translation of the x-coordinate allows us to assume that $x(T) = 0$. So we fix a curve $E : y^2 = x^3 + ax^2 + cx + d$ which contains $T := (0, \sqrt{d})$ as a 3-torsion point. The point $(0, \sqrt{d})$ is easily shown to be in $E[3]$ if and only if $c^2 = 4ad$. So our curve has one of the following two forms:

$c = 0$: Now $E : y^2 = x^3 + d$, and $T := (0, \sqrt{d}) \in E[3]$.

$c \neq 0$: If one puts $b := -c/(2a)$, the curve E is given by $y^2 = x^3 + a(x-b)^2$, and $(0, \sqrt{d}) \in E[3]$, with $d = ab^2$.

We compute the quotient of $E : y^2 = x^3 + d$ by the group $< \tau_T >$ (the case $c = 0$; now E has j-invariant 0). We have $T = (0, \sqrt{d})$ and $-T = (0, -\sqrt{d})$. The group-law-algorithm for E shows that the maps $\tau_{\pm T}$ are given by $(x, y) \mapsto$

$$(\phi_\pm(x,y), \psi_\pm(x,y)) := \left(\frac{y^2 \mp 2\sqrt{d}y + d - x^3}{x^2}, -\frac{y^3 \mp 3\sqrt{d}y^2 + 3dy \mp d\sqrt{d}}{x^3} + y \mp 2\sqrt{d} \right).$$

First we note that, since $\tau_{\pm T}^3 = id_E$, we have $(\phi_\pm, \psi_\pm)^3(x,y) = (x,y)$. The maps $\tau_T = (\phi_+, \psi_+)$ and $\tau_{-T} = (\phi_-, \psi_-)$ are isomorphisms of E, so there are induced isomorphisms $\alpha : (x,y) \mapsto (\phi_+(x,y), \psi_+(x,y))$ and $\alpha^2 : (x,y) \mapsto (\phi_-(x,y), \psi_-(x,y))$ of the function field

[3] In fact, it is easily shown that each unramified quotient of degree 3 must be division by translation over a 3-torsion point, since lemma 5.2.3 shows that an element $g \in Isom(E)$ has order 3 exactly when either $g = \tau_P$ for some $P \in E[3]$, or $g = \tau_P \circ \phi$ for some $P \in E$ and $\phi \in Aut(E)$ with $|\phi| = 3$; an element $\tau_P \circ \phi$ with $\phi \neq id$ has however always a fixed point, since $\phi(\tau_P(Q)) = Q \Leftrightarrow \tau_{\phi(P)}(\phi(Q)) = Q \Leftrightarrow \phi(P) = (id - \phi)(Q)$, and $id - \phi$ is surjective for each $\phi \in Aut(E) \setminus \{id_E\}$.

$k(E) = k(x, y)$. The quotient of E by $< \tau_T >$ is the curve corresponding to the function field $k(E)^{<\alpha>}$. So our task is to find this field of invariants, and to find the corresponding curve.

The functions $\xi(x, y) := x + \phi_+(x, y) + \phi_-(x, y) = x + 4d/x^2$ and $\eta(x, y) := y + \psi_+(x, y) + \psi_-(x, y) = y(1 - 8d/x^3)$ are clearly invariant under the isomorphism α of the function field $k(x, y) = k(E)$. So the field $k(\xi, \eta)$ is contained in $k(x, y)^{<\tau_T>}$. To show that equality holds, it suffices to verify $|k(x, y) : k(\xi, \eta)| = 3$, since $| < \tau_T > | = 3$. An investigation of some other field extensions provides us with the necessary information:

- $|k(x, y) : k(x)| = 2$. Indeed, the minimal polynomial of y over $k(x)$ is $Y^2 - (x^3 + d) \in k(x)[Y]$.

- $|k(x) : k(\xi)| = 3$. Since $x^2\xi = x^3 + 4d$, we know that x satisfies the polynomial $F(X) := X^3 - \xi X^2 + 4d \in k(\xi)[X]$. Suppose that $F(X) = (X^2 + aX + b)(X + c)$, for certain $a, b, c \in k(\xi)$. Comparison of the coefficients reveals $a + c = -\xi$, $b + ac = 0$ and $bc = 4d$. Elimination of b and c from the last equation gives

$$a\xi^2 + 2a^2\xi + (a^3 - 4d) = 0. \tag{5.1}$$

  But we know that $a \in k(\xi)$, say $a = p(\xi)/q(\xi)$ for certain polynomials p and q. So multiplication of both sides of equation (5.1) by $q(\xi)^3$ results in an algebraic dependence relation for ξ over k, which is absurd. Hence $F(X)$ is the minimal polynomial of x over $k(\xi)$, and $|k(x) : k(\xi)| = 3$.

- $|k(\xi, \eta) : k(\xi)| = 2$. On the one hand we have

$$\eta^2 = y^2(1 - 8d/x^3)^2 = x^3 - 15d + \frac{48d^2}{x^3} + \frac{64d^3}{x^6},$$

  and on the other hand

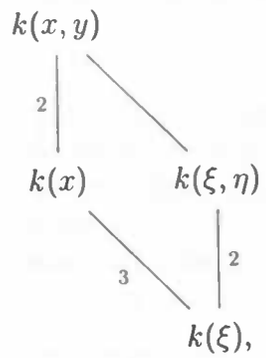
$$\xi^3 = (x + 4d/x^2)^3 = x^3 + 12d + \frac{48d^2}{x^3} + \frac{64d^3}{x^6}.$$

  Subtraction of these two equations gives

$$\eta^2 = \xi^3 - 27d. \tag{5.2}$$

  Thus $|k(\xi, \eta) : k(\xi)| = 2$.

We obtain the following picture of field extensions:



from which we see $|k(x,y) : k(\xi,\eta)| = 3$. Since $k(\xi,\eta) \subset k(x,y)^{<\alpha>}$ and $| < \alpha > | = 3$, this proves that $k(\xi,\eta) = k(x,y)^{<\alpha>}$.

The absolutely irreducible curve $\tilde{E}$ given by equation (5.2) has function field $k(\xi,\eta)$, since if we write $k(\tilde{E}) = k(\tilde{\xi},\tilde{\eta})$, the map $\tilde{\xi} \mapsto \xi(x,y)$ and $\tilde{\eta} \mapsto \eta(x,y)$ is an isomorphism from $k(\tilde{E})$ onto $k(\xi(x,y),\eta(x,y))$. Thus $\tilde{E}$ is the quotient of E by $< \tau_T >$.

The morphism $E \to \tilde{E}$ describing our quotient map, say

$$P = (x(P), y(P)) \mapsto (\alpha,\beta)(P) = (\alpha(x(P), y(P)), \beta(x(P), y(P))),$$

should be that map, which induces the comorphism $k(\tilde{E}) \hookrightarrow k(E)$ given by the injection $(\xi,\eta) \mapsto (\xi(x,y),\eta(x,y))$, and it is clear that the map $(\alpha(P) := \xi(x(P),y(P)), \beta(P) := \eta(x(P),y(P)))$ has this property. So we conclude that if E is given by $E : y^2 = x^3 + d$, and $T = (0,\sqrt{d}) \in E[3]$, then $\tilde{E} := E/ < \tau_T >: \eta^2 = \xi^3 - 27d$, and the morphism $E \to \tilde{E}$ is given by $(x,y) \mapsto (\xi(x,y),\eta(x,y))$.

In the case $E : y^2 = x^3 + a(x-b)^2$ (i.e. $c \neq 0$), it can be shown by the same method that $E/ < \tau_T >: \eta^2 = \xi^3 - 27a(\xi - 4a - 27b)^2$, and the morphism $E \to E/ < \tau_T >$ is given by $(x,y) \mapsto (\xi(x,y),\eta(x,y))$, where now

$$\xi(x,y) = 9(2y^2 + 2ab^2 - x^3 - \frac{2}{3}ax^2)x^{-2} \text{ and } \eta(x,y) = 27y(-4abx + 8ab^2 - x^3)x^{-3}.$$

Dividing out an elliptic curve by $[-1]$:

Because of the nice form of $\tilde{E} = E/ < \tau_T >$ in both the cases $c = 0$ and $c \neq 0$, the inverse of a point $(\xi,\eta) \in \tilde{E}$ is given by $-(\xi,\eta) = (\xi,-\eta)$. Since the fixed field of $k(\xi,\eta)$ under this automorphism is exactly $k(x)$, it follows immediately that the map $\tilde{E} \xrightarrow{/[-1]} \mathbb{P}^1$ is given by $(\xi,\eta) \mapsto \xi$. This map is indeed 2 to 1, except at ∞ and points P with $\eta(P) = 0$.

Appendix A

Classification of the Subgroups of $SL(2,q)$, and Dickson's Lemma

The groups $SL(2,q)$ play a central role in this thesis. We will repeatedly need information about its subgroups. The complete list of subgroups of $SL(2,q)$ is known; it was first written down by L.E. Dickson [Di]. In this appendix we present a proof of this classification theorem, and we prove another result of Dickson, known as *Dickson's lemma*. The material of this appendix is taken from Section 3.6 [Su]. We start with making some conventions and recalling some elementary definitions and facts in group and field theory.

