Difference Equations with Semisimple Galois Groups in Positive Characteristic

Von der Fakultät für Mathematik, Informatik und Naturwissenschaften der RWTH Aachen University zur Erlangung des akademischen Grades einer Doktorin der Naturwissenschaften genehmigte Dissertation

vorgelegt von

Diplom-Mathematikerin Annette Maier

aus Freiburg im Breisgau.

Berichter:
Universitätsprofessorin Dr. rer. nat. Julia Hartmann
Universitätsprofessor em. Dr. rer. nat. B. Heinrich Matzat

Tag der mündlichen Prüfung: 16. Dezember 2011

Zusammenfassung

Sei F ein Körper und σ ein Automorphismus auf F. Eine (lineare) Differenzengleichung über F ist eine Gleichung der Form $\sigma(y) = Ay$, wobei A ein Element in $\mathrm{GL}_n(F)$ und y einen Vektor mit n Unbestimmten bezeichnet. Man kann dann Lösungen in Erweiterungskörpern von F betrachten und so genannte Picard-Vessiot Ringe definieren, welche ein maximal unabhängiges System von Lösungen enthalten und gleichzeitig auf eine gewisse Weise minimal mit dieser Eigenschaft sind. Falls ein solcher Picard-Vessiot Ring zu der gegebenen Differenzengleichung existiert, kann man ihm eine lineare algebraische Gruppe, die Differenzen-Galoisgruppe, zuordnen.

Sei nun $F = \mathbb{F}_q(s,t)$ und σ der Automorphismus auf F, der $\mathbb{F}_q(t)$ punktweise fixiert und s auf s^q abbildet. Das Hauptresultat der vorliegenden Dissertation besagt, dass folgende Gruppen als Differenzen-Galoisgruppen über F vorkommen: die speziellen linearen Gruppen SL_n, die symplektischen Gruppen Sp_{2d}, die speziellen orthogonalen Gruppen SO_n (wobei hier q ungerade vorausgesetzt wird) und die Dickson Gruppe G_2. Für all diese Gruppen werden explizite Differenzengleichungen angegeben. Weiterhin wird gezeigt, dass jede halbeinfache, einfach zusammenhängende Gruppe $\mathcal{G}$, die über $\mathbb{F}_q$ definiert ist, für ein geeignetes $i \in \mathbb{N}$ als σ_i-Differenzen-Galoisgruppe über $F_i = \mathbb{F}_{q^i}(s,t)$ vorkommt, wobei $\sigma_i(s) = s^{q^i}$. Da alle betrachteten Gruppen zusammenhängend sind, können diese Ergebnisse von $\mathbb{F}_q(s,t)$ bzw $\mathbb{F}_{q^i}(s)(t)$ nach $\overline{\mathbb{F}_q(s)}(t)$ geliftet werden. Dies führt zu so genannten rigid analytisch trivialen Prä-t-Motiven mit denselben Galoisgruppen. Die Kategorie der rigid analytisch trivialen Prä-t-Motive enthält die Kategorie der t-Motive, welche in der Arithmetik von Funktionenkörpern von Interesse ist.

Um die besagten Gruppen realisieren zu können, werden verschiedene Kriterien entwickelt, die Schranken an Differenzen-Galoisgruppen geben. Zunächst wird gezeigt, dass ein Picard-Vessiot Ring zu $\sigma(y) = Ay$ existiert, falls A gewisse Konvergenzbedingungen erfüllt. Sei nun $\sigma(y) = Ay$ eine solche Differenzengleichung mit Differenzen-Galoisgruppe $\mathcal{H}$ und sei $\mathcal{G} \leq \mathrm{GL}_n$ eine gegebene lineare algebraische Gruppe. Wenn A in $\mathcal{G}(F)$ enthalten ist, so gilt $\mathcal{H} \leq \mathcal{G}$, d.h. $\mathcal{H}$ kann nach oben beschränkt werden. Um $\mathcal{H} = \mathcal{G}$ zeigen zu können, wird folgendes Kriterium bewiesen: Sei $\alpha \in \mathbb{F}_q$ derart, dass das Ersetzen von s durch α die Matrix $A \in \mathrm{GL}_n(\mathbb{F}_q(s,t))$ auf ein wohldefiniertes Element $A_\alpha \in \mathrm{GL}_n(\mathbb{F}_q(t))$ abbildet. Dann enthält $\mathcal{H}$ ein gewisses Konjugiertes von A_α. Mithilfe dieser Kriterien kann nun wie folgt vorgegangen werden, um die Gruppe $\mathcal{G}$ zu realisieren. Man konstruiere die Matrix A derart, dass die Konvergenzbedingungen erfüllt sind und sodass beliebige Konjugierte der Familie $\{A_\alpha \mid \alpha \in \mathbb{F}_q\}$ die Gruppe $\mathcal{G}$ erzeugen. Um dies entscheiden zu können, befasst sich die vorliegende Arbeit auch mit der Erzeugung von linearen algebraischen Gruppen. Zum einen werden explizite Erzeuger der klassischen Gruppen konstruiert, die auch nach gewisser Konjugation noch die Gruppe erzeugen. Zum anderen wird ein etwas allgemeineres Resultat für reduktive Gruppen, welche über $\mathbb{F}_q$ zerfallen, bewiesen.

Abstract

Let F be a field with an automorphism σ on F. A (linear) difference equation over F is an equation of the form $\sigma(y) = Ay$ with $A \in \mathrm{GL}_n(F)$ and y a vector consisting of n indeterminates. There is the notion of a Picard-Vessiot ring which is in some sense a " smallest" difference ring extension R of F such that there exists a full set of solutions with entries in R to the given difference equation. If there exists a Picard-Vessiot ring, one can assign a difference Galois group to the Picard-Vessiot ring, which turns out to be a linear algebraic group (in the scheme theoretic sense).

Let $F = \mathbb{F}_q(s,t)$ with σ defined to be the automorphism that fixes $\mathbb{F}_q(t)$ pointwise and maps s to s^q. The main result of this thesis is that the following groups occur as difference Galois groups over F: the special linear groups SL_n, the symplectic groups Sp_{2d}, the special orthogonal groups SO_n (here we have to assume q odd), and the Dickson group G_2 (in both cases q odd and even). We give explicit difference equations for all of these groups. As another result, we show that every semisimple and simply-connected group $\mathcal{G}$ that is defined over $\mathbb{F}_q$ occurs as a σ_i-difference Galois group over $F_i = \mathbb{F}_{q^i}(s,t)$ for some $i \in \mathbb{N}$, where $\sigma_i(s) = s^{q^i}$.
We also lift our difference equations from $\mathbb{F}_q(s,t)$ to $\overline{\mathbb{F}_q(s)}(t)$ using the fact that all of our constructed Galois groups are connected. As a result we obtain rigid analytically trivial pre-t-motives with the same Galois groups. The category of rigid analytically trivial pre-t-motives contains the category of t-motives, which occurs in the arithmetic of function fields.

For an outline of the approach, suppose we are given a linear algebraic group $\mathcal{G} \leq \mathrm{GL}_n$. Assume that we have fixed a difference equation $\sigma(y) = Ay$ over F for which we would like to show that there exists a Picard-Vessiot ring with difference Galois group equal to $\mathcal{G}$. For the existence of a Picard-Vessiot ring, we use a Henselian type of argument to show that under certain assumptions, there exist enough solutions inside a suitable extension L of F. If moreover A is contained in $\mathcal{G}(F)$, we deduce that the difference Galois group $\mathcal{H}$ is contained in $\mathcal{G}$. In order to be able to show that $\mathcal{H} \geq \mathcal{G}$ holds, we develop a lower bound criterion as follows. Let $\alpha \in \mathbb{F}_q$ be an element such that the matrix A_α obtained from $A \in \mathrm{GL}_n(\mathbb{F}_q(s,t))$ by substituting s by α is a well-defined element of $\mathrm{GL}_n(\mathbb{F}_q(t))$. Then $\mathcal{H}$ contains a certain conjugate of A_α.
With these criteria at hand, we construct a matrix A that meets the assumptions on our criterion for the existence of a Picard-Vessiot ring, and such that any conjugates of the elements A_α ($\alpha \in \mathbb{F}_q$) generate $\mathcal{G}$. The latter condition leads us to questions on generating linear algebraic groups. We construct explicit generators of the classical groups that generate the group even up to a certain conjugacy. We also present a more general result for arbitrary reductive groups that split over $\mathbb{F}_q$.

Contents

Introduction

In analogy to the Galois theory of polynomials (or differential equations), *difference Galois theory* studies extensions generated by solutions to difference equations with respect to a fixed automorphism σ of the base field F. A (linear) *difference equation* is an equation of the form

$$\sigma(y) = Ay$$

with $A \in \mathrm{GL}_n(F)$ and y a vector consisting of n indeterminates. There is the notion of a *Picard-Vessiot ring* which is in some sense a " smallest" ring extension R of F together with an extension of σ such that there exists a full set of solutions with entries in R to the given difference equation. In case the *constants* C of F (the elements fixed by σ) are algebraically closed, there always exists a unique Picard-Vessiot ring (up to isomorphism). The *difference Galois group* can then be defined as the group of automorphisms of R that leave F (pointwise) invariant and commute with σ; it turns out to be a linear algebraic group defined over C. This can be generalized to the case of an arbitrary field of constants C, leading to difference Galois groups that are affine group schemes defined over C provided that there exists a Picard-Vessiot ring. Similar to the inverse problem in classical Galois theory, it is a natural question to ask which affine group schemes defined over C occur as Galois groups of some difference equations over the fixed base field F with fixed automorphism σ.

Let $F = \mathbb{F}_q(s,t)$ be a function field in two variables over the finite field $\mathbb{F}_q$ with σ acting trivially on $\mathbb{F}_q(t)$ and mapping s to s^q. In other words, σ is the Frobenius homomorphism on $\mathbb{F}_q(s)$ extended to F by setting $\sigma(t) = t$. Then the constants of F are $C = \mathbb{F}_q(t)$. The main result of this thesis is that the following groups occur as difference Galois groups over F: the special linear groups SL_n, the symplectic groups Sp_{2d}, the special orthogonal groups SO_n (here we have to assume q odd), and the Dickson group G_2 (in both cases q odd and even). We give explicit difference equations for all of these groups. See Theorems 5.4.4, 5.5.4, 5.6.4, 5.7.7 and 5.8.4, respectively. As another result, we show that every semisimple and simply-connected group $\mathcal{G}$ that is defined over $\mathbb{F}_q$ occurs as a σ_i-difference Galois group over $F_i = \mathbb{F}_{q^i}(s,t)$ for some $i \in \mathbb{N}$, (Theorem 6.4.1), where $\sigma_i(s) = s^{q^i}$.

For an outline of the approach, suppose we are given a linear algebraic group $\mathcal{G}$. Assume that we have fixed a difference equation $\sigma(y) = Ay$ for which we would like to show that there exists a Picard-Vessiot ring with difference Galois group equal to $\mathcal{G}$. For the existence of a Picard-Vessiot ring, it is sufficient to show that there exists a fundamental solution matrix $Y \in \mathrm{GL}_n(L)$ (i.e., $\sigma(Y) = AY$) for some field extension L of F such that σ extends to L without giving rise to new constants. We always work with L being the field of fractions of the ring of power series in t that converge in a certain sense (with coefficients in a field extension K of $\mathbb{F}_q(s)$). Using a Henselian type of argument, it can be deduced that if the representing matrix A is contained in $\mathrm{GL}_n(\mathbb{F}_q(s)[t]_{(t)})$ and the coefficient matrices in its t-adic expansion can be bounded in a certain way, we always have a fundamental solution matrix $Y \in \mathrm{GL}_n(L)$, (Theorem 3.1.3). If moreover A is contained in $\mathcal{G}$, then Y can be chosen inside $\mathcal{G}(L)$, (Theorem 3.2.4). Let $\mathcal{H}$ denote the difference Galois group. Then $Y \in \mathcal{G}(L)$ implies that $\mathcal{H}$ is a closed subgroup scheme of $\mathcal{G}$ defined over $\mathbb{F}_q(t)$. The Picard-Vessiot ring R will turn out to be separable over F and it can be deduced that $\mathcal{H}$ is geometrically reduced; that is, it is a linear algebraic subgroup of $\mathcal{G}$. In order to be able to show that $\mathcal{H} \geq \mathcal{G}$ holds, we develop a lower bound criterion as follows. Let $\alpha \in \mathbb{F}_q$ be an element such that A is specializable modulo the ideal $(s-\alpha)$, that is, $A \in \mathcal{G}(\mathfrak{o}[t]_{(t)})$, where $\mathfrak{o} = \mathbb{F}_q[s]_{(s-\alpha)}$ denotes the valuation ring corresponding to $s-\alpha$. Then $\mathcal{H}(\mathbb{F}_q[[t]])$ contains a certain conjugate of the specialized matrix $A_\alpha \in \mathcal{G}(\mathbb{F}_q[[t]])$, (see Corollary 3.3.11). The criterion developed here actually works in the more general case $F = k(t) \supset \mathbb{F}_q(t)$ with k a (not necessarily discretely) valued field with finite residue field.
The idea to work with specializations to obtain elements of the Galois group up to conjugacy is inspired by finite Galois theory. Every finite Galois extension of $\mathbb{F}_q(s)$ is the Picard-Vessiot ring of a difference equation $\sigma_0(y) = A_0 y$ with $A_0 \in \mathrm{GL}_n(\mathbb{F}_q(s))$ and with σ_0 the ordinary Frobenius homomorphism on $\mathbb{F}_q(s)$. In [Mat04], Matzat gave a lower bound criterion for these kind of difference equations using specializations of A_0 from $\mathbb{F}_q(s)$ to $\mathbb{F}_q$, which led to the explicit realization of various finite groups of Lie type over $\mathbb{F}_q(s)$, (see [AM10]).
In our context of difference Galois theory, we are able to obtain elements inside $\mathcal{H} \leq \mathcal{G}$ up to a certain conjugacy. Hence we need to choose A so that it specializes to elements that generate $\mathcal{G}$ up to conjugacy. In case $\mathcal{G}$ is a classical group, we lift a result due to Malle, Saxl and Weigl concerning generation of $\mathcal{G}(\mathbb{F}_q)$, and construct explicit maximal tori T_1 and T_2 defined over $\mathbb{F}_q$ such that any $\mathcal{G}(\mathbb{F}_q + t\overline{\mathbb{F}}_q[[t]])$-conjugates of them generate $\mathcal{G}$, (Theorem 4.2.5). We then build A in such a way that it specializes to elements t_1, t_2 that generate dense subgroups of T_1 and T_2. In case $\mathcal{G} = G_2$, we proceed in a similar way.

To show that every semisimple and simply-connected group $\mathcal{G}$ that is defined over $\mathbb{F}_q$ occurs as a σ_i-difference Galois group over $F_i = \mathbb{F}_{q^i}(s,t)$ for some $i \in \mathbb{N}$, (Theorem 6.4.1), we use a result of Nori asserting that $\mathcal{G}(\mathbb{F}_q)$ itself can be realized over $\mathbb{F}_q(s)$. We can extend the matrix $A_0 \in \mathrm{GL}_n(\mathbb{F}_q(s))$ coming from Nori's result to an $A \in \mathrm{GL}_n(\mathbb{F}_q(s)[t]_{(t)})$ with constant coefficient matrix A_0. This implies that $\mathcal{G}(\mathbb{F}_q)$ is contained in $\mathcal{H}(\mathbb{F}_q[[t]])$, and we choose A such that it specializes to an element generating a dense subgroup of a maximal torus T that splits over $\mathbb{F}_{q^i}$. Using our lower bound criterion, it then suffices to show the following: If $\mathcal{G}$ is an $\mathbb{F}_q$-split reductive group with split maximal torus T, any $\mathcal{G}(\mathbb{F}_q + t\overline{\mathbb{F}}_q[[t]])$-conjugate of T together with $\mathcal{G}(\mathbb{F}_q)$ generates a dense subgroup of $\mathcal{G}$, (Theorem 4.3.1).