A.1 Preliminaries on Groups and Fields

Convention A.1.1
Let G be a finite group and $S \subset G$ a subset. For x and g in G, the conjugate $x^{-1}gx$ is denoted by g^x. The *normalizer* of S in G, the *centralizer* of S in G and the *center* of G are denoted by

$$\begin{aligned} N_G(S) &:= \{g \in G \mid S^g = S\}; \\ C_G(S) &:= \{g \in G \mid x^g = x, \forall\, x \in S\}; \\ Z(G) &:= C_G(G) = \{z \in G \mid zx = xz, \forall\, x \in G\}, \end{aligned}$$

respectively. The conjugacy class in G containing x is written $\mathfrak{Cl}(x)$. The set of maximal Abelian subgroups of G will be denoted by $\mathcal{M}_G$. The order of an element $x \in G$ is denoted by both $ord(x)$ and $|x|$ ■

Definition A.1.2
If all elements of G have finite and bounded order, the *exponent* $exp(G)$ of G is the least common multiple of the orders of all of its elements. G is called an *elementary Abelian p-group* (p prime) if $exp(G) = p$. In this case, G is a direct product of cyclic groups of order p. A group of order a power of p is called a *p-group*. If H is a subgroup of a group

G then K is called a *complement* of H in G if $HK = G$ and $H \cap K = \{1\}$. Suppose that the group G acts on a set Σ. The *stabilizer* of a subset $T \subset \Sigma$ in G is defined to be

$$Stab_G(T) := \{g \in G \mid gt = t \; \forall t \in T\}.$$

The action of G on Σ is *transitive* if for all $x, y \in \Sigma$ there exists $g \in G$ with $gx = y$; it is *k-transitive* if the induced action of G on $\Sigma^{[k]} := \{$ordered k-tuples of distinct elements of $\Sigma\}$ is transitive. Conjugate elements of G have the same number of fixed points ■

We will now list some results which will be used throughout this appendix, and occasionally in other chapters as well. Proofs can be found in [Su] and [Ro].

Lemma A.1.3

a) *(Normalizers, centralizers) Let G be a group, $S \subset G$ a subset, $x \in G$, and $H \leq G$ a subgroup. Then we have $N_G(S^x) = N_G(S)^x$, $C_G(S^x) = C_G(S)^x$, $N_H(S \cap H) = N_G(S) \cap H$ and $C_H(S) = C_G(S) \cap H$.*

b) *(p-groups) All p-groups have a nontrivial center. An application of Sylow's theorem shows that if $P \leq G$ is a p-subgroup which is a Sylow p-subgroup of $N_G(P)$, then P is a Sylow p-subgroup of G. In particular, each p-subgroup P of G satisfying $P = N_G(P)$ is a Sylow p-subgroup of G.*

c) *(Modular Law) If G is a group with subgroups H, K, L satisfying $K \leq L$, then*

$$(HK) \cap L = (H \cap L)K.$$

d) *If a subgroup H of a group G is contained in $Z(G)$, then for each $x \in G$, $< H, x >$ is Abelian.*

e) *If H, K and G are groups with $H, K \leq G$, and $x \in G$, then HxK is the disjoint union of $|K : K \cap H^x|$ right cosets of H.*

f) *Let G be a finite group, $H \leq G$ and $n = |G : N_G(H)|$. Then H has exactly n conjugate subgroups in G, for*

$$H^{g_1} = H^{g_2} \Leftrightarrow H^{g_1 g_2^{-1}} = H \Leftrightarrow g_1 g_2^{-1} \in N_G(H) \Leftrightarrow g_1 N_G(H) = g_2 N_G(H).$$

g) *(Schur-Zassenhaus) If N is a normal subgroup of the finite group G, and $|N|$ and $|G : N|$ are relatively prime, then N has a complement in G, and any two such complements are conjugate in G* ■

Lemma A.1.4

Let p be a prime number, let $\mathbb{F}_p$ be a prime field of characteristic p, and fix an algebraic closure $\bar{\mathbb{F}}$ of $\mathbb{F}_p$. Suppose that $\mathbb{F}$ is a finite or infinite field of characteristic p, and let $\mathbb{F}^+$ and $\mathbb{F}^*$ denote the underlying additive resp. multiplicative groups.

a) *Every finite subgroup of* $\mathbb{F}^+$ *is an elementary Abelian p-group.*

b) *Every finite subgroup* G *of* $\mathbb{F}^*$ *is cyclic of order relatively prime to* p.

c) *Let* n *be a positive integer which is relatively prime to* p, *and denote by* $\alpha_1, \ldots \alpha_n$ *the* n *distinct primitive* n*th roots of unity in* $\bar{\mathbb{F}}$. *For any* $1 \leq k < n$ *we have*

$$\alpha_1^k + \ldots + \alpha_n^k = 0.$$

PROOF: (a) This is clear since $\mathbb{F}^+$ is a vector space over $\mathbb{F}_p$.

(b) We assume known that the multiplicative group of a finite field is cyclic, of order prime to p of course. To prove part (b), put $e := exp(G)$. Then $g^e = 1$ for all $g \in G$, so G is contained in the set of roots of $X^e - 1$. In fact G equals the set of roots of $X^e - 1$ since $e \big| |G|$. Since the splitting field of $X^e - 1$ over $\mathbb{F}_p$ is finite, G must be a subgroup of some $\mathbb{F}_{p^m}^*$. Hence G is cyclic of order prime to p.

(c) Since $(n,p) = 1$ there are indeed n distinct n-th roots of unity. By (b) these roots form a cyclic group $< \alpha >$. For $1 \leq k < n$ we have $\alpha^k - 1 \neq 0$ but $(\lambda^k - 1)(1 + \lambda + \lambda^2 + \ldots + \lambda^{(n-1)}) = \lambda^{nk} - 1 = 0$, therefore the second factor must equal 0 ■

A.2 The subgroups of $SL(2,q)$

In this section we aim to proving the following theorem:

Theorem 7
(Classification of the subgroups of $SL(2,p^n)$**)** *Let* p *be a prime number, and* $n > 1$. *Suppose* G *is a subgroup of* $SL(2,p^n)$, *and define* $q := max\{p^m \mid m \geq 1,\ p^m \mid \#G\}$. *Then* G *is isomorphic to one of the groups in the following table:* [1]

Case I: $p \nmid \lvert G \rvert$.				
	$G \cong$	$\lvert G \rvert$	(p,q)	(s,t)
(i)	*cyclic*	*lemma 4.1.1*	$(\geq 2, 1)$	$(1,0)$
(ii)	$< x, y \mid x^n = y^2, x^y = x^{-1} >$	$4n$	$(\geq 3, 1)$	$\begin{cases} (1,1) & \text{if } n \text{ odd} \\ (0,3) & \text{if } n \text{ even} \end{cases}$
(iii)	$SL(2,3)$	24	$(\geq 5, 1)$	$(1,1)$
(iv)	$\hat{\Sigma}_4$	48	$(\geq 5, 1)$	$(0,3)$
(v)	$SL(2,5)$	60	$(\geq 7, 1)$	$(0,3)$

[1] The group $\hat{\Sigma}_4$ in (iv) is a so-called representation group of the symmetric group Σ_4, see [Su]. Furthermore, in (vi), the group Q is elementary Abelian, by proposition A.2.5.

Case II: $p \mid \lvert G \rvert$. *Let* $Q \leq G$ *be a Sylow* p*-subgroup, such that* $\lvert Q \rvert = q$.				
	$G \cong$	$\lvert G \rvert$	(p,q)	(s,t)
(vi)	$Q \lhd G$ *and* G/Q *cyclic*	$q\alpha$ *(some* α*)*	$(\geq 2, \geq p)$	$(0,0)$ or $(1,0)$
(vii)	D_{2n}	$2n$, n *odd*	$(2,2)$	$(0,1)$
(viii)	$SL(2,5)$	60	$(3,3)$	$(0,2)$
(ix)	$SL(2,q)$	$q^3 - q$	$(\geq 2, \geq 4)$; $(3,3)$	$(0,2)$ or $(0,1)$
(x)	$< SL(2,q), d_\lambda >$ *where* $< \lambda^2 >= \mathbb{F}_q^*$ *but* $\lambda \notin \mathbb{F}_q$	$2(q^3 - q)$	$(\geq 2, \geq 3)$	$(0,2)$

The numbers s and t are to be defined shortly. They are used in the proof of this theorem. Except for some minor changes and additional comments (like the proof of the inequality $qg_1 < g$ following equation (A.5), and in the proofs of proposition A.2.5 (d), the case $(s,t) = (0,2)$ (P.66 - P.69), and Dickson's lemma A.3.2), the proofs of this classification theorem and Dickson's lemma that we present in the remainder of this appendix, can be found in [Su].

Convention A.2.1
We fix an algebraically closed field F of characteristic p throughout, and assume that all the finite fields $\mathbb{F}_{p^n}$ in question are contained in F. In particular, the subgroups G in the theorem are finite subgroups of $SL(2,F)$.

Let K denote an arbitrary field of characteristic p. It is easy to see that the center of $SL(2,K)$ is $\{\pm 1\}$. So it is independent of K; it depends only on p, in the sense that it is trivial if and only if $p = 2$. From now on, denote $\{\pm 1\}$ by $\mathcal{Z}$ ■

To begin, let us reduce the problem of finding the subgroups of $SL(2,p^n)$ to the case in which G contains the center $\mathcal{Z}$ of $SL(2,p^n)$. That is, assuming that the theorem holds for subgroups containing $\mathcal{Z}$, we now want to show that the theorem remains valid for subgroups which do not contain $\mathcal{Z}$. If G is such a group, it follows that $p \neq 2$, and that the size of G is odd, since (by lemma 4.1.1(a)) -1 is the only element of order 2 in $SL(2,p^n)$.

By assumption, the group $G' := G\mathcal{Z}$ is a group occurring in the above list. Since $|G'| = 2|G|$ with $|G|$ odd, we can at once say that G' cannot be of the types (ii), (iii), (iv), (v), (vii) and (viii). If G' were of type (ix), then $|G'| = q(q-1)(q+1)$ would be divisible by 8, since $q \geq 3$. Therefore we would have $4 \big| |G|$, a contradiction. Similarly, G' cannot be of type (x), since then $16 \big| |G'|$. Conclude that G' must be of type (i) or (vi). If G' is cyclic of order prime to p, then any subgroup of G' (in particular G) must be cyclic of order prime to p too, so G is of type (i) as well. Finally, if $Q \lhd G'$, then $Q \lhd G$ and $|G/Q| = (1/2)|G'/Q|$ is prime to p, so G is of type (vi).

We can conclude that indeed, it suffices to show that the theorem holds for subgroups G containing $\mathcal{Z}$. Since for $G \subset SL(2,p^n)$ also $G \subset SL(2,F)$, we will study the groups G as subgroups of $SL(2,F)$.