It should be mentioned that in case $F = \overline{\mathbb{F}}_q(s)((t))$ with σ acting coefficient-wise as the Frobenius homomorphism on $\overline{\mathbb{F}}_q(s)$ (hence the constants of F equal $\mathbb{F}_q((t))$), the inverse problem has been solved by Matzat. Namely, Theorem 2.3 in [Mat09] implies that any linear algebraic group defined over $\mathbb{F}_q((t))$ occurs as a difference Galois group over $\overline{\mathbb{F}}_q(s)((t))$. However, this result is based on taking t-adical limits, so it cannot be transferred to our non-complete base field $\mathbb{F}_q(s)(t)$ or even $\overline{\mathbb{F}}_q(s)(t)$.

There is a certain class of difference equations that occurs in the number theory of function fields. In 1974, Drinfeld introduced a class of $\mathbb{F}_q[t]$-modules which are today called *Drinfeld modules*, (see [Dri74]). These modules can be regarded as a function field analog of elliptic curves. An important example is the Carlitz module, which Carlitz had already introduced in 1935, [Car35], in order to study class field theory over the rational function field. As when passing from elliptic curves to abelian varieties, one can step up from Drinfeld modules to a category of higher dimensional objects, called *t-modules*, which were introduced by Anderson in 1986, (see [And86]). Anderson also introduced the category of so-called *t-motives* which is anti-equivalent to the category of t-modules, (more precisely, to the category of so-called abelian t-modules). A t-motive gives rise to a unique difference equation over $(\overline{\mathbb{F}_q(s)}(t), \sigma)$, where $\sigma(\alpha) = \alpha^q$ for all $\alpha \in \overline{\mathbb{F}_q(s)}$ and $\sigma(t) = t$, that posseses a Picard-Vessiot ring inside a certain field. In this way, one can assign a difference Galois group to a t-motive. It has been shown by Papanikolas, (see [Pap08, Theorem 4.5.10]), that this difference Galois group coincides with the so-called t-motivic Galois group assigned to a t-motive using the fact that the category of t-motives is a Tannakian category. Difference Galois theory has proved very powerful in transcendence theory over function fields, due to the fact that the dimension of the difference Galois group equals the transcendence degree of the Picard-Vessiot ring. For more details on the theory of t-motives, we refer the reader to the survey articles [BP11] and [Cha10] and the references listed there.

We lift our difference equations with Galois groups $\mathrm{SL}_n, \mathrm{Sp}_{2d}, \mathrm{SO}_n$, G_2 from $\mathbb{F}_q(s,t)$ to $\overline{\mathbb{F}_q(s)}(t)$ using the fact that all of these groups are connected. As result we obtain *rigid analytically trivial pre-t-motives* with these Galois groups. The category of rigid analytically trivial pre-t-motives contains the category of t-motives.

This thesis is organized as follows. The first chapter provides some background on the Galois theory of difference equations (with not necessarily algebraically closed fields of constants) treating all statements used later. In Chapter 2, we set up some notation and conventions that will be used throughout all following chapters. In Chapter 3, we develop techniques to guarantee that a difference equation has a certain difference Galois group. Specifically, Section 3.1 is concerned with the existence of Picard-Vessiot rings, while Sections 3.2 and 3.3 provide upper and lower bounds for difference Galois groups. Chapter 4 deals with finding generators that generate a linear algebraic group even after certain conjugacy. In Chapter 5, we then combine the results from Chapters 3 and 4 to construct difference equations with Galois groups SL_n, Sp_{2d}, SO_n and G_2, whereas Chapter 6 is devoted to the case of arbitrary semisimple simply-connected groups. In the last chapter, we give a short introduction to t-motives and translate our results to this setting.

Acknowledgments

I am deeply grateful to my advisor Prof. J. Hartmann for offering me the opportunity to pursue this project, for introducing me to lots of interesting mathematics, for her kind and useful advice, and for her constant support and encouragement.

I would like to thank Prof. B.H. Matzat for being available for my questions and for donating his time to write a report of this thesis. Prof. D. Harbater, Dr. L. Taelman and Dr. M. Wibmer have my appreciation for multiple fruitful discussions.

My thanks also go to everyone from Lehrstuhl A, especially my office mates, for the friendly and productive atmosphere. Finally, I would like to express my gratitude to all my friends and family for their encouragement throughout this project, with a special thank you to Katha and Max.

Chapter 1

Basics of Difference Galois Theory

In this chapter, we collect some basic facts about difference modules. Although most of it is well known, the literature seems to focus either on algebraically closed fields of constants (such as in [vdPS97]) or on a much more general (non-linear) theory of difference equations (such as in [Wib10b]), resulting in Galois groupoids. Therefore, we give a self-contained introduction to the theory of (linear) difference modules over difference fields with not necessarily algebraically closed field of constants.

1.1 Difference Rings and Difference Equations

Definition 1.1.1. *A* difference ring (R, ϕ) *is a commutative ring R equipped with a ring homomorphism $\phi\colon R \to R$. A* difference field *is a difference ring which is a field. The* constants C_R *of a difference ring R are the elements of R fixed by ϕ. A difference ring $S \geq R$ such that the homomorphism ϕ on S extends that on R is called a* difference ring extension. *A* difference ideal *of a difference ring R is a ϕ-stable ideal of R and R is called a* simple difference ring *if its only difference ideals are (0) and R. If R and S are difference rings, a homomorphism $\sigma\colon R \to S$ commuting with the difference structure on R and S is called a* difference homomorphism. *The set of all such is denoted by* $\mathrm{Hom}^{\phi}(R, S)$.

Remark 1.1.2. *Other than in [vdPS97], we do not assume ϕ to be an automorphism, as the following examples will demonstrate.*

Example 1.1.3.

- *Fix an element $q \in \mathbb{C}^{\times}$. Then $\mathbb{C}(t)$ together with ϕ given by $\phi(t) = qt$ is a so-called q-difference field with constants $\mathbb{C}$ if q is not a root of unity.*
- *Let now q be a prime power. Then $\mathbb{F}_q(s)$ together with the ordinary Frobenius homomorphism $\phi_q\colon \mathbb{F}_q(s) \to \mathbb{F}_q(s), z \mapsto z^q$ is a difference*

field with constants $\mathbb{F}_q$. This is an example where the difference homomorphism is not surjective.

- *Let q again be a prime power and consider $\mathbb{F}_q(s,t)$. Let ϕ_q be the homomorphism on $\mathbb{F}_q(s,t)$ fixing t and restricting to the ordinary Frobenius homomorphism on $\mathbb{F}_q(s)$. Then $\mathbb{F}_q(s,t)$ is a difference field extension of $\mathbb{F}_q(s)$, with constants $\mathbb{F}_q(t)$.*

Proposition 1.1.4. *Let (R,ϕ) be a simple difference ring (e.g. a difference field). Then C_R is a field.*

Proof. If $0 \neq a \in R$ is constant, then the principal ideal generated by a is a non-zero difference ideal and is thus all of R. Hence a is invertible inside R and clearly, the inverse is also constant. □

Definition 1.1.5. *Let (R,ϕ) be a difference ring and $A \in \mathrm{GL}_n(R)$. Then $\phi(Y) = AY$ is called a* (linear) difference equation *over R. Let S/R be an extension of difference rings. A matrix $Y \in \mathrm{GL}_n(S)$ satisfying $\phi(Y) = AY$ (where ϕ is applied coordinate-wise to Y) is called a* fundamental solution matrix *(or* fundamental matrix*, for short) for $\phi(Y) = AY$. The* solution space $\mathrm{Sol}_S(A)$ *is the set of all elements $y \in S^n$ with $\phi(y) = Ay$.*

Lemma 1.1.6. *Let $(S,\phi)/(R,\phi)$ be an extension of difference rings and let $\phi(Y) = AY$ be a difference equation given by a matrix $A \in \mathrm{GL}_n(R)$. Assume that there exist two fundamental matrices Y_1 and Y_2 contained in $\mathrm{GL}_n(S)$. Then $Y_2^{-1}Y_1$ is contained in $\mathrm{GL}_n(C_S)$.*

Proof. We have $\phi(Y_2^{-1}Y_1) = (AY_2)^{-1}AY_1 = Y_2^{-1}Y_1$, hence $Y_2^{-1}Y_1 \in \mathrm{GL}_n(S)$ has constant entries. It follows that the determinant is constant and as it is invertible inside S, it is also invertible inside C_S. Thus $Y_2^{-1}Y_1$ is contained in $\mathrm{GL}_n(C_S)$. □

Lemma 1.1.7. *Let $(E,\phi)/(F,\phi)$ be an extension of difference fields with field of constants $C = C_F = C_E$. Let further $\phi(Y) = AY$ be a difference equation over F for a matrix $A \in \mathrm{GL}_n(F)$ and let $y_1,\dots,y_m$ be contained in $\mathrm{Sol}_E(A)$. Then $y_1,\dots y_m$ are linearly independent over E if and only if they are linearly independent over C.*

Proof. Suppose $y_1,\dots,y_m$ are linearly independent over C but not over E. Choose $a_1,\dots,a_m \in E$ such that $\sum_{i=1}^{m} a_i y_i = 0$ is a non-trivial zero combination of minimal length. We may assume $a_1 = 1$. We apply ϕ and get $0 = \sum_{i=1}^{m} \phi(a_i)\phi(y_i) = \sum_{i=1}^{m} \phi(a_i)Ay_i$. We can now multiply with A^{-1} from the left to obtain $\sum_{i=1}^{m} \phi(a_i)y_i = 0$. Since $\phi(a_1) = 1 = a_1$, we get a shorter zero combination by subtracting $\sum_{i=1}^{m} \phi(a_i)y_i = 0$ from $\sum_{i=1}^{m} a_i y_i = 0$. Thus,

by minimality, $a_i = \phi(a_i)$ for all i. Hence all a_i are contained in C, a contradiction. □

Corollary 1.1.8. *Let E/F be an extension of difference fields and let $\phi(Y) = AY$ be a difference equation over F (for a matrix $A \in \mathrm{GL}_n(F)$). Let C be the field of constants of E. Then $\mathrm{Sol}_E(A)$ is a vector space over C of dimension less than or equal to n. We have equality if and only if there exists a fundamental solution matrix $Y \in \mathrm{GL}_n(E)$.*

Proof. It is clear from the definition that $\mathrm{Sol}_E(A)$ is a vector space over C. Any C-basis consists of elements in E^n that are linearly independent over E, by Lemma 1.1.7. Hence the dimension is at most n. The dimension equals n if and only if there exist n solutions, that are linearly independent over E (again by Lemma 1.1.7). This is equivalent to the existence of a fundamental matrix inside $\mathrm{GL}_n(E)$, since the columns of such matrix are contained in the solution space. □

Example 1.1.9. *Let (F, ϕ) be a difference field and consider an n-th order scalar difference equation*

$$l(x) := \phi^n(x) + \alpha_{n-1}\phi^{n-1}(x) + \cdots + \alpha_1\phi(x) + \alpha_0 x = 0$$

for $\alpha_0 \in F^\times$ and $\alpha_1, \ldots, \alpha_n \in F$. This is equivalent to the linear difference equation given by the matrix

$$A = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & & & & \ddots \\ -\alpha_0 & -\alpha_1 & \ldots & & -\alpha_{n-1} \end{pmatrix}.$$

Indeed, any solution y of l (i.e., $l(y) = 0$) contained in a difference field extension E gives rise to a solution vector $(y, \phi(y), \ldots, \phi^{n-1}(y))^{\mathrm{tr}} \in \mathrm{Sol}_E(A)$ and vice versa. In this way, the concept of scalar difference equations is covered by the theory of linear difference equations. In the situation of differential equations, the converse is also true, that is, every matrix is differentially equivalent to a matrix coming from a linear differential operator. This follows from the existence of cyclic vectors, a result usually referred to as cyclic vector lemma. The analog statement for difference equations has been proven for $\mathrm{char}(F) = 0$ in [HS99, Thm. B.2] under the assumption that ϕ is an automorphism and that there exist non-periodic elements.

Difference equations naturally arise in the study of difference modules:

Definition 1.1.10. *Let (F, ϕ) be a difference field. A* difference module *(or ϕ-module, for short) over F is a finite dimensional F-vector space M together with a ϕ-semilinear map $\Phi\colon M \to M$, (i.e., Φ is additive and for*

any $\lambda \in F$ and $x \in M$ we have $\Phi(\lambda x) = \phi(\lambda)\Phi(x)$) such that there exists a representing matrix D contained in $\mathrm{GL}_n(F)$, where $n = \dim_F(M)$. A representing matrix *D is defined as follows: With respect to a fixed basis of M, the action of Φ is completely described by the images of the basis elements. The representing matrix D (with respect to this basis) collects these images in its columns. Conversely, every $D \in \mathrm{GL}_n(F)$ gives rise to an n-dimensional difference module.*
A fundamental (solution) matrix *for M in some ring extension $R \geq F$ is defined to be a fundamental matrix for D^{-1} contained in $\mathrm{GL}_n(R)$.*

Remark 1.1.11. *Let (M, Φ) be a difference module over (F, ϕ) and fix a basis $\mathcal{B} = \{e_1, \ldots, e_n\}$ of M over F. We write $x_\mathcal{B} \in F^n$ for the representation of an element $x \in M$ with respect to $\mathcal{B}$. Let $x = \sum_{i=1}^n \lambda_i e_i$ be an element in M. Then $\Phi(x) = \sum_{i=1}^n \phi(\lambda_i)\Phi(e_i)$, hence $\Phi(x)_\mathcal{B} = D \cdot \phi(\lambda_1, \ldots, \lambda_n)^{\mathrm{tr}} = D\phi(x_\mathcal{B})$.*
Now if (R, ϕ) is a difference ring extension of (F, ϕ), then every element $y = (\lambda_1, \ldots, \lambda_n)^{\mathrm{tr}} \in \mathrm{Sol}_R(D^{-1})$ represents an element $x = \sum_{i=1}^n \lambda_i e_i \in M \otimes_F R$. We can extend the action of Φ naturally to $M \otimes_F R$ by $\Phi \otimes \phi$. We have $\phi(y) = D^{-1}y$, hence $\Phi(x)_B = D\phi(y) = DD^{-1}y = y = x_\mathcal{B}$, that is, $\Phi(x) = x$. Thus the elements of $M \otimes_F R$ fixed by Φ are exactly those $x \in M \otimes_F R$ such that $x_\mathcal{B}$ is contained in $\mathrm{Sol}_R(D^{-1})$. We conclude that there exists a Φ-invariant basis of $M \otimes_F R$ if and only if there exists a fundamental solution matrix $Y \in \mathrm{GL}_n(R)$ of the difference equation given by D^{-1}.