From now on, we may assume that G is a finite subgroup of $SL(2,F)$, which contains the center $\mathcal{Z}$ of $SL(2,F)$.

Convention A.2.2
For elements in $SL(2,F)$, we introduce the following abbreviations:

$$d_\lambda := \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \qquad t_\alpha := \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}$$

$$\hat{d}_\lambda := \begin{pmatrix} 0 & \lambda \\ -\lambda^{-1} & 0 \end{pmatrix} \qquad \mathrm{w} := \hat{d}_1$$

$$D := \{d_\omega : \omega \in F^*\} \qquad \hat{D} := \{\hat{d}_\omega : \omega \in F^*\}$$

$$T := \{t_\lambda : \lambda \in F\} \qquad H := DT \ \blacksquare$$

The elements of $\hat{D}$ have order 2 if $p = 2$, and order 4 otherwise. The following proposition summarizes some identities in $SL(2,F)$, which we will use frequently.

Proposition A.2.3

(a) *(i)* $d_\lambda d_\mu = d_{\lambda\mu}$, $d_\lambda \hat{d}_\mu = \hat{d}_{\lambda\mu}$, $\hat{d}_\lambda d_\mu = \hat{d}_{\lambda\mu^{-1}}$, $\hat{d}_\lambda \hat{d}_\mu = d_{-\lambda\mu^{-1}}$

(ii) $t_\alpha t_\beta = t_{\alpha+\beta}$, $d_\lambda^{-1} t_\alpha d_\lambda = t_{\lambda^2\alpha}$

(iii) $d_\lambda^{-1} = d_{\lambda^{-1}} = \mathrm{w}^{-1} d_\lambda \mathrm{w}$, $\hat{d}_\lambda^{-1} = \hat{d}_{-\lambda}$

(b)

$T \cong F^+$ (elementary Abelian p-group) ;
$T \lhd H$;
$D \cong F^*$;
$H = \left\{ \left(\begin{smallmatrix} \lambda & 0 \\ \alpha & \lambda^{-1} \end{smallmatrix}\right) \mid \lambda \in F^*, \alpha \in F \right\}$;
$H/T \cong F^*$;
$< D, \mathrm{w} > = D \cup \hat{D}$

(c) *(i)* *For fixed $\alpha \in F^*$: $\{x \in SL(2,F) \mid t_\alpha^x = t_\beta$ for some $\beta\} = H$ and $C_{SL(2,F)}(t_\alpha) = C_{SL(2,F)}(-t_\alpha) = T \times \mathcal{Z} \leq H$.*

(ii) *For fixed $\lambda \in F^* \setminus \{\pm 1\}$ we have $\{x \in SL(2,F) \mid d_\lambda^x = d_\mu$ for some $\mu\} = < D, \mathrm{w} >$ and $C_{SL(2,F)}(d_\lambda) = D$.*

(iii) *For $D_1 \leq D$ and $|D_1| \geq 3$ we have $N_{SL(2,F)}(D_1) = < D, \mathrm{w} >$.*

(iv) *$C_{SL(2,F)}(x)$ is Abelian $\Leftrightarrow x \in SL(2,F) \setminus \mathcal{Z}$.*

Proof: III.6.2-4 [Su] ■

In the proof of the next proposition and later on, we will need to know about the action of linear groups on the projective line. Let E be any field and let V_E be the two-dimensional

vector space E^2 over E. The element in $\mathbb{P}^1_E$ corresponding with $(u,v) \in V_E$ will be denoted by $(u:v)$. The rule $(g,(u:v)) \mapsto g\binom{u}{v}$ makes the two-dimensional linear groups over E act on $\mathbb{P}^1_E$, and the following lemma summarizes some basic facts about this action.

Lemma A.2.4
Let the subfield $E \leq F$ be finite or equal to F.

(a) $SL(2,E)$ (and therefore $PSL(2,E)$) acts 3-transitive on $\mathbb{P}^1_E$ if $char(E) = 2$ or $E = F$, and 2-transitive otherwise. Moreover, if $p > 2$ and L is a quadratic extension of E then any triple $t_1 \in (\mathbb{P}^1_E)^3$ can be mapped to any other $t_2 \in (\mathbb{P}^1_E)^3$ by an element in $SL(2,L)$.

(b) consider the action of $SL(2,E)$ on $\mathbb{P}^1_E$.

(i) $x \in SL(2,E) \setminus \mathcal{Z} \Rightarrow x$ has at most two fixed points.

(ii) $\omega \in E^* \setminus \{\pm 1\} \Rightarrow d_\omega$ fixes $(1:0)$ and $(0:1)$;
$\lambda \in E^* \Rightarrow t_\lambda$ fixes only the point $P := (0:1) \in \mathbb{P}^1_E$ and $Stab_{SL(2,E)}(P) = H$.

(iii) $1 \neq Q \leq T^y \cap SL(2,E)$ for some $y \in SL(2,F) \Rightarrow$ the elements of Q have a common fixed point in $\mathbb{P}^1_E$ and for $x \in Q \setminus \mathcal{Z}$ this is the only fixed point.

Proof: For part (a) see Chapter 3, (6.6) [Su]. Suzuki states and proves part (b)(i) and (b)(ii) for the case $E = F$, see (6.7) [Su], although he uses it later on also for finite subfields $E \leq F$. But the proof doesn't change at all:

(b)(i) Suppose x has two fixed points $P \neq Q \in \mathbb{P}^1_E$ and let u and v be vectors in V_E corresponding to P and Q respectively. Then u and v form a basis of eigenvectors for V_E and since $det(x) = 1$, the corresponding eigenvalues must be ω and ω^{-1} for some $\omega \in F^*$. Let $R \neq P, Q$ be a third point in $\mathbb{P}^1_E$ fixed by x, and let w be a vector corresponding to R, with eigenvalue μ, say. Then $w = \alpha u + \beta v$ $(\alpha, \beta \in F^*)$, so $\mu(\alpha u + \beta v) = \mu w = xw = x(\alpha u + \beta v) = \omega\alpha u + \omega^{-1}\beta v \Rightarrow \mu = \omega = \omega^{-1} \Rightarrow \omega = \pm 1$ so x is conjugate to ± 1, that is $x \in \mathcal{Z}$.

(b)(ii) Follows from matrix computation.

(b)(iii) Write $y = \binom{a\ b}{c\ d}$ and choose $\lambda \in F^*$ with $t^y_\lambda \in Q$. Then $\begin{pmatrix} 1-ab\lambda & -b^2\lambda \\ a^2\lambda & 1+ab\lambda \end{pmatrix} = t^y_\lambda \in SL(2,E) \Rightarrow ab\lambda, b^2\lambda \in E \Rightarrow ab^{-1} \in E$. The only fixed point of t_λ is $(0:1)$ so $t^y_\lambda R = R \Rightarrow t_\lambda yR = yR \Rightarrow yR = (0:1) \Rightarrow R = y^{-1}(0:1) = (-b:a) \in \mathbb{P}^1_E$. This shows that non-identity elements in Q have a common fixed point in $\mathbb{P}^1_E$ ■

The numbers s and t occurring in the last column of the tables in theorem 7 will be defined shortly; they stand for the number of maximal Abelian subgroups of G satisfying a particular property. The necessary information about the set of maximal Abelian subgroups of G is listed below. Recall that G is an arbitrary finite subgroup of $SL(2,F)$ containing $\mathcal{Z} = \mathcal{Z}(SL(2,F))$.

Proposition A.2.5
Let $\mathcal{M}$ be the set of all maximal Abelian subgroups of G. The following hold:

(a) $\mathcal{M} = \{C_G(x) \mid x \in G \setminus \mathcal{Z}\}$.

(b) Any two distinct members of $\mathcal{M}$ have intersection $\mathcal{Z}$.

(c) Each member of $\mathcal{M}$ is of one of the following forms:

(i) Cyclic of order n with $(n,p) = 1$;

(ii) $Q \times \mathcal{Z}$ where $Q \leq G$ is an elementary Abelian Sylow p-subgroup of G,

and each subgroup of the form (ii) is maximal Abelian.

(d) If $A = C_G(x) \in \mathcal{M}$ is of type (i), then $|N_G(A) : A| \leq 2$. If, in particular, $|N_G(A) : A| = 2$, then for each $y \in N_G(A) \setminus A$, we have $y^{-1}xy = x^{-1}$, and $ord(y) = 2$ or 4 according as $p = 2$ or $p \neq 2$.

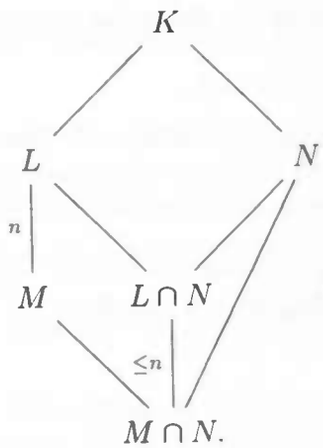
(e) For each Sylow p-subgroup $1 \neq Q \leq G$ there exists a cyclic group $K \leq G$ such that $N_G(Q) = QK$ and $Q \cap K = \{1\}$. If $|K| > |Z|$ then $K \in \mathcal{M}$.

Proof: (a) and (b): For $x \in \mathcal{Z}$ we of course have $C_{SL(2,F)}(x) = SL(2,F)$. If $x \notin \mathcal{Z}$, then $C_G(x) = C_{SL(2,F)}(x) \cap G$ is Abelian by proposition A.2.3(c)(iv). Choose an $M \in \mathcal{M}$ with $C_G(x) \leq M$. Then $M \leq C_{SL(2,F)}(x)$ (because M is Abelian), and hence $M \leq C_{SL(2,F)}(x) \cap G = C_G(x)$, so $C_G(x) = M \in \mathcal{M}$. Now choose $A \in \mathcal{M}$. For each noncentral element $x \in G \setminus \mathcal{Z}$, the group $< \mathcal{Z}, x >$ is Abelian, so A must contain a noncentral element, say x. Suppose B is another member of $\mathcal{M}$ and let $y \in A \cap B$, then $A \cup B \subseteq C_G(y) \Rightarrow C_G(y)$ is not Abelian, so $y \in \mathcal{Z}$, proving part (b). Therefore $A \cap C_G(x) = A$ or $\mathcal{Z}$, and $x \notin \mathcal{Z}$, so $A \leq C_G(x)$, i.e. $A = C_G(x)$.