Remark 1.1.12. *Not every injective, ϕ-semilinear map gives rise to a difference module. For instance, endow $F = \mathbb{F}_q(s)$ with the ordinary Frobenius map ϕ and let $M = F^2$ with basis e_1, e_2. Now consider the ϕ-semilinear map given by $\Phi(e_1) = e_1$ and $\Phi(e_2) = se_1$. Then Φ is injective since no non-trivial linear combination $\phi_q(\alpha) + \phi_q(\beta)s$ can be zero, as s is not contained in the image of ϕ_q. Hence Φ is injective, but the representing matrix D equals $\begin{pmatrix} 1 & s \\ 0 & 0 \end{pmatrix}$, and is thus not contained in $\mathrm{GL}_n(F)$.*

1.2 Picard-Vessiot Rings

We now establish the notion of Picard-Vessiot rings of difference equations (which do not necessarily exist, and in case there exists one, it is not necessarily unique up to isomorphism, either).

Definition 1.2.1. *Let (F, ϕ) be a difference field with constants C and let A be an element in $\mathrm{GL}_n(F)$. An extension of difference rings R/F is called a Picard-Vessiot ring for A if the following holds:*

- *R is a simple difference ring.*

- *The field of constants of R is C.*
- *There exists a fundamental matrix $Y \in \mathrm{GL}_n(R)$, i.e., $\phi(Y) = AY$.*
- *R is generated as F-algebra by $\{Y_{ij}, \det(Y)^{-1} \mid 1 \leq i, j \leq n\}$.*

We will use the notation $F[Y, Y^{-1}] := F[Y_{ij}, \det(Y)^{-1} \mid 1 \leq i, j \leq n]$.

Remark 1.2.2. *a) In the literature, sometimes the second condition is dropped in the definition of a Picard-Vessiot ring in order to guarantee the existence of Picard-Vessiot extension.*

b) The last condition implies that R is minimal in the sense that no proper difference subring satisfies the first three conditions. Indeed, the second condition asserts that two fundamental matrices differ by an element in $\mathrm{GL}_n(C)$ so there can be no smaller difference ring R' with fundamental matrix contained in $\mathrm{GL}_n(R)$.

Definition 1.2.3. *If (M, Φ) is a difference module over (F, ϕ) with representing matrix $D \in \mathrm{GL}_n(F)$, a* Picard-Vessiot ring *of M is defined to be a Picard-Vessiot ring for the equation $\phi(Y) = AY$ with $A := D^{-1} \in \mathrm{GL}_n(F)$.*

Proposition 1.2.4. *Let R be a simple difference ring. Then R is reduced.*

Proof. Clearly, the radical of a difference ideal is again a difference ideal and since 1 is not contained in $\sqrt{(0)}$, we have $\sqrt{(0)} = (0)$ by simplicity of R. Thus there are no nilpotent elements in R other than zero. □

Remark 1.2.5. *Other than in the differential theory, a simple difference ring is not necessarily integral, even if the field of constants is algebraically closed. For a simple example in any characteristic not equal to 2, see [vdPS97, 1.6].*

Theorem 1.2.6. *Let F be a difference field with constants C and let R/F be an extension of difference rings such that R is a finitely generated F-algebra. Assume that R is a simple difference ring. Then the constants C_R of R are algebraic over C.*

Proof. We skip the proof, as we won't actually use this theorem. In case C is algebraically closed, a proof can be found in [vdPS97, 1.8] and the proof can be carried over to the case of arbitrary constants. Alternatively, we refer the reader to [Wib10a, 2.11], where the theorem is proven in a much more general situation (i.e., for constrained extensions of σ-pseudofields). The proof there makes use of a difference version of a Chevalley theorem which is proven in the same paper. □

Remark 1.2.7. *It is worth noticing that the converse is not true. That is, there can be elements that are separable algebraic over C but not constant. Take for example $R = F = \overline{\mathbb{F}}_q$ with $\phi = \phi_q$ the Frobenius homomorphism. Then $C_R = \mathbb{F}_q$. This is different from the differential case where there is a unique extension of a derivation to any separable algebraic extension.*

Example 1.2.8. *Let F be a field of characteristic $p > 0$, q a power of p and let $\phi = \phi_q$ be the ordinary Frobenius homomorphism on F. Let M be a difference module over F. Then M is called a finite Frobenius module over F. It can be shown that there always exists a unique (up to isomorphism) Picard-Vessiot ring for M which is then a finite Galois extension of F. Conversely, every Galois extension of F can be derived in this way (using additive polynomials). If the representing matrix of a finite Frobenius module M is of "sufficiently nice shape", it is also possible to derive a polynomial describing the corresponding Galois extension. We refer to [Mat04] for details.*

The objective of this section is to guarantee the existence of Picard-Vessiot rings provided there exists a fundamental matrix contained in a difference field extension with no new constants (see Theorem 1.2.11 below). As in the differential theory, we use the following correspondence of ideals for the proof.

Lemma 1.2.9. *Let (R, ϕ) be a simple difference ring with field of constants C and let S be a C-algebra. Equip $R \otimes_C S$ with the structure of a difference ring via $\phi \otimes_C \mathrm{id}$. Let $\mathcal{I}(S)$ denote the set of ideals inside S and let $\mathcal{I}(R \otimes_C S)^\phi$ denote the set of difference ideals in $R \otimes_C S$. Then there is a bijection*

$$\Gamma \colon \mathcal{I}(S) \to \mathcal{I}(R \otimes_C S)^\phi,\ I \mapsto R \otimes I = I \cdot R \otimes_C S,$$
$$\Delta \colon \mathcal{I}(R \otimes_C S)^\phi \to \mathcal{I}(S),\ J \mapsto J \cap S.$$

Proof. There is a short proof in [Wib10b, Prop.1.4.15] for this correspondence in a slightly different setting. The proof also works in our setup as we will now make sure. First note that Γ is well defined since every element in $S \subseteq R \otimes_C S$ is ϕ-stable. Let I be an ideal in S. Choose a vector space basis $\mathcal{B} = \{b_i \mid i \in \mathcal{I}\}$ of R over C. Then $\{b_i \otimes 1 \mid i \in \mathcal{I}\}$ is a basis of $R \otimes_C S$ as S-module. Thus $\Gamma(I)$ consists of all finite sums $\sum_{i \in \mathcal{I}} b_i \otimes s_i$ with all $s_i \in I$ and hence $\Delta(\Gamma(I)) = I$.

Let now J be a difference ideal inside $R \otimes_C S$. We will show that $\Gamma(\Delta(J)) = J$ holds. Clearly, $\Gamma(\Delta(J)) \subseteq J$. For the converse, let $\{e_i \mid i \in \mathcal{J}\}$ be a C-basis of $\Delta(J)$ and extend to a C-basis $\{e_i \mid i \in \mathcal{J} \cup \mathcal{J}'\}$ of S (such that $\mathcal{J} \cap \mathcal{J}' = \varnothing$). Then $\{1 \otimes e_i \mid i \in \mathcal{J} \cup \mathcal{J}'\}$ is also an R-basis of the free R-module $R \otimes_C S$ and $\{1 \otimes e_i \mid i \in \mathcal{J}\}$ is an R-basis of $R \otimes_C \Delta(J) = \Gamma(\Delta(J))$. Suppose that $\Gamma(\Delta(J)) \subsetneq J$ and let $a \in J \backslash \Gamma(\Delta(J))$ be an element of shortest

length, i.e., $a = \sum_{i \in \mathcal{J} \cup \mathcal{J}'} a_i \otimes e_i$ and $\tilde{\mathcal{J}}_a = \{i \in \mathcal{J} \cup \mathcal{J}' | a_i \neq 0\}$ is of minimal cardinality. We set $\tilde{\mathcal{J}} = \tilde{\mathcal{J}}_a$ and the minimality implies that we have $\tilde{\mathcal{J}} \subseteq \mathcal{J}'$. Fix an $i_0 \in \tilde{\mathcal{J}}$. Then

$$\{r_{i_0} \in R \mid \forall i \in \tilde{\mathcal{J}} \backslash \{i_0\} \; \exists r_i \in R : \sum_{i \in \tilde{\mathcal{J}}} r_i \otimes e_i \in J\}$$

is a difference ideal inside R, which is non-zero (since it contains $a_{i_0} \neq 0$). As R is difference simple, this ideal contains 1 and we may therefore assume that $a_{i_0} = 1$ holds. But then

$$a - \phi(a) = \sum_{i \in \tilde{\mathcal{J}} \backslash \{i_0\}} (a_i - \phi(a_i)) \otimes e_i$$

is of shorter length than a and has thus to be zero. We conclude that $a_i - \phi(a_i) = 0$ holds for all $i \in \tilde{\mathcal{J}}$ and thus a is contained in $(C \otimes_C S) \cap J = \Delta(J) \subseteq \Gamma(\Delta(J))$, a contradiction. □

Corollary 1.2.10. *Let (E, ϕ) be a difference field with field of constants C and let further $Z = (Z_{ij})_{i,j \leq n}$ consist of n^2 indeterminates. Equip $E[Z, Z^{-1}]$ with the difference homomorphism extending the given one on E and acting trivially on Z, i.e., $\phi(Z) = Z$. Then there is a bijection between $\mathcal{I}(C[Z, Z^{-1}])$, the set of ideals in $C[Z, Z^{-1}]$, and $\mathcal{I}(E[Z, Z^{-1}])^\phi$, the set of difference ideals in $E[Z, Z^{-1}]$ given by:*

$$\Gamma \colon \mathcal{I}(C[Z, Z^{-1}]) \to \mathcal{I}(E[Z, Z^{-1}])^\phi, \; I \mapsto I \cdot E[Z, Z^{-1}],$$
$$\Delta \colon \mathcal{I}(E[Z, Z^{-1}])^\phi \to \mathcal{I}(C[Z, Z^{-1}]), \; J \mapsto J \cap C[Z, Z^{-1}].$$

Proof. This follows directly from Lemma 1.2.9 by setting $R = E$ and $S = C[Z, Z^{-1}]$. □

Theorem 1.2.11. *Let (F, ϕ) be a difference field with field of constants C and let A be contained in $\mathrm{GL}_n(F)$. Assume that E/F is a difference field extension such that*

a) The field of constants of E is C,

b) There exists a fundamental matrix $Y \in \mathrm{GL}_n(E)$, i.e., $\phi(Y) = AY$,

Then $R := F[Y, Y^{-1}] \subseteq E$ is a Picard-Vessiot ring for A and R is the only Picard-Vessiot ring for A that is contained in E.

Proof. Any Picard-Vessiot ring contained in E is generated by a fundamental matrix in $\mathrm{GL}_n(E)$ and its inverse, so the uniqueness (inside E) follows from Lemma 1.1.6 together with $C_E = C \subseteq F$.
To see that R is a Picard-Vessiot ring it is sufficient to show that R is difference simple. Let X be a matrix consisting of n^2 indeterminates. Equip

$F[X, X^{-1}]$ with the difference homomorphism extending that on F such that $\phi(X) = AX$ holds. Then the natural homomorphism $\nu\colon F[X, X^{-1}] \to E$ given by $X_{ij} \mapsto Y_{ij}$ is a difference homomorphism with image R. Set $I = \ker(\nu)$. Then R is difference isomorphic to $F[X, X^{-1}]/I$ and we have to show that I is a maximal difference ideal inside $F[X, X^{-1}]$. Let $P \subsetneq F[X, X^{-1}]$ be a maximal difference ideal in $F[X, X^{-1}]$ containing I.

Define a set of n^2 new variables (Z_{ij}) by $Z = Y^{-1}X$. Then
$E \otimes F[X, X^{-1}] \cong E[X, X^{-1}] \cong E[Z, Z^{-1}]$, since Y has entries in E. Note that $E \otimes F[X, X^{-1}]$ becomes a difference ring via $\phi(e \otimes f) = \phi(e) \otimes \phi(f)$ and this is compatible with the difference structure on $E[Z, Z^{-1}]$ given by $\phi(Z) = Z$. Indeed, $\phi(Z) = Y^{-1}A^{-1}AX = Z$. Hence we can apply Corollary 1.2.10 to the difference ideal $P_E := P \cdot E[X, X^{-1}]$ inside $E[Z, Z^{-1}]$ which is therefore generated by $\mathfrak{p} := P_E \cap C[Z, Z^{-1}]$. Note that $E[Z, Z^{-1}]/P_E \cong (E \otimes_F F[X, X^{-1}])/(E \otimes_F P) \cong E \otimes_F (F[X, X^{-1}]/P) \neq 0$, where we used that E/F is free and thus flat. Hence P_E is a proper ideal of $E[Z, Z^{-1}]$ and so $\mathfrak{p}$ is a proper ideal of $C[Z, Z^{-1}]$. We can thus choose a maximal ideal $\mathfrak{m} \supseteq \mathfrak{p}$ inside $C[Z, Z^{-1}]$ containing $\mathfrak{p}$. Then $L := C[Z, Z^{-1}]/\mathfrak{m}$ is a finite field extension of C (see [AM69, Cor. 7.10]). (This is, by the way, the moment where it gets slightly more complicated because we do not assume our constants to be algebraically closed and thus in general $L \neq C$.)

Let $\kappa\colon C[Z, Z^{-1}] \twoheadrightarrow L$ be the residue map modulo $\mathfrak{m}$. Now E/F is flat, and thus

$$\begin{aligned} E \otimes_F (F[X, X^{-1}]/P) &\cong E[X, X^{-1}]/P_E = E[Z, Z^{-1}]/P_E \\ &\cong E \otimes_C (C[Z, Z^{-1}]/\mathfrak{p}) \overset{\mathrm{id}\otimes\kappa}{\twoheadrightarrow} E \otimes (C[Z, Z^{-1}]/\mathfrak{m}) = E \otimes_C L, \end{aligned}$$

where all homomorphisms are difference homomorphisms. Denote the resulting difference epimorphism $E \otimes_F (F[X, X^{-1}]/P) \twoheadrightarrow E \otimes_C L$ by γ. We then have the following commutative diagram of difference homomorphisms:

$$\begin{array}{ccc} E \otimes_F F[X, X^{-1}] & \xrightarrow{1\otimes X \mapsto Y\otimes Z} & E \otimes_C C[Z, Z^{-1}] \\ \downarrow & & \downarrow{\scriptstyle \mathrm{id}\otimes\kappa} \\ E \otimes_F (F[X, X^{-1}]/P) & \xrightarrow[\gamma]{} & E \otimes_C L \end{array}$$

where we write $Y \otimes Z$ short for the matrix product $(Y \otimes 1) \cdot (1 \otimes Z)$. Let now $\overline{Z}$ denote the image of Z inside $C[Z, Z^{-1}]/\mathfrak{m} = L$. We tensor the diagram up with $\otimes_C L$ and extend it to the following commutative diagram of difference

homomorphisms:

$$\begin{array}{ccc}
F[X,X^{-1}]\otimes_C L & & \\
{\scriptstyle X\otimes 1\mapsto 1\otimes X\otimes \overline{Z}^{-1}}\downarrow & & \\
E\otimes_F F[X,X^{-1}]\otimes_C L & \xrightarrow{1\otimes X\otimes 1\mapsto Y\otimes Z\otimes 1} & E\otimes_C C[Z,Z^{-1}]\otimes_C L \\
\downarrow & & \downarrow{\scriptstyle \mathrm{id}\otimes\kappa\otimes\mathrm{id}} \\
E\otimes_F (F[X,X^{-1}]/P)\otimes_C L & \xrightarrow[\gamma\otimes\mathrm{id}]{} & E\otimes_C L\otimes_C L \\
 & & \downarrow{\scriptstyle \mathrm{id}\otimes\mu} \\
 & & E\otimes_C L
\end{array}$$

where $\mu\colon L\otimes_C L\twoheadrightarrow L$ denotes the multiplication map. Let now ψ denote the resulting composition difference homomorphism
$\psi\colon F[X,X^{-1}]\otimes_C L\to E\otimes_C L$. We choose the upper path to compute

$$\psi\colon X\otimes_C 1\mapsto 1\otimes_F X\otimes_C \overline{Z}^{-1}\mapsto Y\otimes_C Z\otimes_C \overline{Z}^{-1}\mapsto Y\otimes_C \overline{Z}\otimes_C \overline{Z}^{-1}\mapsto Y\otimes_C 1$$

We conclude that $\psi=\nu\otimes_C \mathrm{id}_L$ and thus $\ker(\psi)=\ker(\nu)\otimes_C L=I\otimes_C L$, since L/C is flat. On the other hand, if we choose the lower path, it is clear that $P\otimes_C L$ is contained in $\ker(\psi)$. Hence $P\otimes_C L\subseteq I\otimes_C L$ and thus $P\subseteq I$, since L/C is free and thus faithfully flat. We conclude that $I=P$ is a maximal difference ideal in $F[X,X^{-1}]$. □

Definition 1.2.12. *In the situation as in Theorem 1.2.11, i.e., if R is an integral domain that is Picard-Vessiot for A, we call* $\mathrm{Quot}(R)$ *a* Picard-Vessiot extension *for A.*

Remark 1.2.13. *Other than in differential theory, the existence of a Picard-Vessiot ring does not imply the existence of a Picard-Vessiot extension, since a difference Picard-Vessiot ring is not necessarily a domain. It is therefore more natural to work with the total quotient rings of Picard-Vessiot rings instead of the field of fractions. However, the (explicitly constructed) Picard-Vessiot rings of the difference modules considered later on will always be domains, so Theorem 1.2.11 will be sufficient for our purpose.*

1.3 Galois Theory

We now give a construction of the Galois group scheme $\mathcal{G}$ of a Picard-Vessiot ring R, which turns out to be a linear algebraic group under certain separability assumptions. Other than in [Pap08], we will not assume our Picard-Vessiot ring to be integral. Also, our construction is more intrinsic as we are working with torsors. The Galois group scheme is then represented by the constants of $R\otimes_F R$.

Lemma 1.3.1. *Let (R, ϕ) be a simple difference ring with field of constants C. Let further S and S' be C-algebras and equip $R \otimes_C S$ and $R \otimes_C S'$ with the structure of a difference ring via $\phi \otimes_C \mathrm{id}$. Then $C_{R\otimes_C S} = C \otimes_C S$ and there is a natural bijection between $\mathrm{Hom}_C(S', S)$ and $\mathrm{Hom}_R^\phi(R \otimes_C S', R \otimes_C S)$.*

Proof. Since C is a field, we can choose a basis $\{s_\alpha | \alpha \in \mathcal{A}\}$ of S over C. Let $\sum r_\alpha \otimes s_\alpha \in R \otimes_C S$ be a constant. Then $\sum \phi(r_\alpha) \otimes s_\alpha = \sum r_\alpha \otimes s_\alpha$, hence all r_α are contained in C and thus $C_{R\otimes_C S} = C \otimes_C S \cong S$. Similarly, we have $C_{R\otimes_C S'} \cong S'$. Now if σ is contained in $\mathrm{Hom}_R^\phi(R \otimes_C S', R \otimes_C S)$, it maps constants to constants and hence restricts to a homomorphism contained in $\mathrm{Hom}_C(S', S)$. This yields a map $\mathrm{Hom}_R^\phi(R \otimes_C S', R \otimes_C S) \to \mathrm{Hom}_C(S', S)$ with inverse given by base extension. □

Proposition 1.3.2. *Let (F, ϕ) be a difference field with constants C and let R/F be a Picard-Vessiot ring for a matrix $A \in \mathrm{GL}_n(F)$. Then we have an R-linear isomorphism of difference rings*

$$R \otimes_F R \cong R \otimes_C C_{R\otimes_F R},$$

where $R \otimes_F R$ and $R \otimes_C C_{R\otimes_F R}$ are considered as difference rings via $\phi \otimes_F \phi$ and $\phi \otimes_C \mathrm{id}$, resp. Furthermore, we have

$$C_{R\otimes_F R} \cong C[Y^{-1} \otimes_F Y, (Y^{-1} \otimes_F Y)^{-1}]$$

where we again use the notation $Y^{-1} \otimes_F Y$ for the matrix product $Y^{-1} \otimes 1 \cdot 1 \otimes Y$.

Proof. Let

$$\psi \colon R \otimes_C C_{R\otimes_F R} \to R \otimes_F R$$

be the ring homomorphism given by $R \to R \otimes_F R$, $a \mapsto a \otimes 1$ on the left and the natural inclusion $C_{R\otimes_F R} \subseteq R \otimes_F R$ on the right. Then ψ is a difference ring homomorphism. All entries of $Y^{-1} \otimes_F Y$ and $Y \otimes_F Y^{-1}$ are constant and we have $1 \otimes_F Y = (Y \otimes_F 1) \cdot (Y^{-1} \otimes_F Y)$ as well as $1 \otimes_F Y^{-1} = (Y^{-1} \otimes_F 1) \cdot (Y \otimes_F Y^{-1})$. As R is generated over F by the entries of Y and Y^{-1} we conclude that ψ is surjective. The kernel of ψ is generated by its intersection with $C_{R\otimes_F R}$, by Lemma 1.2.9. As ψ is injective on $C_{R\otimes_F R}$, it is injective overall, so we proved the first statement.

To see that $C_{R\otimes_F R} = C[Y^{-1} \otimes Y, (Y^{-1} \otimes Y)^{-1}] = C[Y^{-1} \otimes Y, Y \otimes Y^{-1}]$ holds, we first observe that the very same proof as above yields a difference ring isomorphism

$$\tilde{\psi} \colon R \otimes_C C[Y^{-1} \otimes Y, Y \otimes Y^{-1}] \to R \otimes_F R.$$

Hence we get a difference ring isomorphism

$$\gamma := \tilde{\psi}^{-1} \circ \psi \colon R \otimes_F C_{R\otimes_F R} \to R \otimes_C C[Y^{-1} \otimes Y, Y \otimes Y^{-1}].$$

A difference ring homomorphism maps constant elements on constant elements, hence $\gamma(C_{R\otimes_F R})$ is contained in the constants of $R\otimes_C C[Y^{-1}\otimes Y, Y\otimes Y^{-1}]$. These are exactly $C[Y^{-1}\otimes Y, Y\otimes Y^{-1}]$ by Lemma 1.3.1. Hence γ induces an injective ring homomorphism

$$\gamma\colon C_{R\otimes_F R}\to C[Y^{-1}\otimes Y, Y\otimes Y^{-1}].$$

Clearly, this is surjective, as both $Y^{-1}\otimes Y, Y\otimes Y^{-1}$ are constant inside $R\otimes_F R$ and they are fixed by γ. □

Definition 1.3.3. *Let (F,ϕ) be a difference field with field of constants C and let R be a Picard-Vessiot ring for a matrix $A\in \mathrm{GL}_n(F)$. We write $\underline{Aut}(R/F)$ for the functor from the category of C-algebras to the category of groups sending a C-algebra S to the group $\mathrm{Aut}^{\phi}(R\otimes_C S/F\otimes_C S)$ of difference automorphisms fixing $F\otimes_C S$. Note that we consider $R\otimes_C S$ as difference ring via $\phi\otimes \mathrm{id}$.*

Next, we would like to show that $\underline{Aut}(R/F)$ is representable, i.e., it is an affine group scheme. We start with a preliminary lemma.

Lemma 1.3.4. *Let (F,ϕ) be a difference field with field of constants C and let R be a Picard-Vessiot ring for a matrix $A\in \mathrm{GL}_n(F)$. Then for every C-algebra S (considered as constant difference ring), we have*

$$\mathrm{Aut}^{\phi}(R\otimes_C S/F\otimes_C S)=\mathrm{End}^{\phi}(R\otimes_C S/F\otimes_C S).$$

Proof. Let $\sigma\colon R\otimes_C S\to R\otimes_C S$ be a difference homomorphism acting trivially on $F\otimes_C S$. We have to show that σ is bijective. Let I be the kernel of σ. Then I is a difference ideal of $R\otimes_C S$ and is thus generated by $I\cap S$, by Lemma 1.2.9. But as σ restricts to the identity on S, we have $I\cap S=(0)$ and σ is thus injective.
Let $Y\in \mathrm{GL}_n(R)$ be a fundamental matrix. Then $\det(Y)$ is contained in $R^{\times}\subseteq (R\otimes_C S)^{\times}$ and hence $\det(\sigma(Y))=\sigma(\det(Y))$ is also invertible inside $R\otimes_C S$. We conclude that $\sigma(Y)$ is contained in $\mathrm{GL}_n(R\otimes_C S)$. Also, $\phi(\sigma(Y))=\sigma(\phi(Y))=\sigma(AY)=A\sigma(Y)$. Hence both Y and $\sigma(Y)$ are fundamental matrices for A contained in $R\otimes_C S$, so there exists a $B\in \mathrm{GL}_n(C_{R\otimes_C S})$ such that $\sigma(Y)=YB$, by Lemma 1.1.6. Now $C_{R\otimes_C S}=S$ holds by Lemma 1.3.1, thus $B\in \mathrm{GL}_n(S)$. Recall that R is a Picard-Vessiot ring, hence we have $R=F[Y,Y^{-1}]$ and thus $R\otimes_C S$ is generated by the entries of Y and its inverse determinant over $F\otimes_C S$. As $Y=\sigma(Y\otimes B^{-1})$, we conclude that σ is surjective. □

Theorem 1.3.5. *The group functor $\underline{Aut}(R/F)$ is represented by the C-algebra $C_{R\otimes_F R}$, and is thus an affine group scheme over C.*

Proof. We abbreviate $R_{\mathcal{G}} := C_{R\otimes_F R}$. Let S be a C-algebra. We have to show that $\underline{Aut}(R/F)(S) = \mathrm{Hom}_C(R_{\mathcal{G}}, S)$ holds. We have

$$\mathrm{Hom}_C(R_{\mathcal{G}}, S) = \mathrm{Hom}_R^{\phi}(R \otimes_C R_{\mathcal{G}}, R \otimes_C S) = \mathrm{Hom}_R^{\phi}(R \otimes_F R, R \otimes_C S),$$

where we use Lemma 1.3.1 for the first equality and the second equality follows from Proposition 1.3.2. It is well known (and easy to see) that there is a natural bijection between $\mathrm{Hom}_R(R\otimes_F R, R\otimes_C S)$ and $\mathrm{Hom}_F(R, R\otimes_C S)$ given by restriction and base extension. This bijection obviously preserves difference homomorphisms, and we get

$$\mathrm{Hom}_R^{\phi}(R \otimes_F R, R \otimes_C S) = \mathrm{Hom}_F^{\phi}(R, R \otimes_C S).$$

Similarly,

$$\begin{aligned} \mathrm{Hom}_F^{\phi}(R, R \otimes_C S) &= \mathrm{Hom}_{F\otimes_C S}^{\phi}(R \otimes_F (F \otimes_C S), R \otimes_C S) \\ &= \mathrm{Hom}_{F\otimes_C S}^{\phi}(R \otimes_C S, R \otimes_C S). \end{aligned}$$

Finally, we use Lemma 1.3.4 to conclude

$$\mathrm{Hom}_{F\otimes_C S}^{\phi}(R \otimes_C S, R \otimes_C S) = \mathrm{Aut}_{F\otimes_C S}^{\phi}(R \otimes_C S) = \underline{\mathrm{Aut}}(R/F)(S).$$

□

Definition 1.3.6. *Let (F, ϕ) be a difference field with field of constants C and let R be a Picard-Vessiot ring for a matrix $A \in \mathrm{GL}_n(F)$. We define the Galois group scheme of R/F to be $\mathcal{G}_{R/F} = \underline{\mathrm{Aut}}(R/F)$. Similarly, if (M, Φ) is a difference module over (F, ϕ) with a Picard-Vessiot ring R, we call $\mathcal{G}_{M,R} = \underline{\mathrm{Aut}}(R/F)$ the Galois group scheme of M (with respect to R, which is not unique, in general). In case E is a Picard-Vessiot extension of M with Picard-Vessiot ring $R \subseteq E$, we set $\mathcal{G}_{M,E} = \mathcal{G}_{M,R}$.*

Remark 1.3.7. *In case C is algebraically closed, the C-rational points of $\mathcal{G}$ are usually called the Galois group* $\mathrm{Gal}(R/F) = \mathrm{Aut}^{\phi}(R/F)$ *of R over F. However, if C is not algebraically closed, $\mathcal{G}(C)$ may not contain enough information to recover $\mathcal{G}$.*

Theorem 1.3.8 (Torsor-theorem)**.** *Let (F, ϕ) be a difference field with field of constants C and let R be a Picard-Vessiot ring for a matrix $A \in \mathrm{GL}_n(F)$. Then* $\mathrm{Spec}(R)$ *is a $\mathcal{G}_{R/F}$-torsor, i.e.,* $\mathrm{Spec}(R)$ *is a $\mathcal{G}_{R/F}$-variety via the morphism*

$$\Gamma\colon \mathrm{Spec}(R) \times_C \mathcal{G}_{R/F} \to \mathrm{Spec}(R)$$

such that

$$\mathrm{id} \times\Gamma\colon \mathrm{Spec}(R) \times_C \mathcal{G}_{R/F} \to \mathrm{Spec}(R) \times_F \mathrm{Spec}(R)$$

is an isomorphism.

Proof. We have $\mathrm{Spec}(R) \times_C \mathcal{G}_{R/F} \cong \mathrm{Spec}(R \otimes_C C_{R\otimes_F R})$ and $\mathrm{Spec}(R) \times_F \mathrm{Spec}(R) \cong \mathrm{Spec}(R \otimes_F R)$. By Proposition 1.3.2, there exists an R-linear isomorphism $R \otimes_F R \to R \otimes_C C_{R\otimes_F R}$ and the claim follows. □

As a corollary, we get the well-known identity between transcendence degree of Picard-Vessiot extensions and dimension of their Galois group scheme.

Corollary 1.3.9. *Let (F, ϕ) be a difference field with field of constants C and let R be a Picard-Vessiot ring for a matrix $A \in \mathrm{GL}_n(F)$ with Galois group scheme $\mathcal{G} = \mathcal{G}_{R/F}$. Then*

a) $R \otimes_F \overline{F} \cong C[\mathcal{G}] \otimes_C \overline{F}$, where $\overline{F}$ denotes an algebraic closure of F.

b) $\mathrm{trdeg}(R/F) = \dim(\mathcal{G})$, where $\mathrm{trdeg}(R/F)$ denotes the transcendence degree of R as F-algebra.

Proof. a) Abbreviate $X = \mathrm{Spec}(R)$. Theorem 1.3.8 implies that X is a $\mathcal{G}$-torsor. We have $R \otimes_F \overline{F} \cong C[\mathcal{G}] \otimes_C \overline{F}$ if and only if $X \times_F \overline{F} \cong \mathcal{G} \times_C \overline{F}$, which is equivalent to X having an $\overline{F}$-rational point (as for any $x \in X(\overline{F})$, $g \mapsto g \cdot x$ yields an isomorphism $\mathcal{G} \times_C \overline{F} \cong X \times_F \overline{F}$). Now $X(\overline{F}) \cong (X \times_F \overline{F})(\overline{F}) \neq \varnothing$ as $X \times_F \overline{F}$ is an affine scheme of finite type over $\overline{F}$, so its $\overline{F}$-rational points are exactly its closed points (which correspond to the maximal ideals of $R \otimes_F \overline{F}$).

b) follows directly from a).