(c) Let $C_G(x) \in \mathcal{M}$ and suppose $x = d_\lambda^y$ for some $\lambda \in F^* \setminus \{\pm 1\}$ and $y \in SL(2,F)$. Then $C_G(x) = C_{SL(2,F)}(x) \cap G = C_{SL(2,F)}(d_\lambda)^y \cap G = D^y \cap G$ by proposition A.2.3(c)(ii). By proposition A.2.3(b) $D \cong F^*$ so $C_G(x)$ is isomorphic to a finite subgroup of F^*, which by lemma A.1.4(b) must be a cyclic subgroup of size relatively prime to p. Now assume $x = \pm t_\alpha^y$ for some $\alpha \in F^*$ and $y \in SL(2,F)$. By proposition A.2.3(c)(i) we have $C_G(x) = C_{SL(2,F)}(\pm t_\alpha^y) \cap G = (T \times \mathcal{Z})^y \cap G = (T^y \times \mathcal{Z}) \cap G$. Since $\mathcal{Z} \leq G$, this equals $(T^y \cap G) \times \mathcal{Z}$. Also, since $T \cong F^+$, lemma A.1.4(a) shows that $C_G(x) = Q^y \times \mathcal{Z}$, where Q is a finite elementary Abelian p-subgroup of T. Suppose that Q^y is contained in the Sylow p-subgroup S of G. Since $Q \neq \{1\}$ we can choose a nontrivial element z in the center of S, and find $C_G(x) = Q^y \times \mathcal{Z} \subseteq S \times \mathcal{Z} \subseteq C_G(z) \in \mathcal{M}$. Hence $C_G(x) = C_G(z)$ and Q^y must equal S. So $C_G(x)$ is the direct product of an elementary Abelian Sylow p-subgroup of G with $\mathcal{Z}$. If R is another Sylow p-subgroup of G, then $R = S^y$ for some $y \in G$ so $R \times \mathcal{Z} = (S \times \mathcal{Z})^y$ is maximal Abelian as well.

(d) Suzuki spends few words on this. Let us do it better: We have seen in the proof of (c), that $x = d_\lambda^y$ for some $\lambda \in F^* \setminus \{\pm 1\}$ and $y \in SL(2,q)$, and that $A = C_G(x) = D^y \cap G$. By lemma A.1.3 (a), we find $N_G(A) = N_G(D^y \cap G) = N_{SL(2,F)}(D^y) \cap G = (N_{SL(2,F)})^y \cap G$.

Next, proposition A.2.3 (b) and (c)(iii) show that $N_G(A) =< D, w >^y \cap G = (D \cup \hat{D})^y \cap G$. We conclude that up to $SL(2,F)$-conjugation, $A = D \cap G$, $N_G(A) = (D \cup \hat{D}) \cap G$, and $N_G(A) \setminus A = \hat{D} \cap G$.
To prove $|N_G(A) : A| \leq 2$, take a look at the following diagram of group inclusions (where K, L, M and N denote arbitrary groups, and $n := |L : M|$):



Indeed, the map $l(M \cap N) \mapsto lM$ is a well-defined and injective map from the set of left cosets of $M \cap N$ in $L \cap N$ to the set of left cosets of M in L. Now, just substitute $SL(2,F)$, $< D, w >$, D and G for K, L, M and N, respectively, and notice that $| < D, w >: D| = 2$. Finally, the identities in proposition A.2.3(a) can be used to show that any element in $N_G(A) \setminus A$ conjugates x into its inverse. Since these elements are conjugate to an element in $\hat{D}$ they have order 2 or 4.

(e) Assume $A = C_G(\pm t_\alpha) = (T \times Z) \cap G = Q \times Z$ for some Sylow p-subgroup $Q = T \cap G$ of G. We have

$$\begin{aligned} N_G(Q) &= N_G(T \cap G) \\ &= \bigcap_{t_\alpha \in G} (\{x \in SL(2,F) \mid t_\alpha^x = t_\beta \text{ for some } \beta\} \cap G) \\ &= H \cap G \end{aligned}$$

the last equality following from proposition A.2.3 (c)(i). Since $Q \leq N_G(Q) \cap T \leq G$ and $N_G(Q) \cap T$ is a p-subgroup of G (by lemma A.1.4(a)), we have $N_G(Q) \cap T = Q$. Now an isomorphism theorem shows:

$$N_G(Q)/Q = N_G(Q)/(N_G(Q) \cap T) \cong TN_G(Q)/T = (H \cap G)T/T \leq H/T \cong F^*.$$

Since $N_G(Q)/Q \leq F^*$, lemma A.1.4(b) shows that this subgroup must be cyclic of order n relatively prime to p. Write $N_G(Q)/Q =< x >$ and choose $y \in N_G(Q)$ such that $y \cdot Q = x$. If $ord(y) = n$ then $N_G(Q) = Q < y >$ and $< y > \cap N_G(Q) = \{1\}$. In the other case we have $y^n \in Q \setminus \{1\}$, but $(y^p)^n = (y^n)^p = 1$ since Q has exponent p. Since $(|Q|, n) = 1$ we find $N_G(Q) = Q < y^p >$ and $Q \cap < y^p >= \{1\}$.

Suppose $|K| > |\mathcal{Z}|$. Since K is Abelian we can choose $A \in \mathcal{M}$ containing K, and since $(|K|, p) = 1$, A must be of the form (i), that is A is conjugate to the group $< d_\lambda >$ for some $\lambda \in F^* \setminus \{\pm 1\}$. We have seen above that G acts on $\mathbb{P}^1_F$ and the previous lemma showed that d_λ, and therefore also the generator of $K \leq A$, has exactly two fixed points P_1 and $P_2 \in \mathbb{P}^1_F$. The same lemma showed that the elements of T have a common fixed point P and $Stab_{SL(2,F)}(P) = H \geq H \cap G = N_G(Q) \geq K$ so the generator of K fixes P. Hence d_λ fixes P as well and we see $A \leq Stab_{SL(2,F)}(P) \cap G = N_G(Q) = QK$. Using $Q \leq T$ and the fact that A is conjugate to a subgroup of D we have $A \cap Q = \{1\}$, so that the modular law (lemma A.1.3(c)) shows $A = A \cap QK = (Q \cap A)K = K$. Hence $K \in \mathcal{M}$ ■

We will now define s and t, and show that there are only 6 possibilities for the pair (s,t). If $p \mid |G|$, fix a Sylow p-subgroup $Q \leq G$. Since all Sylow p-subgroups of G are conjugate in G, the set $\mathcal{M}$ contains all the conjugates of $Q \times \mathcal{Z}$, and all other members (thus *all members*, if p and $|G|$ are coprime) of $\mathcal{M}$ are cyclic of order prime to p. Partition this last class of members of $\mathcal{M}$ into conjugacy classes $C_1, \ldots, C_{s+t}$ such that for a representative $A_i \in \mathcal{M}$ of C_i we have:

$$|N_G(A_i) : A_i| = \begin{cases} 1 & \text{if } 1 \leq i \leq s, \\ 2 & \text{if } s < i \leq s+t. \end{cases} \tag{A.1}$$

Any member of $\mathcal{M}$ contains $\mathcal{Z}$ so $|\mathcal{Z}|$ divides its order. $N_G(Q)$ contains $\mathcal{Z}$ as well, but Q does not, unless $p = 2$. Therefore we can introduce the following notations:

$$\begin{aligned} e &:= |\mathcal{Z}| \\ e \cdot g &:= |G| \\ e \cdot g_i &:= |A_i| \\ q &:= |Q| \\ e \cdot k &:= |N_G(Q) : Q| \end{aligned}$$

If $p \| |G|$ then $q > 1$ and, by proposition A.2.5 (e), $N_G(Q) = QK$ for some K with $|K| = e \cdot k$. Furthermore, if $k \neq 1$ then $\mathcal{Z} \underset{\neq}{<} K$, so $K \in C_i$ for some i. Hence $k = 1$ or g_i for some i. The following equation will be used repeatedly in finding the structure of G.

Lemma A.2.6
Still assuming that G is a finite subgroup of $SL(2,q)$ containing the center $\mathcal{Z} = \mathcal{Z}(SL(2,q))$, we have, in the above notations:

$$1 = \frac{1}{g} + \frac{q-1}{qk} + \sum_{i=1}^{s} \frac{g_i - 1}{g_i} + \sum_{i=s+1}^{s+t} \frac{g_i - 1}{2g_i} \tag{A.2}$$

Proof: The number of noncentral elements in G is $e(g-1)$. We can count these elements in another way: By proposition A.2.5(b) and (c) the number of noncentral elements equals

$\sum_{A\in\mathcal{M}} |A \setminus \mathcal{Z}|$. For $A_i \in C_i$ proposition A.2.5(b) shows that $A_i^g = A_i \Leftrightarrow g \in N_G(A_i)$ and $A_i \cap A_i^g = \mathcal{Z}$ otherwise. So C_i contains $|G : N_G(A_i)|$ maximal Abelian subgroups of G (representatives of distinct cosets of $N_G(A_i)$ in G defining distinct conjugates of A_i), each of them containing $|A_i \setminus \mathcal{Z}|$ noncentral elements and each two of them having no noncentral elements in common. Hence

$$\#\{g \in G \setminus \mathcal{Z} | \exists A \in C_i \text{ with } g \in A \text{ for some } i\} = \sum_{i=1}^{s} \frac{e^2 g(g_i - 1)}{e g_i} + \sum_{i=s+1}^{s+t} \frac{e^2 g(g_i - 1)}{2 e g_i}.$$

The other noncentral elements must be contained in some conjugate of $Q \times \mathcal{Z}$. There are $|G : N_G(Q\times\mathcal{Z})| = eg/eqk$ such conjugates and each of them contains $|(Q\times\mathcal{Z})\setminus\mathcal{Z}| = e(q-1)$ noncentral elements, so we obtain $eg(q-1)/qk$ new noncentral elements. Adding these to the ones contained in some C_i and dividing by eg proves the lemma ■

Since $\mathcal{Z} \underset{\neq}{\leq} A_i$ we have $g_i \geq 2$ so that $(g_i - 1)/g_i \geq 1/2$. Therefore

$$1 = \frac{1}{g} + \frac{q-1}{qk} + \sum_{i=1}^{s} \frac{g_i - 1}{g_i} + \sum_{i=s+1}^{s+t} \frac{g_i - 1}{2g_i} > \sum_{i=1}^{s} \frac{1}{2} + \frac{1}{2} \sum_{i=s+1}^{s+t} \frac{1}{2} = \frac{2s+t}{4} \tag{A.3}$$

and the only possible $s, t \geq 0$ satisfying $2s + t < 4$ are

$$(s,t) = (0,0), (1,0), (0,1), (1,1), (0,2) \text{ or } (0,3). \tag{A.4}$$

We are now able to prove theorem 7, by showing that for each possible pair (s,t), each subgroup G of $SL(2,p^n) \subset SL(2,F)$ containing $\mathcal{Z}$ with $(s(G),t(G)) = (s,t)$ is one occurring in the tables of theorem 7.