□

Theorem 1.3.10. *Let (F, ϕ) be a difference field with field of constants C and let R be a Picard-Vessiot ring for a matrix $A \in \mathrm{GL}_n(F)$. Assume further that R is separable over F. Then the Galois group scheme $\mathcal{G} := \mathcal{G}_{R/F}$ of R/F is a linear algebraic group over C, that is, an affine group scheme of finite type over C, such that $\mathcal{G} \times_C \overline{C}$ is reduced (i.e., $\mathcal{G}$ is "geometrically reduced").*

Proof. By Theorem 1.3.5, $\mathcal{G}$ is an affine group scheme, represented by $R_{\mathcal{G}} := C_{R\otimes_F R}$. By Proposition 1.3.2, we have $R_{\mathcal{G}} \cong C[Y \otimes_F Y^{-1}, (Y \otimes_F Y^{-1})^{-1}]$, so $R_{\mathcal{G}}$ is finitely generated over C. It follows that $\mathcal{G}$ is of finite type over C. Now $\mathcal{G} \times_C \overline{C}$ is reduced if and only if $R_{\mathcal{G}} \otimes_C \overline{C}$ is reduced. It is therefore sufficient to show that $R_{\mathcal{G}} \otimes_C \overline{F}$ is reduced which is isomorphic to $R \otimes_F \overline{F}$, by Corollary 1.3.9a). We assumed that R is separable over F, hence $R \otimes_F \overline{F}$ is reduced. □

As in classical Picard-Vessiot theory, an explicit linearization of $\mathcal{G}_{R/F}$ can be given using a fundamental solution matrix:

Proposition 1.3.11. *Let R be a Picard-Vessiot ring over a difference field (F, ϕ) for a matrix $A \in \mathrm{GL}_n(F)$. Let C be the field of constants and let $\mathcal{G}$ be the Galois group scheme. Assume further that R is separable over F. Then there is a closed embedding $\rho\colon \mathcal{G} \hookrightarrow \mathrm{GL}_n$ of linear algebraic groups such that for any C-algebra S, we have*

$$\rho_S\colon \mathcal{G}(S) = \mathrm{Aut}^{\phi}(R \otimes_C S/F \otimes_C S) \to \mathrm{GL}_n(S),\ \sigma \mapsto Y^{-1}\sigma(Y).$$

Proof. Again, we set $R_{\mathcal{G}} := C_{R\otimes_F R}$, the coordinate ring of $\mathcal{G}$. We know that $\mathcal{G}$ is a linear algebraic group by Theorem 1.3.10. Recall that the coordinate ring $R_{\mathcal{G}}$ of $\mathcal{G}$ is the image of the homomorphism $\mu\colon C[Z, Z^{-1}] = C[\mathrm{GL}_n] \to R \otimes_F R,\ Z \mapsto Y^{-1} \otimes Y$. Hence we have a surjection on the coordinate rings $C[\mathrm{GL}_n] \twoheadrightarrow C[\mathcal{G}]$ which induces a closed embedding $\rho\colon \mathcal{G} \hookrightarrow \mathrm{GL}_n$. Now let σ be an element in $\mathrm{Aut}^{\phi}(R \otimes_C S/F \otimes_C S)$. We have to figure out which element in $\mathcal{G}(S) = \mathrm{Hom}_C(R_{\mathcal{G}}, S)$ corresponds to σ, explicitly. Therefore, we have to take a close look at the proof of Theorem 1.3.5. The homomorphism contained in $\mathrm{Hom}_R^{\phi}(R \otimes_F R, R \otimes_C S)$ that corresponds to σ maps $a \otimes_F b$ to $a \otimes 1 \cdot \sigma(b \otimes_C 1)$. Now the isomorphism $R \otimes_C R_{\mathcal{G}} \to R \otimes_F R$ constructed in Proposition 1.3.2 maps $1 \otimes \overline{Z}$ to $Y^{-1} \otimes Y$, where $\overline{Z}$ denotes the image of Z in $R_{\mathcal{G}} \cong C[Z, Z^{-1}]/\ker(\mu)$. Hence the homomorphism in $\mathrm{Hom}_R^{\phi}(R\otimes_C R_{\mathcal{G}}, R\otimes_C S)$ corresponding to σ maps $1 \otimes_C \overline{Z}$ to $(Y^{-1} \otimes_C 1)\cdot\sigma(Y \otimes_C 1) \in R \otimes_C S$. We have already seen in the proof of Lemma 1.3.4 that $(Y^{-1} \otimes_C 1)\cdot\sigma(Y \otimes_C 1)$ is contained in $\mathrm{GL}_n(C \otimes_C S) = \mathrm{GL}_n(S)$, and thus σ corresponds to the element in $\mathrm{Hom}_C(R_{\mathcal{G}}, S) = \mathcal{G}(S)$ given by $\overline{Z} \mapsto Y^{-1}\sigma|_R(Y)$, which corresponds to the element $Y^{-1}\sigma(Y)$ inside $\mathrm{GL}_n(S)$. □

Proposition 1.3.11 becomes particularly useful in order to obtain upper bounds on $\mathcal{G}_{R/F}$: Let R/F be a separable Picard-Vessiot ring for an $A \in \mathrm{GL}_n(F)$ with Galois group scheme $\mathcal{G}_{R/F}$. Assume that there exists a fundamental solution matrix Y that is contained in $\tilde{\mathcal{G}}(R)$ for some closed subgroup $\tilde{\mathcal{G}} \leq \mathrm{GL}_n$ defined over C. Then for all $\gamma \in \mathrm{Aut}(R \otimes_C S/F \otimes_C S)$, $\gamma(Y)$ is contained in $\tilde{\mathcal{G}}(R \otimes_C S)$ and $\mathcal{G}_{R/F} \cong \rho(\mathcal{G}_{R/F})$ is thus contained in $\tilde{\mathcal{G}}$.

Recall that the definition of the Galois group scheme of a linear difference equation depends on a fixed Picard-Vessiot ring. The following Corollary implies that distinct Picard-Vessiot rings lead to Galois group schemes that become isomorphic over $\overline{C}$.

Corollary 1.3.12. *Let (R_1, ϕ_1) and (R_2, ϕ_2) be Picard-Vessiot rings over a difference field (F, ϕ) for the same matrix $A \in \mathrm{GL}_n(F)$. Let C be the field of constants and let $\overline{C}$ denote an algebraic closure of C. Assume further that R_1 and R_2 are both separable over F. Then the Galois group schemes $\mathcal{G}_{R_1/F}$ and $\mathcal{G}_{R_2/F}$ are conjugate by an element in $\mathrm{GL}_n(\overline{C})$.*

Proof. We only sketch the proof as we won't actually use this result.
As $\mathcal{G}_{R_1/F}$ and $\mathcal{G}_{R_2/F}$ are both linear algebraic groups by Theorem 1.3.10, it

suffices to show that $\mathcal{G}_{R_1/F}(\overline{C})$ and $\mathcal{G}_{R_2/F}(\overline{C})$ are conjugate inside $\mathrm{GL}_n(\overline{C})$. Let I be a maximal difference ideal inside $R_1 \otimes_F R_2$ with respect to the difference structure given by $\phi_1 \otimes \phi_2$ on $R_1 \otimes_F R_2$. As R_1 and R_2 are difference simple, we obtain inclusions from R_1 and R_2 into $R := (R_1 \otimes_F R_2)/I$. Now the constants of R will be contained in $\overline{C}$, by Theorem 1.2.6 (which we didn't prove). As both Y_1 and Y_2 are fundamental matrices of $A \in \mathrm{GL}_n(F)$, Lemma 1.1.6 implies that $B := Y_1^{-1} \otimes_F Y_2 \in \mathrm{GL}_n(R)$ has constant entries. This implies that $R_1 \otimes_C \overline{C}$ and $R_2 \otimes_C \overline{C}$ are isomorphic as difference $\overline{C}$-algebras and $\mathcal{G}_{R_1/F}(\overline{C})$ and $\mathcal{G}_{R_2/F}(\overline{C})$ are conjugate via $B \in \mathrm{GL}_n(\overline{C})$, which can be seen using Proposition 1.3.11. □

Proposition 1.3.13. *Let (R, ϕ) be a Picard-Vessiot ring over a difference field (F, ϕ) with Galois group scheme $\mathcal{G}$. Let $\frac{a}{b}$ be an element in the total quotient ring of R (the localization at the set of all non zero divisors inside R). If $\frac{a}{b}$ is functorially invariant under the action of $\mathcal{G}$, i.e., for every C-algebra S and every $\sigma \in \mathrm{Aut}^{\phi}(R \otimes_C S/F \otimes_C S)$ we have*

$$\sigma(a \otimes_C 1) \cdot (b \otimes_C 1) = (a \otimes_C 1) \cdot \sigma(b \otimes_C 1),$$

then $\frac{a}{b}$ is contained in F.

Proof. Consider $S = R_{\mathcal{G}} := C_{R \otimes_F R}$ and consider the following F-linear difference homomorphism

$$R \xrightarrow{x \mapsto 1 \otimes x} R \otimes_F R \xrightarrow{\mu} R \otimes_C R_{\mathcal{G}},$$

where we use the isomorphism $\mu \colon R \otimes_F R \to R \otimes_C R_{\mathcal{G}}$ of difference R-modules from Proposition 1.3.2. This induces an $(F \otimes_C R_{\mathcal{G}})$-linear difference homomorphism

$$\sigma \colon R \otimes_C R_{\mathcal{G}} \to R \otimes_C R_{\mathcal{G}}.$$

By Lemma 1.3.4, this is an element in $\mathrm{Aut}^{\phi}(R \otimes_C R_{\mathcal{G}}/F \otimes_C R_{\mathcal{G}})$. By assumption, we thus have

$$\sigma(a \otimes_C 1) \cdot (b \otimes_C 1) = (a \otimes_C 1) \cdot \sigma(b \otimes_C 1).$$

We apply μ^{-1} on both sides (note that $\mu^{-1}(x \otimes_C 1) = x \otimes_F 1$ for all $x \in R$ since μ^{-1} is R-linear) to get $(1 \otimes_F a) \cdot (b \otimes_F 1) = (a \otimes_F 1) \cdot (1 \otimes_F b)$. Hence $b \otimes_F a = a \otimes_F b$ and we conclude that $\frac{a}{b}$ is contained in F. □

We just proved the easy direction of a Galois correspondence for difference modules. We refer the reader to [AM05, Thm. 3.9] and [Wib10b, Thm. 3.10.7] for full proofs of the Galois correspondence in the general setting.

1.4 Base Change

An F-algebra is called *regular* if $R \otimes_F \tilde{F}$ is an integral domain for every field extension $\tilde{F}/F$. By Corollary 1 in [Bou90, V.5.17], this is equivalent to $R \otimes_F \overline{F}$ being an integral domain for an algebraic closure $\overline{F}$ of F. If R is a field extension of F such that R is a regular F-algebra, R is called a *regular extension* of F.

Proposition 1.4.1. *Let (F, ϕ) be a difference field and let R/F be a Picard-Vessiot extension for a matrix $A \in \mathrm{GL}_n(F)$ such that its Galois group scheme $\mathcal{G}$ is a connected linear algebraic group, that is, it is geometrically reduced and absolutely irreducible. Then*

a) R is a regular F-algebra. In particular, R is an integral domain.

b) $\mathrm{Quot}(R)$ is a regular extension of F. In particular, F is relatively algebraically closed in $\mathrm{Quot}(R)$ and $\mathrm{Quot}(R)/F$ is a separable extension.

Proof. a) As $\mathcal{G}$ is a connected linear algebraic group, $\overline{C}[\mathcal{G}] = C[\mathcal{G}] \otimes_C \overline{C}$ is an integral domain which implies that $C[\mathcal{G}]$ is a regular C-algebra. Hence $C[\mathcal{G}] \otimes_C \overline{F}$ is an integral domain and it is isomorphic to $R \otimes_F \overline{F}$ by Corollary 1.3.9. It follows that R is regular as an F-algebra.

b) As R is a regular F-algebra, its field of fractions $\mathrm{Quot}(R)$ is a regular extension of F (see [Bou90, V.17.4 Corollary]). By Proposition 9 in [Bou90, V.17.5], this is equivalent to F being relatively algebraically closed inside $\mathrm{Quot}(R)$ and $\mathrm{Quot}(R)/F$ being separable.

□

Theorem 1.4.2. *Let (F, ϕ) be a difference field and let R/F be a Picard-Vessiot ring for a matrix $A \in \mathrm{GL}_n(F)$ such that its Galois group scheme $\mathcal{G}$ is a connected linear algebraic group.*
If $(\tilde{F}, \phi)$ is an algebraic difference field extension of F such that $\tilde{F}$ and R are both contained in some common difference field E without new constants, then $R \otimes_F \tilde{F}$ is a Picard-Vessiot ring over $(\tilde{F}, \phi)$ for A with Galois group scheme $\mathcal{G}$.

Proof. By Proposition 1.4.1, R is an integral domain and $\mathrm{Quot}(R)$ is regular over F, so $\mathrm{Quot}(R) \otimes_F \tilde{F}$ is an integral domain. Also, as $\tilde{F}$ is an algebraic extension of F, $\mathrm{Quot}(R)$ and $\tilde{F}$ are linearly disjoint over F by Proposition 9 in [Bou90, V.17.5]. So they are in particular algebraically disjoint over F (see [Bou90, V.14.5, Corollary 1]) and F is relatively algebraically closed inside $\mathrm{Quot}(R)$, so we can apply Proposition 1 in [Bou90, V.17.2] and get that the natural map $\mathrm{Quot}(R) \otimes_F \tilde{F} \to E$ given by $x \otimes y \mapsto xy$ is injective, since its kernel consists of the nilpotent elements inside $\mathrm{Quot}(R) \otimes_F \tilde{F}$. Clearly, this homomorphism is a difference homomorphism. So we can consider $R \otimes_F \tilde{F} \subseteq \mathrm{Quot}(R) \otimes_F \tilde{F}$ as a difference subring of E.

Let $Y \in \mathrm{GL}_n(R)$ be a fundamental solution matrix for A. Then $Y \otimes 1 \in \mathrm{GL}_n(R \otimes_F \tilde{F})$ is a fundamental solution matrix for A, as well, and $R \otimes_F \tilde{F}$ is generated by the entries of $Y \otimes 1$ and $(Y \otimes 1)^{-1} = Y^{-1} \otimes 1$ as an $\tilde{F}$-algebra, since $R = F[Y, Y^{-1}]$. As E has no new constants, Theorem 1.2.11 now implies that $R \otimes_F \tilde{F}$ is a Picard-Vessiot ring for A over $\tilde{F}$.

We abbreviate $\tilde{R} = R \otimes_F \tilde{F}$ and denote the Galois group scheme of $\tilde{R}/\tilde{F}$ by $\tilde{\mathcal{G}}$. Let S be a C-algebra. Then

$$\tilde{\mathcal{G}}(S) = \mathrm{Aut}^{\phi}(\tilde{R} \otimes_C S/\tilde{F} \otimes_C S) = \mathrm{Hom}^{\phi}_{\tilde{F} \otimes_C S}(\tilde{R} \otimes_C S, \tilde{R} \otimes_C S),$$

where the last equality follows from Lemma 1.3.4. Now

$$\begin{aligned}
&\mathrm{Hom}^{\phi}_{\tilde{F} \otimes_C S}(\tilde{R} \otimes_C S, \tilde{R} \otimes_C S) \\
&\cong \mathrm{Hom}^{\phi}_{\tilde{F} \otimes_F (F \otimes_C S)}(\tilde{F} \otimes_F (R \otimes_C S), \tilde{F} \otimes_F (R \otimes_C S)) \\
&\cong \mathrm{Hom}^{\phi}_{F \otimes_C S}(R \otimes_C S, \tilde{F} \otimes_F (R \otimes_C S)) \\
&\supseteq \mathrm{Hom}^{\phi}_{F \otimes_C S}(R \otimes_C S, R \otimes_C S) = \mathcal{G}(S).
\end{aligned}$$

On the other hand, every $\gamma \in \mathrm{Aut}^{\phi}(\tilde{R} \otimes_C S/\tilde{F} \otimes_C S)$ restricts to an element in $\mathrm{Aut}^{\phi}(R \otimes_C S/F \otimes_C S)$. Indeed, $Y \otimes_F 1 \in \mathrm{GL}_n(R \otimes_F \tilde{F})$ is a fundamental matrix for $\tilde{R}$, hence $((Y^{-1} \otimes_F 1) \otimes_C 1)\gamma((Y \otimes_F 1) \otimes_C 1) \in \mathrm{GL}_n(C \otimes_C S)$ by Proposition 1.3.11. Therefore, $\gamma((Y \otimes_F 1) \otimes_C 1) \in \mathrm{GL}_n(R \otimes_C S)$, so γ restricts to an automorphism of $R \otimes_C S$ and we get $\tilde{\mathcal{G}}(S) \subseteq \mathcal{G}(S)$. Hence $\tilde{\mathcal{G}}(S) \cong \mathcal{G}(S)$ holds for all C-algebras S, so $\tilde{\mathcal{G}} \cong \mathcal{G}$. □

Chapter 2

Notation and Conventions

2.1 Difference Fields

In this section, we define difference fields $k(t) \subseteq K(t) \subseteq L$ with field of constants $\mathbb{F}_q(t)$.

p:	a prime number.
q:	a power of p.
K:	an algebraically closed field containing $\mathbb{F}_q$ that is complete with respect to a fixed non-archimedian absolute value $\lvert\cdot\rvert$ on K.
$\mathcal{O}_{\lvert\cdot\rvert}$:	the valuation ring in K corresponding to $\lvert\cdot\rvert$.
$\mathfrak{m}$:	the maximal ideal inside $\mathcal{O}_{\lvert\cdot\rvert}$.
$K\{t\}$:	the ring of power series that converge on the closed unit disk: $K\{t\} := \{\sum_{i=0}^{\infty} \alpha_i t^i \in K[[t]] \mid \lim_{i\to\infty} \lvert\alpha_i\rvert = 0\}$.
L:	the field of fractions of $K\{t\}$: $L = \mathrm{Quot}(K\{t\})$.
(K, ϕ_q):	on K, the homomorphism $\phi_q \colon K \to K,\ \lambda \mapsto \lambda^q$ is the ordinary Frobenius automorphism. The field of constants then equals $C_K = \mathbb{F}_q$.
(L, ϕ_q):	on $K\{t\}$, the homomorphism ϕ_q is defined by $\phi_q(\sum_{i=0}^{\infty} \alpha_i t^i) = \sum_{i=0}^{\infty} \phi_q(\alpha_i) t^i$ and ϕ_q extends uniquely to L. The field of constants then equals $C_L = \mathbb{F}_q(t)$ (see Lemma 2.1.3).
(k, ϕ_q):	a difference subfield of K containing $\mathbb{F}_q$. Note that ϕ_q is not necessarily surjective on k.
$\overline{k}$:	an algebraic closure of k contained in K.
$\overline{k}^{\mathrm{sep}}$:	a separable algebraic closure of k contained in $\overline{k}$.
$(k(t), \phi_q)$:	the difference structure on $k(t)$ is induced by that on $K(t) \subseteq L$, i.e., ϕ_q only acts on the coefficients of a rational function. Then $C_{k(t)} = \mathbb{F}_q(t)$ holds.

Example 2.1.1. *The standard example one should keep in mind is $k = \mathbb{F}_q(s)$, a function field in one variable with an s-adic absolute value $|\cdot|$. (Of course, one might also consider function fields $\mathbb{F}_q(s_1, \ldots, s_n)$ in several variables with $|\cdot|$ for instance an s_1-adic absolute value.) Then we let K be the completion of an algebraic closure of the completion of k, an algebraically closed field that is complete with respect to the unique extension of $|\cdot|$ on K.*

Remark 2.1.2. *a) Note that $L/k(t)$ is usually not a separable extension (as K/k might not be separable), and thus $(\mathbb{F}_q(t), k(t), L)$ is not a ϕ_q-admissible triple as defined in [Pap08, 4.1.]. However, in all applications we will consider a difference module over $k(t)$ with Picard-Vessiot extension E contained in L and we will explicitly show that E is separable over $k(t)$.*

b) Sometimes people work with the inverse σ of ϕ_q instead of ϕ_q, but since this is not defined on our base field $k(t)$ if k is not perfect, we prefer to work with ϕ_q, instead. Note that in case σ is well-defined, there is a 1-1 *correspondence between fundamental solution matrices Y with respect to σ, (i.e., $\sigma(Y) = D \cdot Y$ for a $D \in \mathrm{GL}_n(k(t))$) and fundamental solution matrices $\tilde{Y}$ with respect to ϕ_q, (i.e., $\tilde{Y} = D \cdot \phi_q(\tilde{Y})$), given by $Y = \phi_q(\tilde{Y})$ and $\tilde{Y} = \sigma(Y)$.*

Lemma 2.1.3. *The constants of (L, ϕ_q) are $C_L = \mathbb{F}_q(t)$.*

Proof. Consider first a constant element $g = \sum_{i=0}^{\infty} \alpha_i t^i \in K\{t\}$. Then we have $\phi_q(g) = g$, i.e., $\phi_q(\alpha_i) = \alpha_i$ holds for all $i \in \mathbb{N}$. As ϕ_q is the ordinary Frobenius homomorphism on K, this means that all α_i are contained in $\mathbb{F}_q$. In particular, each non-zero α_i is of value 1. As $(\alpha_i)_i$ converges to zero, this implies that g is contained in $\mathbb{F}_q[t]$.

Elements in $K\{t\}$ can be regarded as functions $\mathcal{O}_{|\cdot|} \to K$. It follows from Lemma 2.2.3 together with Corollary 2.2.4 of [FvdP04] that every non-zero element $f \in L$ has only finitely many zeroes and poles inside $\mathcal{O}_{|\cdot|}$. More precisely, there exist unique elements $\lambda \in K^\times$, $a_1, \ldots, a_d \in \mathcal{O}_{|\cdot|}$, $a'_1, \ldots, a'_{d'} \in \mathcal{O}_{|\cdot|}$ $(d, d' \in \mathbb{N})$ with $a_i \neq a'_j$ for all i, j, and $\alpha_i \in \mathfrak{m}$ $(i \in \mathbb{N})$ such that

$$f = \lambda(1 + \sum_{i=0}^{\infty} \alpha_i t^i) \frac{(t - a_1) \cdots (t - a_d)}{(t - a'_1) \cdots (t - a'_{d'})}$$

holds and $\sum_{i=0}^{\infty} \alpha_i t^i$ is contained in $K\{t\}$. We have

$$\phi_q(f) = \lambda^q(1 + \sum_{i=0}^{\infty} \alpha_i^q t^i) \frac{(t - a_1^q) \cdots (t - a_d^q)}{(t - a_1'^q) \cdots (t - a_{d'}'^q)}$$

so if f is constant, the unique factorization immediately implies that $\lambda(1 + \sum_{i=0}^{\infty} \alpha_i t^i) \in K\{t\}$ is also constant, hence is contained in $\mathbb{F}_q[t]$ by what we proved above. Therefore,

$$\frac{(t-a_1)\cdots(t-a_d)}{(t-a'_1)\cdots(t-a'_{d'})}$$

is constant too and thus contained in $\mathbb{F}_q(t)$ (of course, not all a_i and a'_i have to be contained in $\mathbb{F}_q$, but they are permuted by the action of ϕ_q). □

2.2 Algebraic Groups and Matrix Conventions

We use the term linear algebraic group defined over a field $\mathbb{F}$ to denote an affine group scheme of finite type over $\mathbb{F}$ that is geometrically reduced (that is, it is reduced over an algebraic closure of $\mathbb{F}$). We consider linear algebraic groups $\mathcal{G}$ over $\mathbb{F}$ as functors from $\mathbb{F}$-algebras to groups. We occasionally write things like $x \in \mathcal{G}$, by which we mean that x is contained in the $\tilde{\mathbb{F}}$-rational points of $\mathcal{G}$ for a suitable algebraically closed field $\tilde{\mathbb{F}}$ which should be clear from the context. If we write $\mathcal{G} \leq \mathrm{GL}_n$, we are given a closed embedding of $\mathcal{G}$ into GL_n and we will work with the coordinates inside GL_n. In particular, for any $\mathbb{F}$-algebra S, $\mathcal{G}(S)$ is identified with a subgroup of $\mathrm{GL}_n(S)$.
Normalizers, centralizers, and root subgroups are taken inside an algebraic closed field if not stated otherwise.

n: a natural number

M_n: for a ring R, $\mathrm{M}_n(R)$ denotes the ring of $n \times n$ matrices over R.

A^B: for a ring R, $A \in \mathrm{M}_n(R)$ and $B \in \mathrm{GL}_n(R)$, A^B denotes the conjugate $B^{-1}AB$.

$S_n \subseteq \mathrm{GL}_n$: we use the following convention for permutation matrices: the permutation matrix A_σ corresponding to a $\sigma \in S_n$ is the matrix with entries $A_{ij} = \delta_{i,\sigma(j)}$. We say that a matrix $A \in \mathrm{GL}_n$ is monomial with respect to a permutation $\sigma \in S_n$ if the entry A_{ij} is non-zero if and only if $i = \sigma(j)$ holds. In other words, there exists a diagonal matrix $d \in \mathrm{GL}_n$ such that $A = dA_\sigma$. Note that then $A^{-1}\,\mathrm{diag}(\lambda_1, \ldots, \lambda_n)A = \mathrm{diag}(\lambda_{\sigma(1)}, \ldots, \lambda_{\sigma(n)})$ holds for all diagonal matrices $\mathrm{diag}(\lambda_1, \ldots, \lambda_n)$.

Sp_{2d}: the symplectic group, where we are working with the symplec-

tic form given by

$$J = \begin{pmatrix} & & & & & -1 \\ & & & & \iddots & \\ & & & -1 & & \\ & & 1 & & & \\ & \iddots & & & & \\ 1 & & & & & \end{pmatrix},$$

i.e., $\mathrm{Sp}_{2d} = \{A \in \mathrm{GL}_{2d} \,|\, A^{\mathrm{tr}} J A = J\}$.

SO_n**:** the orthogonal group in non-even characteristic: $\mathrm{SO}_n = \{A \in \mathrm{SL}_n \,|\, A^{tr} J A = J\}$ with respect to

$$J = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}.$$

Chapter 3

Bounds on Difference Galois Groups

3.1 Existence of Picard-Vessiot Extensions

We start with a multidimensional version of Hensel's Lemma. For $m \in \mathbb{N}$, let $||\cdot||$ denote the maximum norm on K^n induced by $|\cdot|$:

$$||(a_1, \ldots, a_m)|| := \max\{|a_i| \mid 1 \leq i \leq m\}.$$

Lemma 3.1.1 (Hensel's Lemma)**.** *Let $f_1, \ldots, f_m \in \mathcal{O}_{|\cdot|}[X_1, \ldots, X_m]$ be a system of m polynomials in m variables with coefficients in $\mathcal{O}_{|\cdot|}$. Assume that there exists a vector $b = (b_1, \ldots, b_m) \in \mathcal{O}_{|\cdot|}^m$ such that $||(f_1(b), \ldots, f_m(b))|| < |\det(J_b)|^2$, where $J_b = (\frac{\partial f_i}{\partial y_j}(b))_{i,j}$ denotes the Jacobian matrix at b. Then there is a unique $a \in \mathcal{O}_{|\cdot|}^m$ satisfying $f_i(a) = 0$ for all $1 \leq i \leq m$ and*

$$||a - b|| = \frac{||J_b^* \cdot (f_1(b), \ldots, f_m(b))^{\mathrm{tr}}||}{|\det(J_b)|},$$

where J_b^* denotes the adjoint matrix of J_b.

This version of Hensel's Lemma is sometimes also called multi-dimensional Newton's Lemma. It holds for all henselian fields (note that K is henselian as it is complete with respect to a rank one valuation). For a proof, see Theorem 23 and 24 of [Kuh10].

Corollary 3.1.2. *Let A and B be contained in $\mathrm{M}_n(\mathcal{O}_{|\cdot|})$ and consider the system of polynomial equations*

$$AY^q - Y + B = 0,$$

where $Y = (Y_{ij})_{i,j \leq n}$ consists of n^2 indeterminates and $Y^q := (Y_{ij}^q)_{i,j}$. Assume that there exists a $Y' \in \mathrm{M}_n(\mathcal{O}_{|\cdot|})$ such that $||A(Y')^q - Y' + B|| < 1$. Then there exists a unique solution $Y \in \mathrm{M}_n(\mathcal{O}_{|\cdot|})$ of $AY^q - Y + B = 0$ such that $||Y - Y'|| = ||A(Y')^q - Y' + B||$.

Proof. This is an immediate consequence of Lemma 3.1.1. Indeed, let $f_{rs} \in \mathcal{O}_{|\cdot|}[Y_{ij} \mid 1 \leq i,j \leq n]$, $1 \leq r,s \leq n$ be the system of polynomials defining $AY^q - Y + B = 0$ and let A_{rs}, B_{rs} be the coordinates of A and B ($1 \leq r,s \leq n$). Then

$$f_{rs} = \sum_{m=1}^{n} A_{rm} Y_{ms}^q - Y_{rs} + B_{rs},$$

hence $\frac{\partial f_{rs}}{\partial Y_{ij}} = -\delta_{(i,j),(r,s)}$. This means that J_b equals the negative of the $n^2 \times n^2$ identity matrix for all $b \in M_n(K)$, so Y' meets the assumptions of the element b in Lemma 3.1.1. Also, up to a sign, $J_{Y'}^*$ equals the identity matrix, so the claim follows. □

Theorem 3.1.3. *Let $D = \sum_{l=0}^{\infty} D_l t^l \in \mathrm{GL}_n(\mathcal{O}_{|\cdot|}[[t]])$ (with $D_l \in \mathrm{M}_n(\mathcal{O}_{|\cdot|})$) be such that there exists a $\delta < 1$ with*

$$||D_l|| \leq \delta^l$$

for all $l \in \mathbb{N}$. Then there exists a fundamental matrix $Y \in \mathrm{GL}_n(L)$ for D, i.e., $D\phi_q(Y) = Y$. More precisely, $Y = \sum_{l=0}^{\infty} Y_l t^l \in \mathrm{GL}_n(\mathcal{O}_{|\cdot|}[[t]])$ with $Y_l \in \mathrm{M}_n(\mathcal{O}_{|\cdot|})$ satisfying $||Y_l|| \leq \delta^l$ for all $l \in \mathbb{N}$.