$(s,t) = (0,0)$: Since $s = t = 0$, there are no maximal Abelian subgroups of order relatively prime to p, so the only elements of order prime to p in G are the elements in $\mathcal{Z}$. It is clear that if $Q \leq G$ is a Sylow p-subgroup of G, then $G = Q \times \mathcal{Z}$. If $|Q| = 1$ this gives a group of type (i), otherwise we obtain a group of type (vi) □

$(s,t) = (1,0)$: In this case (A.2) becomes

$$\frac{1}{g} + \frac{1}{k} = \frac{1}{qk} + \frac{1}{g_1}.$$

If $p \not| |G|$ then $g_1 = g$ so G is cyclic of order prime to p, giving us a group of type (i). In the other case we have $k > 1$, since $k = 1$ would give $1/g + 1 = 1/q + 1/g_1 \Rightarrow g(q+g_1) - qg_1 = qgg_1 \Rightarrow g(q+g_1) > qgg_1$, leading to a contradiction since $q, g_1 > 1$. Therefore proposition A.2.5(e) implies that $N_G(Q) = QK$ with $K \in \mathcal{M}$ a maximal Abelian subgroup of G which has size prime to p. Since $k = g_1$, by (A.2) we have $g = qk$ so $|N_G(Q)| = |QK| = eqk = eg = |G|$, i.e. $Q \lhd G$ and $G/Q \cong K$ is cyclic of order prime to

p. This is case (vi) again □

$(s,t) = (0,1)$: Now (A.2) becomes

$$1 = \frac{1}{g} + \frac{q-1}{qk} + \frac{g_1 - 1}{2g_1}.$$

If $k > 1$ then we get $1/2 > (q-1)/qk = 1/2 + 1/2g_1 - 1/g \geq 2$ since $g \geq 2g_1$, so we must have $k = 1$. We obtain

$$\frac{1}{q} + \frac{1}{2g_1} = \frac{1}{g} + \frac{1}{2},$$

and see that $q \geq 2$. If $q \geq 4$ then we get $1/2g_1 - 1/g = 1/2 - 1/q \geq 1/4 \Rightarrow 2g \geq gg_1 + 4g_1$ contradicting the fact $g_1 \geq 2$. Therefore consider the following cases:

$(q = 2)$: Now $p = 2$, $Q :=< y >$ is cyclic and (by proposition A.2.5 (c)(i)) $A_1 :=< x >$ is cyclic of odd order g_1. Notice that $2g_1 = g = |G|$ so that we must have $N_G(A_1) = G = A_1Q$. Three relations which hold in G are $x^{g_1} = y^2 = 1$ and (by proposition A.2.5(d)) $x^y = x^{-1}$. Since the group defined by these relations (the dihedral group D_{2g_1}) and G have the same size, we have $G \cong D_{2g_1}$ and we are in case (vii).

$(q = 3)$: In this case $p = 3$, $e = 2$ and $A_1 =< x >$ where x has order $2g_1$ with $(g_1, 3) = 1$. By (A.2) find $1 = 1/g + 1 - 1/3 + 1/2 - 1/2g_1 \Rightarrow 1/6 < 1/6 + 1/g = 1/2g_1 \Rightarrow g_1 = 2$, hence $g = 12$ and $|G| = 24$. If y and $z \neq y^{\pm 1}$ are two elements in $N_G(A_1) \setminus A_1$ then, by proposition A.2.5(d), $< y >$ and $< z >$ are two cyclic groups of order 4, and since $s = 0$ and $t = 1$ these two groups must be in C_1. Since $|G : N_G(A_1)| = 3$ there are no more conjugates of A_1 so $N_G(A_1) = A_1 \cup < y > \cup < z > \lhd G$. By definition of x and y we have $N_G(A_1) =< x, y | x^2 = y^2, x^y = x^{-1} >= Q_8$, the quaternion group. In [Su] it is shown that G is now determined as an extension of Q_8 by C_3, which is isomorphic to $SL(2,3)$. Therefore we are in case (ix) □

$(s,t) = (1,1)$: This case is similar to the previous one. Now (A.2) becomes

$$\frac{1}{2g_2} - \frac{q-1}{qk} = \frac{1}{2} - \frac{1}{g_1} + \frac{1}{g},$$

where $q = 1$. For if $q > 1$ then $(q-1)/qk \geq 1/2k \Rightarrow 1/2g_2 - 1/2k \geq 1/2 - 1/g_1 + 1/g > 1/2 - 1/g_1 \geq 0 \Rightarrow g_2 > k$. Therefore $k = g_1 > g_2 > 1$, and substitution into (A.2) leads to a contradiction: $1/2g_2 - 1/g_1 + 1/qg_1 = 1/2 - 1/g_1 + 1/g < 1/2 - 1/g_1 \Rightarrow (g_1 + g_2)/2g_1g_2 = 1/2g_2 + 1/2g_1 \geq 1/2g_2 + 1/qg_1 > 1/2 \Rightarrow g_1 + g_2 > g_1g_2$. Substitution of $q = 1$ gives $1/2g_2 + 1/g_1 = 1/2 + 1/g > 1/2$ which leaves only the following two possibilities $g_1 = 2$ and $g_1 = 3$:

$(g_1 = 2)$: Now $g = 2g_2$ and $A_2 \lhd G$. Let $A_1 =< y >$ and $A_2 =< x >$. Since $2 \big| |A_1| \big| |G|$ and $q = 1$ we have $p > 2$. By lemma A.1.3 (b), the 2-subgroup A_1 of G with $N_G(A_1) = A_1$ is in fact a Sylow 2-subgroup. Hence $4 \not| |A_2|$ (otherwise the cyclic group A_2 would contain an element of order 4 contradicting proposition A.2.5(b) since all Sylow 2-subgroups are

conjugate). Again by proposition A.2.5(d), since $N_G(A_2) = G$, the two relations $x^y = x^{-1}$ and $x^{g_1} = y^2$ hold in G. The group defined by these generators and relations (a so-called generalized quaternion group, see example 1 in chapter 2 § 9, P.258 [Su]) has size $4g_1$, so $G =< x, y | x^{g_2} = y^2, x^y = x^{-1} >$. This is case (ii) with n odd.

($g_1 = 3$): In this case we must have $g_2 = 2$ and $g = 12$. Since $(g_i, p) = 1$ we have $p > 3$. Write $A_2 =< x >$ and pick $y \in N_G(A_2) \setminus A_2$, then $x^2 = y^2 = -I$ and $x^y = x^{-1}$. As in the case $(s,t) = (0,1)$ it can be shown that $N_G(A_2) \cong Q_8 \lhd G$ and therefore $G \cong SL(2,3)$. This is case (iii) □

$(s,t) = (0,2)$: Now equation (A.2) becomes

$$\frac{1}{2g_1} + \frac{1}{2g_2} = \frac{1}{g} + \frac{q-1}{qk}.$$

The assumption $q = 1$ leads to $2g_1g_2 = g(g_1 + g_2)$ contradicting $g \geq 2g_1$ and $g_1 + g_2 > g_2$ so we must have $q > 1$. If $k = 1$ then (A.2) gives the contradiction $1/2 \geq 1/2g_1 + 1/2g_2 = 1/g + (q-1)/q > 1/2$ so $k > 1$ as well. By proposition A.2.5 (e) we have, w.l.o.g., $N_G(Q) = QA_1$ with $A_1 \cap Q = \{I\}$ and $k = g_1$. In particular $eqg_1 = |N_G(Q)| \leq |G| = eg$ so $qg_1 \leq g$. Substituting g_1 for k results into

$$\frac{1}{2g_2} = \frac{1}{g} - \frac{1}{qg_1} + \frac{1}{2g_1} \leq \frac{1}{2g_1}. \tag{A.5}$$

[2] In fact we have $qg_1 < g$. One can use the Schur-Zassenhaus theorem A.1.3 (g) to prove this: If $qg_1 = g$ then $N_G(Q) = QA_1 = G$. The above equation shows $g_1 = g_2$ and since $Q \cap A_2 = \{I\}$ we have $QA_2 = G$ as well. Therefore A_1 and A_2 are two complements of the normal subgroup $Q \lhd G$ in G, which by the Schur-Zassenhaus theorem are conjugate in G. This contradicts $t = 2$, hence we have $g_1 < g_2$.

$N_G(Q)$ acts on Q by conjugation. One of the orbits is $\{I\}$. Choose $x \in Q \setminus \{I\}$. By proposition A.2.5 $C_G(x) = Q \times \mathcal{Z} \leq N_G(Q)$ so $|N_G(Q) : C_G(x)| = k = g_1$, and since $C_G(x)$ is just the stabilizer of x, the orbit-stabilizer-lemma shows that the orbit $\mathcal{O}(x)$ containing x has size $k = g_1$. Therefore

$$q = |Q| \equiv 1 \mod g_1. \tag{A.6}$$

Clearing denominators in (A.5) gives $g(qg_1 - qg_2 + 2g_2) = 2qg_1g_2$ showing that $g | 2qg_1g_2$. Setting $a := 2qg_1g_2/g$ turns the previous equation into

$$qg_1 = (q-2)g_2 + a, \tag{A.7}$$

so $g_2 = (q-1)g_2 - qg_1 + a$ which together with (A.6) shows

$$g_2 \equiv a \mod g_1. \tag{A.8}$$

[2] Suzuki doesn't prove this (see P.402 [Su]).

By definition $(g/2g_2)a = qg_1$. Since $(p, g_2) = 1$ we have $(a, q) = 2$ if $p = 2$ and $(a, q) = 1$ if $p > 2$, i.e. $a|2g_1$ or g_1 according as $p = 2$ or $p > 2$. We will distinguish the two cases $q \leq 3$ and $q \geq 4$:

($q \leq 3$): By (A.6) we must have $q = 3$ and $g_1 = 2$. (A.7) implies $2 = g_1 > (q-2)g_2/q = g_2/3$. Together with $g_1 < g_2$ and $(g_2, 3) = 1$ this leaves only two possibilities for g_2:

($g_2 = 4$): Now (A.7) and (A.5) show $a = 2$ and $g = 24$. So $g_1 = \frac{a}{2}(q-1), g_2 = \frac{a}{2}(q+1)$ and $g = \frac{a}{2}q(q^2-1)$ where $q = 3$ and $a = 2$ (so $|G| = 2 \cdot 3 \cdot 8 = 48$). We will see that in the case $q \geq 4$ the same set of equations is satisfied where $a = 1$ or 2. There it is shown that G is either of type (ix) or (x). In fact, in this particular case ($q = 3$) G will turn out to be of type (x).

($g_2 = 5$): Now $a = 1$ and $g = 2qg_1g_2 = 60$. As before $N_G(A_1) \cong Q_8$ is a Sylow 2-subgroup of G and $N_G(A_1)$ contains 3 conjugates of A_1. Since $|G : N_G(A_1)| = 15$, G contains exactly 15 subgroups of size 4 so there are 5 Sylow 2-subgroups in G. Conjugation defines a homomorphism $G \to S_5$. Since the only elements acting trivially on the set of Sylow 2-subgroups are the ones in $\mathcal{Z}$, the map $G/\mathcal{Z} \to S_5$ is an injection. Since $G/\mathcal{Z}$ has size 60 it must be isomorphic to $A_5 \lhd S_5$. In [Su] it is shown that the extension G of A_5 (in fact a representation group for A_5) must be isomorphic with $SL(2,5)$. We have found a group of type (viii) $\square$ ($q \leq 3$)

($q \geq 4$): This is the hardest part of all. We will see that here G is isomorphic to some $SL(2,q)$ or a quadratic extension of $SL(2,q)$ (cases (ix) and (x)). By (A.7) we have $g_1 > g_2(q-2)/q$. Since $q \geq 4$ this shows $2g_1 > g_2 > g_1$. We have seen $a|2g_1$. Moreover $a \neq 2g_1$ since otherwise (A.7) would give the contradiction $g_1 = g_2$, and $a \neq g_2$ since the assumption $a = g_2$ implies (by (A.7)) $q(g_2 - g_1) = g_2$, contradicting $(g_2, q) = 1$. Now (A.8) shows that $g_2 = g_1 + a$. Therefore (A.7) and the definition of a give

$$\begin{aligned} g_1 &= a(q-1)/2 \\ g_2 &= a(q+1)/2 \\ g &= aq(q^2-1)/2 \end{aligned}$$

Since $q - 1 = 2g_1/a$ and $q \equiv 1 \mod g_1$ we must have $2/a \in \mathbb{Z}$, i.e. either $a = 1$ or $a = 2$. Notice that $p = 2 \Rightarrow 2|a \Rightarrow a = 2 \Rightarrow |G| = g = q(q^2-1)$.

Claim:

$$G \text{ is of type } \begin{cases} \text{(ix)} & \text{if } |G| = eaq(q^2-1)/2 = q(q^2-1), \\ \text{(x)} & \text{if } |G| = eaq(q^2-1)/2 = 2q(q^2-1). \end{cases}$$

Remember that we also still have to prove the case $p = q = 3, a = 2$ (see the case $G_2 = 4$ above). Let E be an extension of $\mathbb{F}_p$ with the property $G \subset SL(2,E)$. Lemma A.2.4(b)(iii) shows that the elements of Q have a common fixed point $P_1 \in \mathbb{P}^1_E$. This point is fixed by $N_G(Q)$: Choose $y \in N_G(Q)$ and $x \in Q$, then $x^y \in Q$ so $x^y P_1 = P_1 \Rightarrow xyP_1 = yP_1 \Rightarrow yP_1 = P_1$. We assumed $N_G(Q) = QA_1$ so A_1 fixes P_1. By the proof of proposition A.2.5(c)(i) A_1 is of the form $< x > = < d_\lambda^y >$ with $\lambda \in \mathbb{F}^* \setminus \{\pm 1\}$ and $y = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL(2,F)$. So

lemma A.2.4(b)(ii) shows that the elements of A_1 have a second common fixed point P_2. Calculation shows that the two fixed points of A_1 are $(-b:a)$ and $(-d:c)$. W.l.o.g. $P_1 = (-b:a)$ so $ab^{-1} \in E$. Therefore $cd^{-1} = acb^{-1}d^{-1}(ab^{-1})^{-1} = -x_{21}x_{12}^{-1}(ab^{-1})^{-1} \in E$, i.e. $P_2 \in \mathbb{P}^1_E$ as well (Here Suzuki refers to his version of lemma A.2.4(b) but thereby doesn't prove that indeed $P_2 \in \mathbb{P}^1_E$!) For an element $u \in Q \setminus \{1\}$ define $P_3 := uP_2 \neq P_1, P_2$. By lemma A.2.4(a) we can choose an element $v \in SL(2,F)$ (and even in $SL(2,E)$ if $char(E) = 2$) such that $P_1, P_2, P_3 = v(0:1), v(1:0), v(1:1)$, respectively. Consider the group G^v. Clearly A_1^v fixes $(0:1)$ and $(1:0)$, Q^v fixes $(0:1)$ and $u^v(0:1) = (0:1)$. Hence (by the proof of proposition A.2.5(c)) $A_1^v \leq D$ and $Q^v \leq T$, in particular $u^v \in T$. Finally $uv(1:0) = uP_2 = P_3 = v(1:1) \Rightarrow u^v(1:0) = (1:1)$ so $u^v = t_1 = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. We can conclude that up to conjugation by v we have

$$u = t_1 \in Q = T \cap G; \qquad A_1 = D \cap G;$$
$$P_1 = (0:1); \qquad P_2 = (1:0); \qquad P_3 = (1:1)$$

Define $i := ea/2$ so that $|G| = iq(q^2-1)$ (we've seen $i = 1$ if $p = 2$, and in case $q = 3$ we have $i = 2$). Then $\exists \lambda \in F^* \setminus \{\pm 1\}$ such that $A_1 =< d_\lambda >$ and $|\lambda| = eg_1 = i(q-1)$. In particular $< \lambda^i >= \mathbb{F}_q^*$.

Define $\Lambda := \{\lambda \in E \mid t_\lambda \in Q\}$. We will show that $\Lambda = \mathbb{F}_q$ and $\mathrm{w} = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in G$: The proof of proposition A.2.5(d) shows that $N_G(A_1) \setminus A_1 = \hat{D} \cap G$ and since $|N_G(A_1) : A_1| = 2$ we can choose $x = \hat{d}_\beta \in \hat{D} \cap G$. We have $N_G(Q)^x \cap Q = \{I\}$ since $N_G(Q) = QA_1 \leq TD = H$ and conjugation by x turns an element $\left(\begin{smallmatrix} a & 0 \\ c & d \end{smallmatrix}\right) \in H$ into the upper diagonal matrix $\left(\begin{smallmatrix} d & -\beta^2 c \\ 0 & a \end{smallmatrix}\right)$. Therefore $|Q : N_G(Q)^x \cap Q| = |Q| = q$, and lemma A.1.3 (e) remarks that $N_G(Q)xQ$ is the disjoint union of q right cosets of $N_G(Q)$ in G. It is easy to show that $N_G(Q) \cap N_G(Q)xQ = \emptyset$, so $|N_G(Q) \cup N_G(Q)xQ| = |N_G(Q)|(1+q) = qeg_1(q+1) = iq(q^2-1) = |G|$, hence

$$G = N_G(Q) \cup N_G(Q)xQ \tag{A.9}$$

Now pick $t_\alpha \in Q \setminus \{I\}$, then $t_\alpha^x = transpose(t_{-\alpha\beta^2}) \notin H \geq N_G(Q)$ so by (A.9) there exist $d_\mu t_\gamma \in N_G(Q) = A_1 Q$ and $t_\delta \in Q$ such that

$$\begin{pmatrix} 1 & -\alpha\beta^2 \\ 0 & 1 \end{pmatrix} = t_\alpha^x = (d_\mu t_\gamma) x t_\delta = d_\mu t_\gamma \hat{d}_\beta t_\delta = \begin{pmatrix} \delta\beta\mu & \mu\beta \\ \gamma\delta\mu\beta - \mu^{-1}\beta & \gamma\beta\mu \end{pmatrix}$$

Comparison of the entries of the two matrices shows that $\mu = -\alpha\beta$. Since $t_{-1} = u^{-1} \in Q$ we can take $\alpha = -1$ and find $\mu = \beta$. This means that if $x = \hat{d}_\beta \in G$ then also $d_\beta \in G$. So $d_\beta^{-1}x = \mathrm{w} \in G$ as well, and we may assume that $x = \mathrm{w}$. Now for arbitrary $\alpha \in \Lambda$ we find $\mu = -\alpha$ showing that $d_{-\alpha} \in A_1 = D \cap G$ whenever $\alpha \in \Lambda$. Suppose $i = 1$, then $A_1 =< d_\lambda >$ with $< \lambda >= \mathbb{F}_q^*$ so $\Lambda \leq \mathbb{F}_q$. Since $|\Lambda| = |Q| = q$ we have $\Lambda = \mathbb{F}_q$. On the other hand, if $i = 2$ then $< d_\lambda >= A_1 \leq N_G(Q)$ so for each $t_\alpha \in Q$ and each $\eta \in < \lambda >$ we have $t_{\eta^2\alpha} = (d_\eta)^{-1} t_\alpha d_\eta \in Q$. Let η run over $< \lambda >$, then $< \eta^2 >= \mathbb{F}_q^*$, so taking $\alpha = 1$ shows that $\mathbb{F}_q \leq \Lambda$. Again $\Lambda = \mathbb{F}_q$.