Proof. Observe that $D\phi_q(Y) = Y$ is equivalent to

$$D_0 Y_l^q + D_1 Y_{l-1}^q + \cdots + D_l Y_0^q = Y_l \quad \text{for all } l \in \mathbb{N}.$$

We define $(Y_l)_{l \geq 0}$ inductively. For $l = 0$, we need to solve $D_0\phi_q(Y_0) = Y_0$. The Lang isogeny (see [Bor91, V.16.4]) asserts that such a Y_0 exists inside $\mathrm{GL}_n(K)$, as K is algebraically closed. Then $Y_0^q = D_0^{-1} Y_0$ holds, hence $\mathcal{O}_{|\cdot|}[(Y_0)_{ij} \mid 1 \leq i \leq n]$ is finitely generated as an $\mathcal{O}_{|\cdot|}$-module, since $D_0 \in \mathrm{GL}_n(\mathcal{O}_{|\cdot|})$. Therefore, all entries of Y_0 are integral over $\mathcal{O}_{|\cdot|}$ (see for example [AM69, Prop. 5.1]) and as $\mathcal{O}_{|\cdot|}$ is integrally closed inside K, we conclude that $||Y_0|| \leq 1 = \delta^0$ holds. On the other hand, $D_0\phi_q(Y_0) = Y_0$ implies $\det(D_0)\det(Y_0)^q = \det(Y_0)$, hence $\det(Y_0)^{-1}$ is integral over $\mathcal{O}_{|\cdot|}$ which implies $\det(Y_0) \in \mathcal{O}_{|\cdot|}^{\times}$ and therefore $Y_0 \in \mathrm{GL}_n(\mathcal{O}_{|\cdot|})$.

Now suppose that $Y_0, \ldots, Y_{l-1}$ have been chosen such that for all $1 \leq i \leq l-1$, $||Y_i|| \leq \delta^i$ and $D_0 Y_i^q + D_1 Y_{i-1}^q + \cdots + D_i Y_0^q = Y_i$ holds. We claim that we can find $Y_l \in \mathrm{M}_n(\mathcal{O}_{|\cdot|})$ such that $D_0 Y_l^q + D_1 Y_{l-1}^q + \cdots + D_l Y_0^q = Y_l$ and $||Y_l|| \leq \delta^l$. Set

$$A := D_0 \in \mathrm{M}_n(\mathcal{O}_{|\cdot|})$$

and

$$B := D_1 Y_{l-1}^q + \cdots + D_l Y_0^q \in \mathrm{M}_n(\mathcal{O}_{|\cdot|}).$$

We have to find a solution to the polynomial system of equations

$$AY^q - Y + B = 0.$$

We have

$$\begin{aligned} ||B|| &= ||D_1 Y_{l-1}^q + \cdots + D_l Y_0^q|| \\ &\leq \max\{||D_i Y_{l-i}^q|| \mid 1 \leq i \leq l\} \\ &\leq \max\{||D_i|| \cdot ||Y_{l-i}||^q \mid 1 \leq i \leq l\} \\ &\leq \max\{\delta^i \cdot \delta^{(l-i)q} \mid 1 \leq i \leq l\} \\ &\leq \delta^l, \end{aligned}$$

where we used that the maximum norm $||\cdot||$ coming from a non-archimedian absolute value is sub-multiplicative with respect to the matrix multiplication. Let $\theta \in \mathcal{O}_{|\cdot|}$ be an element such that $|\theta| \leq \delta$ and set $Y_l' = \theta^l \cdot I_n$, where I_n denotes the identity matrix. Then we have

$$||A(Y_l')^q - Y_l' + B|| \leq \max\{||A|| \cdot ||Y_l'||^q, ||Y_l'||, ||B||\} \leq \delta^l < 1.$$

Hence by Corollary 3.1.2, there exists an element $Y_l \in \mathrm{M}_n(\mathcal{O}_{|\cdot|})$ such that $AY_l^q - Y + B = 0$ and $||Y_l - Y_l'|| = ||A(Y_l')^q - Y_l' + B|| \leq \delta^l$. As $||Y_l'|| \leq \delta^l$, we conclude $||Y_l|| \leq \delta^l$.

The resulting matrix $Y = \sum_{l=0}^{\infty} Y_l t^l \in \mathrm{M}_n(K\{t\}) \subseteq \mathrm{M}_n(L)$ satisfies $D\phi_q(Y) = Y$ and $||Y_l|| \leq \delta^l$ for all $l \in \mathbb{N}$. In particular, $Y \in \mathrm{M}_n(\mathcal{O}_{|\cdot|}[[t]])$ and we have seen above that $Y_0 \in \mathrm{GL}_n(\mathcal{O}_{|\cdot|})$, hence $Y \in \mathrm{GL}_n(\mathcal{O}_{|\cdot|}[[t]])$. □

Lemma 3.1.4. *a) Let $f = \sum_{i=0}^{m} f_i t^i \in \mathcal{O}_{|\cdot|}[t]$ be such that $f_0 \in \mathcal{O}_{|\cdot|}^{\times}$ and $f_i \in \mathfrak{m}$ for all $i > 0$. Then there exists a $\delta < 1$ such that $|f_i| \leq \delta^i$ holds for all i.*

b) Let $f \in \mathcal{O}_{|\cdot|}[[t]]^{\times}$ and assume there exist a $\delta < 1$ such that the absolute value of the i-th coefficients of f is less than or equal to δ^i for all i. Then the same is true for the i-th coefficient of f^{-1}.

c) Let $f, g \in \mathcal{O}_{|\cdot|}[[t]]$ and assume there exist a $\delta < 1$ such that the absolute value of the i-th coefficients of f and g are both less than or equal to δ^i. Then the same is true for the i-th coefficient of fg and $f + g$.

Proof. a) Set $\delta = \max\{|f_j| \mid 1 \leq j \leq m\}^{\frac{1}{m}} < 1$.

b) Let $\alpha_i \in \mathcal{O}$ be the coefficients of f: $f = \sum_{i=0}^{\infty} \alpha_i t^i \in \mathcal{O}[[t]]$. Then $\alpha_0 \in \mathcal{O}^{\times}$ and $|\alpha_i| \leq \delta^i$ for all i. Let $\beta_i \in \mathcal{O}$ denote the coefficients of f^{-1}. Then $|\beta_0| = |\alpha_0^{-1}| = 1$ and for $i > 1$, we have $\beta_i\alpha_0 + \cdots + \beta_0\alpha_i = 0$, hence $|\beta_i| \leq \max\{|\beta_j\alpha_{i-j}| \mid 0 \leq j \leq i-1\}$ and the claim follows inductively.

c) Let β_i and γ_i denote the i-th coefficients of f and g, resp. Then the i-th coefficient of fg equals $\beta_0\gamma_i + \beta_1\gamma_{i-1} + \cdots + \beta_i\gamma_0$ which is obviously

bounded from above by δ^i and the same is true for the i-th coefficient $\beta_i + \gamma_i$ of $f + g$.

□

Example 3.1.5. *Set $k = \mathbb{F}_q(s)$ with the s-adic absolute valuation $|\cdot|$ satisfying $|s| = \frac{1}{2}$. Let $(K, |\cdot|)$ be the completion of the algebraic closure of the completion of $(k, |\cdot|)$.*
We take a look at the difference module $(k(t)^2, \Phi)$ over $(k(t), \phi_q)$ where Φ is given by

$$\begin{pmatrix} f & -1 \\ 1 & 0 \end{pmatrix}$$

over $k(t)$, where

$$f = \frac{2t^2 + 2st + s^2 - 2}{t^2 + st + 1}.$$

If we alter f to

$$\tilde{f} = \frac{2s^{q-1}t^2 + 2st + s^2 - 2}{s^{q-1}t^2 + st + 1},$$

$\tilde{f}$ is contained in $\mathcal{O}_{|\cdot|}[[t]]$ and by Lemma 3.1.4 its i-th coefficient can be bounded from above by δ^i for a suitable $\delta < 1$ (more precisely, we can set $\delta := \frac{1}{2}$ in case $q \geq 3$ and $\delta := \frac{1}{\sqrt{2}}$ for $q = 2$). Consider a new difference module with representing matrix

$$\begin{pmatrix} \tilde{f} & -1 \\ 1 & 0 \end{pmatrix}$$

over $k(t)$. This matrix meets all assumptions of Theorem 3.1.3, so there exists a fundamental solution matrix inside $\mathrm{GL}_n(L)$ for this module. By Theorem 1.2.11, Y generates a Picard-Vessiot extension for this difference module.

Furthermore, if one considers specializations $s \mapsto \mathbb{F}_q^\times$, f and $\tilde{f}$ both specialize to the same element in $\mathbb{F}_q(t)$, as $s^{q-1} \mapsto 1$. In Section 3.3, we will show how to deduce information on the Galois group scheme of a difference module from such specializations.

A further class of examples covered by Theorem 3.1.3 is given in the following Corollary.

Corollary 3.1.6. *Suppose we are given a scalar difference equation*

$$\sum_{i=0}^{n} g_i(t)\phi_q^i(x) = 0 \tag{3.1}$$

with $g_i \in \mathcal{O}_{|\cdot|}[t]$, satisfying:

a) the constant coefficient of g_n has absolute value 1,

b) the constant coefficient of g_0 has absolute value 1,

c) For all $0 \leq i \leq n$, all coefficients of g_i, except (possibly) the constant coefficient, are contained in $\mathfrak{m}$.

Then there exist n $\mathbb{F}_q(t)$-linearly independent solutions x in $K\{t\} \subset L$.

Proof. Note that g_n and g_0 are invertible inside $\mathcal{O}_{|\cdot|}[[t]]$, by assumptions a) and b). For $0 \leq i \leq n-1$, set $\alpha_i := \frac{g_i}{g_n} \in \mathcal{O}_{|\cdot|}[[t]]$. Then the solutions to the given scalar difference equations are exactly the first coordinates of solution vectors to the linear difference equation $\phi_q(Y) = AY$ given by

$$A = \begin{pmatrix} & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ -\alpha_0 & -\alpha_1 & \dots & & -\alpha_{n-1} \end{pmatrix} \in \mathrm{M}_n(\mathcal{O}_{|\cdot|}[[t]]),$$

as explained in Example 1.1.9. We calculate $D := A^{-1}$

$$D = \begin{pmatrix} -\frac{\alpha_1}{\alpha_0} & & & -\frac{\alpha_{n-1}}{\alpha_0} & -\frac{1}{\alpha_0} \\ 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & 0 \end{pmatrix} \in \mathrm{M}_n(\mathcal{O}_{|\cdot|}[[t]]).$$

We have $\det(D) = \pm\frac{1}{\alpha_0} = \pm\frac{g_n}{g_0}$ which is invertible inside $\mathcal{O}_{|\cdot|}[[t]]$, hence $D \in \mathrm{GL}_n(\mathcal{O}_{|\cdot|}[[t]])$.
Now assumption c) together with Lemma 3.1.4 asserts that for all entries D_{ij} of D, there exists a $\delta_{ij} < 1$, such that $|(D_{ij})_l| \leq |\delta_{ij}|^l$ holds for all $l \in \mathbb{N}$. Let δ denote the maximum of all δ_{ij}. Then $||D_l|| \leq \delta^l$ holds for all $l \in \mathbb{N}$, where D_l denotes the coefficient matrix at t^l of D. Theorem 3.1.3 then gives us a fundamental solution matrix $Y \in \mathrm{GL}_n(L)$ for D with entries in $K\{t\}$. Each column of Y is of the form $(y, \phi_q(y), \dots, \phi_q^{n-1}(y))^{\mathrm{tr}}$ with y a solution to the given scalar difference equation and it follows that these have to be linear independent over $C_L = \mathbb{F}_q(t)$. □

3.2 Upper Bounds

Let F be a difference field with field of constants C_F and let $\mathcal{G}$ be a connected linear algebraic group defined over C_F. For algebraically closed fields of constants it is well known that the Galois group of a difference module is contained in $\mathcal{G}$ if its representing matrix is contained in $\mathcal{G}(F)$ (see for example [vdPS03, Prop. 1.31]). In our setup of difference fields with a valuation and fields of constants $\mathbb{F}_q(t)$, we prove such a criterion under certain assumptions (see Theorem 3.2.4 below). The strategy is to show that there exists a fundamental matrix contained in $\mathcal{G}$ if there exists one in GL_n. This implies that the Galois group scheme is contained in $\mathcal{G}$ (see Prop. 1.3.11).
The fundamental matrix inside $\mathcal{G}$ is constructed by multiplying the given fundamental solution matrix $Y \in \mathrm{GL}_n$ (which could be one coming from Theorem 3.1.3) by a constant matrix $C \in \mathrm{GL}_n(C_F)$ from the right hand side. The transformation $Y \mapsto YC$ maps a fundamental solution matrix on a fundamental solution matrix which is contained in the same Picard-Vessiot extension.

3.2.1 An Upper Bound Theorem

Theorem 3.2.1. *(Chevalley, see [Spr09, Theorem 5.5.3])*
Let $\mathcal{G}$ be a linear algebraic group over the algebraically closed field K and $\mathcal{H}$ a closed subgroup, both defined over the subfield k of K. Then there exists an $m \in \mathbb{N}$ and a closed embedding $\rho\colon \mathcal{G} \to \mathrm{GL}_m$, which is defined over k, such that there is a non-zero element $w \in k^m$ satisfying

$$\mathcal{H}(K) = \{g \in \mathcal{G}(K) \mid \rho(g)w \in Kw\}.$$

Note that the rational representation given in [Spr09] might not be a closed embedding itself, but it can be turned into one by taking the direct sum with an arbitrary closed embedding defined over k.

Lemma 3.2.2. *Let λ be contained in $\mathcal{O}_{|\cdot|}[[t]]^\times$. Then there exists a $\mu \in \mathcal{O}_{|\cdot|}[[t]]^\times$ satisfying*

$$\phi_q(\mu)\mu^{-1} = \lambda.$$

Proof. Let $\lambda = \sum_{i=0}^{\infty} \lambda_i t^i$ with $\lambda_0 \in \mathcal{O}_{|\cdot|}^\times$. Set $\mu = \sum_{i=0}^{\infty} \mu_i t^i$ and define μ_i inductively. We have $\phi_q(\mu) = \lambda\mu$ if and only if

$$\mu_j^q = \mu_j\lambda_0 + \mu_{j-1}\lambda_1 + \cdots + \mu_0\lambda_j \tag{3.2}$$

holds for all $j \in \mathbb{N}$. As K is algebraically closed, we can fix a $\mu_0 \in K^\times$ satisfying $\mu_0^q = \lambda_0\mu_0$. Then $|\mu_0|^{q-1} = |\lambda_0| = 1$, hence μ_0 is contained in $\mathcal{O}_{|\cdot|}^\times$. Now assume that $\mu_0, \ldots, \mu_{i-1} \in \mathcal{O}_{|\cdot|}$ have been fixed such that Equation (3.2) holds for all $0 \le j \le i-1$. Take any $\mu_i \in K$ satisfying Equation (3.2) for $j = i$. Then μ_i is integral over $\mathcal{O}_{|\cdot|}$ and is thus contained in $\mathcal{O}_{|\cdot|}$. □

Definition 3.2.3. *Assume that $\mathcal{O}_{|\cdot|}/\mathfrak{m}$ embeds into K. Then we can extend the canonical homomorphism $\kappa_{|\cdot|}\colon \mathcal{O}_{|\cdot|} \to \mathcal{O}_{|\cdot|}/\mathfrak{m}$ to a ring homomorphism*

$$\kappa_{|\cdot|}\colon \mathcal{O}_{|\cdot|}[[t]] \to (\mathcal{O}_{|\cdot|}/\mathfrak{m})[[t]] \to K[[t]],$$

by setting $\kappa_{|\cdot|}(\sum_{i=0}^{\infty} a_i t^i) = \sum_{i=0}^{\infty} \kappa_{|\cdot|}(a_i)t^i$ for any $a_i \in \mathcal{O}_{|\cdot|}$. Note that $\kappa_{|\cdot|}$ commutes with the action of ϕ_q since ϕ_q is the ordinary Frobenius automorphism on K.