Now the proof of the claim can be completed: Since $\Lambda = \mathbb{F}_q$ and $\mathrm{w} \in G$, all the transvections over $\mathbb{F}_q$ are contained in G. By lemma 4.1.1(f) G contains $SL(2,q)$. We will now distinguish between $i = 1$ and $i = 2$:

($i = 1$): Comparing the orders of G and $SL(2,q)$ shows that $G = SL(2,q)$ (remember that we have conjugated G by an appropriate element $v \in SL(2,F)$!). This is case(ix). Notice that the fact that any two subgroups of order $q-1$ (or $q+1$) are conjugate does not mean that all elements of order $q-1$ are conjugate!

($i = 2$): In this case G contains an element d_λ with $\lambda \notin \mathbb{F}_q$ but $< \lambda^2 >= \mathbb{F}_q^*$. Since $|G|/|SL(2,q)| = 2$, we have $G =< SL(2,q), d_\lambda >$, i.e. G is a group of type (x). In the particular case $q = 3$ and $g_2 = 4$ we saw that $i = 2$ so a group of type (x) with $q = 3$ really occurs. This proves the claim, and also the case $q \geq 4$ □ ($q \geq 4$)
We have proven the case $(s,t) = (0,2)$ □

$(s,t) = (0,3)$: In this case equation (A.2) becomes

$$\frac{1}{2g_1} + \frac{1}{2g_2} + \frac{1}{2g_3} = \frac{1}{g} + \frac{1}{2} + \frac{q-1}{qk}. \tag{A.10}$$

We have $q = 1$ and $k > 1$: Since $t = 3$, G contains noncentral elements so $g > 1$. Therefore $q = 1 \Rightarrow k = g > 1$, and the assumption $q > k = 1$ gives, by (A.10) and $1/2g_i \leq 1/4$, the contradiction $g \geq 4q + 3g(q-1) > 3g$ so in any case $k > 1$ (Suzuki just walks over this). Since k equals one of the g_i, equation (A.10) shows that q must equal 1.

We may assume $1 < g_1 \leq g_2 \leq g_3$. If $g_1 = g_2 = 2$ then $g = 2g_3$ and the only other possibility is $g_1 = 2, g_2 = 3$ and $g_3 \leq 5$. If $g_3 = 3$ as well then $g = 12$ and A_2 and A_3 are subgroups of size 6. These are of the form $< x > \times \mathcal{Z}$ and $< y > \times \mathcal{Z}$ resp. where x and y are elements of order 3 in G. By Sylow's theorem $< x >$ and $< y >$ are conjugate, hence A_2 and A_3 are conjugate as well, a contradiction. Therefore we have to consider only the following three cases:

(i) $g_1 = g_2 = 2$ and $g = 2g_3$. We have $G = N_G(A_3)$ so if $A_3 =< x >$ and $A_1 =< y >$ then $y \in N_G(A_3) \setminus A_3$ so by proposition A.2.5 (d) we have $x^y = x^{-1}$. Moreover $x^{g_3} = y^2 = -I$. Since x and y generate G, and the group defined by the presentation $< x, y | x^{g_3} = y^2, x^y = x^{-1} >$ has $4g_3 = |G|$ elements, G is defined by this presentation. Therefore G is of type (ii). Finally g_3 is even, since if g_3 was odd then $(2, g_3) = 1$, so A_1 and A_2 would be Sylow 2-subgroups and therefore conjugate, a contradiction.

(ii) $g_1 = 2, g_2 = 3, g_3 = 4$ and $g = 24$. Now $|G : N_G(A_2)| = 48/12 = 4$ so A_2 has 4 conjugates in G. This induces a permutation representation $\phi : G \to S_4$. The kernel of this map can be shown to be $\mathcal{Z}$, so $G/\mathcal{Z} \cong S_4$. It is a fact that the only central extension of S_4 that contains exactly one element of order 2 is the group $\hat{\Sigma}_4$ (see (2.21), P.301 [Su]). We end up with the group in row (iv).

(iii) $g_1 = 2, g_2 = 3, g_3 = 5$ and $g = 60$. As in the case $(s,t) = (0,2)$, $q = 3$ and $g_2 = 5$, it can be shown that $G \cong SL(2,5)$. But now $q = 1$ and $p \geq 7$ so this gives a group of type (v) □

This completes the proof of the classification theorem of the subgroups of $SL(2,p^n)$ ■

A.3 Dickson's Lemma

The two lemmas in this section are used in chapter 4, to prove the existence of certain triples of generators of $SL(2,q)$. We start with a lemma that gives, for certain roots of unity ζ over $\mathbb{F}_p$, the index of $\mathbb{F}_p$ in $\mathbb{F}_p(\zeta+\zeta^{-1})$ in terms of the order of p in the group $(\mathbb{Z}/ord(\zeta)\mathbb{Z})^*$.

Lemma A.3.1
Assume that $p \geq 2$ is a prime, and that r is a positive number which is relatively prime to p. Let ζ be a primitive r-th root of unity over $\mathbb{F}_p$, and put $\omega := \zeta+\zeta^{-1}$ and $N := ord(p \in (\mathbb{Z}/r\mathbb{Z})^*) = min\{m \geq 1 \mid r|p^m-1\}$. If either N is odd, or N is even and $r|p^{N/2}+1$, then

a) $\mathbb{F}_p(\zeta) = \mathbb{F}_{p^N}$;

b) $\mathbb{F}_p(\omega) = \begin{cases} \mathbb{F}_{p^{N/2}} & \text{if } N \text{ is even;} \\ \mathbb{F}_{p^N} & \text{if } N \text{ is odd.} \end{cases}$

PROOF: a) By definition, N is the minimal positive number m with the property $\zeta^{p^m} = \zeta$, in other words, $\mathbb{F}_{p^N}$ (the splitting field of $X^{p^N}-X$ over $\mathbb{F}_p$) is the smallest field containing ζ, and thus $\mathbb{F}_p(\zeta) = \mathbb{F}_{p^N}$ [3].

b) Since ω satisfies $\zeta^2-\omega\zeta+1=0$, we have only the two possibilities $|\mathbb{F}_p(\zeta):\mathbb{F}_p(\omega)| = 1$ or 2. If N is odd then of course $|\mathbb{F}_p(\omega):\mathbb{F}_p| = N$, i.e. $\mathbb{F}_p(\omega) = \mathbb{F}_p(\zeta) = \mathbb{F}_{p^N}$. Finally, if N is even then by hypothesis $r|p^{N/2}+1$, thus

$$\zeta^{p^{N/2}+1} = 1 \Rightarrow \zeta^{p^{N/2}} = \zeta^{-1} \Rightarrow \omega^{p^{N/2}-1} = \frac{\omega^{p^{N/2}}}{\omega} = \frac{\zeta^{p^{N/2}}+\zeta^{-p^{N/2}}}{\zeta+\zeta^{-1}} = \frac{\zeta^{-1}+\zeta}{\zeta+\zeta^{-1}} = 1.$$

This shows that $|\mathbb{F}_p(\omega):\mathbb{F}_p| \leq N/2$, and consequently $\mathbb{F}_p(\omega) = \mathbb{F}_{p^{N/2}}$ ■

The final result of this appendix is Dickson's lemma:

Lemma A.3.2
(Dickson) *Let $p \neq 2$ be prime and suppose λ is nonzero and algebraic over $\mathbb{F}_p$. Define $E := \mathbb{F}_p(\lambda)$ and $G :=< x, y >$ where*

$$x = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \text{ and } y = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}.$$

Then $G = SL(2,E)$ whenever $p \neq 3$, or $p = 3$ and $\lambda^2 \neq -1$. In the exceptional case $p = 3$ and $\lambda^2 = -1$ we have $G \cong SL(2,5)$.

[3] The minimal polynomial of ζ over $\mathbb{F}_p$ is in fact $p(X) := \prod_{i=0}^{N-1}(X-\zeta^{p^i})$. Namely, it vanishes at ζ, and it lies in $\mathbb{F}_p[X]$ since the Frobenius homomorphism $F : x \mapsto x^p$ applied to the coefficients a_i of $p(X)$ shows (since F permutes the zeroes cyclically) $p(X) = \prod_{i=0}^{N-1}(X-F(\zeta^{p^i})) = X^N + F(a_{N-1})X^{N-1} + \ldots + F(a_1)X + F(a_0)$, so $F(a_i) = a_i$ for all i. Therefore each a_i is in the field which is fixed pointwise by F, i.e. $a_i \in \mathbb{F}_p$.

Proof: (Taken from [Su], theorem 6.21 on P.409) [4] Since $|x| = |y| = p$ we have $p||G|$, so G is one of the groups mentioned in case II of the classification theorem 7. Since $xy \neq yx$, G cannot be of type (vi). Since $p \neq 2$ case (vii) can be excluded as well. Suppose that G is of type (x), i.e. (by the proof of theorem 7) $G^v =< d_\pi, SL(2,\mathbb{F}_q) >$ with $\pi \notin \mathbb{F}_q$ but $< \pi^2 >= \mathbb{F}_q^*$, for some $v \in SL(2,F)$. Remember (from the proof of theorem 7, the case $(s,t) = (0,2)$) that v was found as follows: Since $t_1 \in G$ we can define (by the proof of proposition A.2.5(c)(ii)) $Q = T \cap G$, a Sylow p-subgroup of G. Hence Q fixes the point $P_1 = (0:1)$. The group A_1 fixes a second point $P_2 = (1:\sigma) \in \mathbb{P}^1_{\mathbb{F}_p(\lambda)}$. Since $t_1 \in Q \setminus \{I\}$ we can take $u = t_1$ so that $P_3 = t_1 P_2 = (1:1+\sigma)$. Now v is the linear map sending $(0,1)$ to $(0,1)$ and $(1,0)$ to $(1,\sigma)$ (cf. the proof of (6.6), P.395 [Su]), i.e. $v = \left(\begin{smallmatrix} 1 & 0 \\ \sigma & 1 \end{smallmatrix}\right) \in SL(2,\mathbb{F}_q)$. Conclude that

$$SL(2,\mathbb{F}_p(\lambda)) \geq G^v =< x^v, y^v >= \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1+\sigma\lambda & \lambda \\ -\sigma^2\lambda & 1-\sigma\lambda \end{pmatrix} \right\rangle =< d_\pi, SL(2,\mathbb{F}_q) >$$

Since $(d_\pi)^{-1} \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) d_\pi = \left(\begin{smallmatrix} a & \pi^{-2}b \\ \pi^2 c & d \end{smallmatrix}\right)$, every element in $G^v =< d_\pi, SL(2,\mathbb{F}_q) >$ has a standard form $x(d_\pi)^i$ where $x \in SL(2,q)$ and $i = 0,1$. So $|G^v : SL(2,\mathbb{F}_q)| = 2$, hence $SL(2,\mathbb{F}_q) \lhd G^v$ and we find a short exact sequence

$$1 \longrightarrow SL(2,\mathbb{F}_q) \longrightarrow G^v \longrightarrow \mathbb{Z}/2\mathbb{Z},$$

showing that every element of order p in G^v is contained in the subgroup $SL(2,\mathbb{F}_q)$. But y^v is an element of order p in G^v which is not in $SL(2,\mathbb{F}_q)$, a contradiction. Conclude that G can't be of type (x) either.
G is a group of type (viii) or (ix). We will first show:

$$G \text{ is of type (viii)} \Leftrightarrow p = q = 3 \text{ and } \lambda^2 = -1.$$

($\Rightarrow$) If G is of type (viii) then $p = q = 3$ and $G/\mathcal{Z} \cong A_5$. The only elements of order 3 in A_5 are the 3-cycles, so if we define ϕ to be the composition of the projection map $G \twoheadrightarrow G/\mathcal{Z}$ with the isomorphism $G/\mathcal{Z} \cong A_5$ then $\phi(x)$ and $\phi(y)$ must be 3-cycles. Since $< \phi(x), \phi(y) >= A_5$ these 3-cycles can only have one letter in common, hence $|\phi(x)\phi(y)| = 5$ and $|xy| = 5$ or 10. This means that xy is conjugate to some $\pm d_\zeta$ where ζ is a fifth root of unity over $\mathbb{F}_3$. $tr(xy) = tr(\pm d_\zeta) \Rightarrow 2 + \lambda = \pm(\zeta \pm \zeta^{-1})$ so $\mathbb{F}_3(\lambda) = \mathbb{F}_3(\zeta + \zeta^{-1})$, and lemma A.3.1 shows (with $r = 5$ and $p = 3$) that $|\mathbb{F}_3(\zeta + \zeta^{-1}) : \mathbb{F}_3| = 2$. This means that $\mathbb{F}_3(\lambda) = \mathbb{F}_9$.
There are only two primitive third roots of unity over $\mathbb{F}_3$ so by the second case in section 4.2 there is only one conjugacy class in $SL(2,5)$ containing the elements of order 3. So x and y are conjugate. An easy calculation shows that we must have $x = y^v$ for some $v = \left(\begin{smallmatrix} a & 0 \\ c & a^{-1} \end{smallmatrix}\right) \in SL(2,9)$. Since $1 = x_{21} = (y^v)_{21} = -c^2\lambda$ we have $\lambda = -c^{-2}$ for some $c \in \mathbb{F}_9$. So $\lambda^2 = c^{-4} \in (\mathbb{F}_9^*)^4 = \{1,-1\}$. But $\lambda^2 = 1 \Rightarrow c^{-4} = 1 \Rightarrow -\lambda = c^{-2} = \pm 1 \in \mathbb{F}_3$, a contradiction. Conclude that $\lambda^2 = -1$. (Using this and

[4] In his proof, Suzuki states at once that G must be a group of either type (viii) or (ix). It is however not very clear why G can't be of type (x); this is what I prove in the first part of my proof.

$p = 3$, calculation shows that $(xy)^5 = -I$, so $|xy| = 10$. So $SL(2,5)$ can be generated by two elements of order 3 whose product has order 10).

($\Leftarrow$) This can be checked easily in GAP using the command *IsomorphismGroups*, which gives an isomorphism between two groups in terms of the generators if the two groups are isomorphic, and fails otherwise. In our case *IsomorphismGroups(Group(x, y), SL(2, 5))* returned the isomorphism defined by

$$x \mapsto \begin{pmatrix} \mu & \mu \\ \mu^2 & \mu \end{pmatrix} \text{ and } y \mapsto \begin{pmatrix} \mu & 1 \\ \mu^3 & \mu \end{pmatrix}$$

where μ is a primitive fifth root of unity.

Hereby we have also proved that G is of type (ix) if and only if $p \neq 3$ or $\lambda^2 \neq -1$, and the only thing left to do is to show that G equals the whole group $SL(2, \mathbb{F}_p(\lambda))$. The argument used above (to exclude case (x)) shows that $G^v = SL(2, \mathbb{F}_q)$ for some $v \in SL(2, \mathbb{F}_p(\lambda))$, hence $\mathbb{F}_q \leq \mathbb{F}_p(\lambda)$. Since $(y^v)_{12} = \lambda \in \mathbb{F}_q$ we have $\mathbb{F}_q = \mathbb{F}_p(\lambda)$, i.e. $G = SL(2, \mathbb{F}_p(\lambda))$ ■

Bibliography

[BD] Baldassarri, F. and Dwork, B.: *On second order linear differential equations with algebraic solutions* , American Journal of Mathematics 101, 42-76 (1979).

[Di] Dickson, L.E.: *Linear Groups, with an Exposition of the Galois Field Theory*, Dover (1958).

[De] *The Grothendieck Theory of Dessins d'Enfants*, London Mathematical Society, Lecture Notes Series 200, CUP, Edited by L. Schneps (1994).

[DG] Darmon, H. and Granville, A.: *On the equations* $z^m = F(x,y)$ *and* $Ax^p + By^q = Cz^r$, University of Georgia Mathematics Preprints Series, No. 28 Volume II (1994).

[Fo] Forster, O.: *Riemannsche Flächen*, Heidelberger Taschenbücher, Band 184, Springer-Verlag (1977).

[Fu] Fulton, W.: *Algebraic Topology, A First Course*, Graduate Texts in Mathematics 153, Springer-Verlag (1995).

[GAP] GAP: *Groups, Algorithms and Programming,* available on the internet at `http://www-gap.dcs.st-andrews.ac.uk/~gap/`.

[Ga] Garling, D.J.H.: *A Course in Galois Theory*, CUP (1986).

[Go] Gorenstein, D.: *Finite Groups*, Harper's Series in Modern Mathematics, Harper & Row (1968).

[Gr] Granville, A.: ABC *Allows Us to Count Squarefrees*, International Mathematics Research Notices No. 19 (1998), 991-1009.

[Hart] Hartshorne, R.: *Algebraic Geometry*, GTM 52, Springer-Verlag (1977).

[Harr] Harris, J.: *Algebraic Geometry, a First Course*, GTM 133, Springer-Verlag (1993).

[Ja] Jaenich, K.: *Topologie*, Springer-Lehrbuch, Springer-Verlag (1996).

[Ma] Matzat, B.H.: *Konstruktive Galoistheorie*, Lecture Notes in Mathematics 1284, Springer-Verlag (1985).

[Mar] Marcus, D. A.: *Number Fields*, Universitext, Springer-Verlag (1987).

[Pu1] van der Put, M.: *Algebraic Topology*, Lecture Notes, Rijksuniversiteit Groningen (1995).

[Pu2] van der Put, M.: *Riemann Surfaces*, Lecture Notes, Rijksuniversiteit Groningen (1995).

[Ro] Robinson, D.: *A Course in the Theory of Groups*, GTM 80, Springer-Verlag (1995).

[Se] Serre, J.-P.: *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15, 259-331 (1972).

[Sh] Shih, K.-Y.: *On the construction of Galois extensions of function fields and number fields*, Mathematische Annalen 207, 99-120 (1974).

[Si] Silverman, J.H.: *The Arithmetic of Elliptic Curves*, GTM 106, Springer-Verlag (1992).

[St] Stichtenoth, H.: *Algebraic Function Fields and Codes*, Universitext, Springer-Verlag (1993).

[Su] Suzuki, M.: *Group Theory I*, Springer-Verlag (1982).

[To] Top, J.: *Descent by 3-isogeny and 3-rank of quadratic fields*, Advances in Number Theory, Editors Ferdinand Q. Gouvea and Noriko Yui, Oxford University Press (1993).

[Vo] Voelklein, H.: *Groups as Galois Groups: an Introduction*, Cambridge Studies in Advanced Mathematics 53, CUP (1996).

[VM] Valentini, R.C. and Madan, M.L.: *A Hauptsatz of L.E. Dickson and Artin-Schreier extensions*, Journal für die reine und angewandte Mathematik, Band 318, 156-177 (1980).

[We] Weber, H.: *Lehrbuch der Algebra, Zweiter Band*, Braunschweig (1896).

[ZS] Zariski, O. and Samuel, P.: *Commutative Algebra*, Vol. I and II, GTM 28 and 29, Springer-Verlag (1975).