In Section 3.1 we constructed fundamental matrices $Y \in \mathrm{GL}_n(L) \cap \mathrm{M}_n(K\{t\})$ (where L is as defined in Section 2). We will eventually need Y to be contained in $\mathcal{G}(K[[t]])$. Of course we still want to stay inside L (to ensure that we have no new constants) so we are looking for fundamental solution matrices contained in $\mathcal{G}(L \cap K[[t]])$. Note that $L \cap K[[t]] = \{\frac{f}{g} \mid f, g \in K\{t\}, t \nmid g\} \supsetneq K\{t\}$, for instance $(1-t)^{-1}$ is contained in $L \cap K[[t]]$ but $(1-t)$ is not invertible inside $K\{t\}$.

Theorem 3.2.4. *Assume that $\mathcal{O}_{|\cdot|}/\mathfrak{m}$ embeds into K. Let $\mathcal{G} \leq \mathrm{GL}_n$ be a connected linear algebraic group defined over $\mathbb{F}_q$. Let further $D \in \mathcal{G}(\mathcal{O}_{|\cdot|}[[t]])$ be such that $\kappa_{|\cdot|}(D)$ is contained in $\mathcal{G}(K)$ (i.e., no t appears!). Assume that there exists a matrix $Y \in \mathrm{GL}_n(\mathcal{O}_{|\cdot|}[[t]]) \cap \mathrm{M}_n(\mathcal{O}_{|\cdot|}\{t\})$ satisfying $D\phi_q(Y) = Y$. Then there exists a $Y' \in \mathcal{G}(L \cap \mathcal{O}_{|\cdot|}[[t]])$ with $D\phi_q(Y') = Y'$.*

Proof. For any matrix $A \in \mathrm{M}_n(\mathcal{O}_{|\cdot|}[[t]])$, we set $\tilde{A} := \kappa_{|\cdot|}(A)$ and similarly for vectors over $\mathcal{O}[[t]]$ and scalars in $\mathcal{O}[[t]]$.

By assumption, we have $\tilde{D} \in \mathcal{G}(K)$. As K is algebraically closed, the Lang isogeny (see [Bor91, V.16.4]) asserts that there exists an $X \in \mathcal{G}(K)$ satisfying $\tilde{D}\phi_q(X) = X$. Now Y is contained in $\mathrm{GL}_n(\mathcal{O}_{|\cdot|}[[t]]) \cap \mathrm{M}_n(\mathcal{O}_{|\cdot|}\{t\})$, hence $\tilde{Y} \in \mathrm{GL}_n(K[[t]]) \cap \mathrm{M}_n(K[t]) \subseteq \mathrm{GL}_n(K(t))$. As $\kappa_{|\cdot|}$ and ϕ_q commute, we have $\tilde{D}\phi_q(\tilde{Y}) = \tilde{Y}$. By Lemma 1.1.6, $C := \tilde{Y}^{-1}X$ is contained in $\mathrm{GL}_n(C_{K(t)}) = \mathrm{GL}_n(\mathbb{F}_q(t))$.

We set $Y' := YC$. Clearly, $D\phi_q(Y') = Y'$ holds since C has constant entries. We claim that Y' is contained in $\mathcal{G}(L \cap \mathcal{O}_{|\cdot|}[[t]])$. First of all, Y has entries in $\mathcal{O}_{|\cdot|}\{t\} \subseteq L$ and C has entries in $\mathbb{F}_q(t) \subseteq L$, hence $YC \in \mathrm{GL}_n(L)$. Also, $Y \in \mathrm{GL}_n(\mathcal{O}_{|\cdot|}[[t]])$, $\tilde{Y} \in \mathrm{GL}_n(K[[t]])$ and $X \in \mathrm{GL}_n(K)$, hence $C = \tilde{Y}^{-1}X \in \mathrm{GL}_n(K[[t]])$. We conclude $C \in \mathrm{GL}_n(\mathbb{F}_q(t)) \cap \mathrm{GL}_n(K[[t]]) \subseteq \mathrm{GL}_n(\mathbb{F}_q[[t]]) \subseteq \mathrm{GL}_n(\mathcal{O}_{|\cdot|}[[t]])$, thus $Y' = YC$ is also contained in $\mathrm{GL}_n(\mathcal{O}_{|\cdot|}[[t]])$. Therefore, it suffices to show that $Y' := YC$ is contained in $\mathcal{G}(\overline{K((t))})$.

By the Chevalley Theorem 3.2.1, there exists a closed embedding $\rho\colon \mathrm{GL}_n \to \mathrm{GL}_m$ defined over $\mathbb{F}_q$ and a non-zero element $w \in \mathbb{F}_q^m$ such that

$$\mathcal{G}(\overline{K((t))}) = \{g \in \mathrm{GL}_n(\overline{K((t))}) \mid \rho(g)w \in \overline{K((t))} \cdot w\}. \tag{3.3}$$

By multiplying w by a suitable element in $\mathbb{F}_q^\times$, we may assume that there exists a $j \leq m$ such that $w_j = 1$.
Note that ρ commutes with both ϕ_q and $\kappa_{|\cdot|}$, as these both act trivially on $\mathbb{F}_q$. Also note that whenever a matrix A is contained in $\mathrm{GL}_n(\mathcal{O}_{|\cdot|}[[t]])$, $\rho(A)$ will be contained in $\mathrm{GL}_m(\mathcal{O}_{|\cdot|}[[t]])$, as ρ is defined over $\mathbb{F}_q \subseteq \mathcal{O}_{|\cdot|}$, hence both $\rho(A)$ and $\rho(A^{-1})$ have entries in $\mathcal{O}_{|\cdot|}[[t]]$.

We will show that there exist $v \in \mathbb{F}_q[[t]]^m$ and $\mu \in \mathcal{O}_{|\cdot|}[[t]]^\times$ such that

$$\rho(Y'^{-1})w = \mu v \tag{3.4}$$

holds. If this is true, we will have

$$\begin{aligned}
\mu^{-1}\rho(Y'^{-1})w &= v = \kappa_{|\cdot|}(v) \\
&= \kappa_{|\cdot|}(\mu^{-1}\rho(Y'^{-1})w) \\
&= \tilde{\mu}^{-1}\rho(\tilde{Y}'^{-1})\tilde{w} \\
&= \tilde{\mu}^{-1}\rho(\tilde{C}^{-1}\tilde{Y}^{-1})w \\
&= \tilde{\mu}^{-1}\rho(C^{-1}\tilde{Y}^{-1})w \\
&= \tilde{\mu}^{-1}\rho(X^{-1})w,
\end{aligned}$$

where we repeatedly used that $\kappa_{|\cdot|}$ acts trivially on $\mathbb{F}_q[[t]]$. Now $X^{-1} \in \mathcal{G}(K)$, hence

$$\rho(X^{-1})w \in Kw$$

by (3.3). Also, $\tilde{\mu} \in K[[t]]^\times$ (as $\mu \in \mathcal{O}_{|\cdot|}[[t]]^\times$) so we conclude

$$\rho(Y'^{-1})w = \mu\tilde{\mu}^{-1}\rho(X^{-1})w \in K[[t]]w$$

which implies that $(Y')^{-1}$ and hence Y' is contained in $\mathcal{G}(\overline{K((t))})$ (see (3.3)).

It remains to show that there exist $v \in \mathbb{F}_q[[t]]^m$ and $\mu \in \mathcal{O}_{|\cdot|}[[t]]^\times$ satisfying Equation (3.4). First note that as $D \in \mathcal{G}(\mathcal{O}_{|\cdot|}[[t]]) \subseteq \mathcal{G}(\overline{K((t))})$, Equation (3.3) implies that there exists a $\lambda \in \overline{K((t))}$ satisfying

$$\rho(D)w = \lambda w.$$

We have $\rho(D) \in \mathrm{GL}_m(\mathcal{O}_{|\cdot|}[[t]])$, hence $\lambda = \lambda w_j = (\rho(D)w)_j \in \mathcal{O}_{|\cdot|}[[t]]$, as $w_j = 1$ and $w \in \mathbb{F}_q^m \subseteq \mathcal{O}_{|\cdot|}^m$. Similarly, $\lambda^{-1} = \lambda^{-1}w_j = (\rho(D)^{-1}w)_j \in \mathcal{O}_{|\cdot|}[[t]]$, hence λ is contained in $\mathcal{O}_{|\cdot|}[[t]]^\times$. We set
$v' := \rho(Y'^{-1})w \in \mathcal{O}_{|\cdot|}[[t]]^m$ and compute

$$\begin{aligned}
\phi_q(v') &= \phi_q(\rho(Y'^{-1})w) \\
&= \phi_q(\rho(Y'^{-1}))w \\
&= \rho(\phi_q(Y'^{-1}))w \\
&= \rho(Y'^{-1}D)w \\
&= \rho(Y'^{-1})\rho(D)w \\
&= \lambda v'.
\end{aligned} \tag{3.5}$$

By Lemma 3.2.2, there exists a $\mu \in \mathcal{O}_{|\cdot|}[[t]]^\times$ satisfying $\phi_q(\mu)\mu^{-1} = \lambda$. We define

$$v := \mu^{-1}v' = \mu^{-1}\rho(Y'^{-1})w.$$

Then $v \in \mathcal{O}_{|\cdot|}[[t]]^m$, and by Equation (3.5), we have

$$\phi_q(v) = \phi_q(\mu^{-1})\phi_q(v') = \phi_q(\mu^{-1})\lambda v' = v,$$

hence $v \in \mathbb{F}_q[[t]]^m$ and (v, μ) satisfy Equation (3.4) by definition. □

Example 3.2.5. *Let k, K, $\tilde{f}$ be as in Example 3.1.5. We again consider the difference module $(k(t)^2, \Phi)$ over $(k(t), \phi_q)$, where Φ is given by*

$$D := \begin{pmatrix} \tilde{f} & -1 \\ 1 & 0 \end{pmatrix}.$$

We have seen in Example 3.1.5 that there exists a fundamental solution matrix $Y \in \mathrm{GL}_2(L) \cap M_2(\mathcal{O}_{|\cdot|}\{t\})$ for this difference module. We would like to use Theorem 3.2.4 to show that there also exists a fundamental matrix in $\mathcal{G} := \mathrm{SL}_2$. (Of course, for $\mathcal{G} = \mathrm{SL}_2$ this could also easily be seen without using Theorem 3.2.4 - see Theorem 3.2.6).
However, we have $\mathcal{O}_{|\cdot|}/\mathfrak{m} \cong \overline{\mathbb{F}}_q$ which can be naturally embedded into K. The determinant of D equals one and we have seen in Example 3.1.5 that $\tilde{f}$ is contained in $\mathcal{O}_{|\cdot|}[[t]]$, hence $D \in \mathcal{G}(\mathcal{O}_{|\cdot|}[[t]])$. Furthermore, $\kappa_{|\cdot|}$ maps $s \mapsto 0$, hence

$$\kappa_{|\cdot|}(D) = \begin{pmatrix} -2 & -1 \\ 1 & 0 \end{pmatrix} \in \mathcal{G}(\overline{\mathbb{F}}_q),$$

i.e., no t appears in $\kappa_{|\cdot|}(D)$. Therefore, all assumptions of Theorem 3.2.4 are satisfied.

3.2.2 An Upper Bound for Linear and Symplectic Groups

For $\mathcal{G} = \mathrm{SL}_n$ and Sp_{2d}, it is quite easy to get an upper bound criterion for general difference fields and without any further assumptions on the representing matrix D apart from $D \in \mathcal{G}(F)$.

Theorem 3.2.6. *Let $\mathcal{G}$ be one of the following connected linear algebraic groups:*

a) the special linear group SL_n,

b) the symplectic group Sp_{2d} for $n = 2d$ even,

Let (F, ϕ) be a difference field with field of constants C_F and let $D \in \mathcal{G}(F)$. Let further E/F be a difference field such that $C_E = C_F$. Assume that there exists a $Y \in \mathrm{GL}_n(E)$ with $D\phi_q(Y) = Y$. Then there exists a $Y' \in \mathcal{G}(E)$ satisfying $D\phi_q(Y') = Y'$.

Proof. We have to construct a matrix $C \in \mathrm{GL}_n(C_F)$ with $Y' := YC \in \mathcal{G}(E)$. a) Note that $Y = D\phi(Y)$ implies $\det(Y) = \det(\phi(Y)) = \phi(\det(Y))$, since $D \in \mathrm{SL}_n(F)$. Hence $\det(Y)$ is contained in $C_E = C_F$ and we can define

$$C = \begin{pmatrix} \frac{1}{\det(Y)} & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}.$$

b) Recall that we are working with the symplectic group corresponding to

$$J = \begin{pmatrix} & & & & -1 \\ & & & \iddots & \\ & & -1 & & \\ & 1 & & & \\ \iddots & & & & \\ 1 & & & & \end{pmatrix},$$

i.e., $\mathrm{Sp}_n = \{A \in \mathrm{GL}_n \,|A^{\mathrm{tr}} JA = J\}$. Define $B = Y^{\mathrm{tr}} JY$. We use $Y = D\phi(Y)$ to compute

$$\begin{aligned} \phi(B) &= \phi(Y)^{\mathrm{tr}} J\phi(Y) \\ &= Y^{\mathrm{tr}} (D^{-1})^{\mathrm{tr}} JD^{-1}Y \\ &= Y^{\mathrm{tr}} JY \\ &= B, \end{aligned}$$

where we used that D^{-1} is symplectic in the third step. Hence B is contained in $\mathrm{GL}_n(C_F)$ and B is skew-symmetric, since J is. Multiplying Y from the right hand side by C transforms B into $C^{\mathrm{tr}} BC$. Every skew-symmetric matrix can be transformed into J by simultaneous row and column transformations (in other words, there is only one symplectic form), so there exists a $C \in \mathrm{GL}_n(C_F)$ satisfying $C^{\mathrm{tr}} BC = J$, i.e., YC is contained in $\mathrm{Sp}_{2d}(E)$. □

Remark 3.2.7. *Note that the same kind of argument also works for differential modules. To wit, let (M, ∂) be a differential module over a differential field F with not necessarily algebraically closed field of constants and denote the corresponding matrix differential equation by $A \in F^{n\times n}$. Assume that there exists a fundamental solution matrix Y, i.e., $\partial(Y) = AY$. Then*

$$\begin{aligned} \partial(Y^{\mathrm{tr}} JY) &= \partial(Y)^{\mathrm{tr}} JY + Y^{\mathrm{tr}} J\partial(Y) \\ &= Y^{\mathrm{tr}} A^{\mathrm{tr}} JY + Y^{\mathrm{tr}} JAY \\ &= Y^{\mathrm{tr}} (A^{\mathrm{tr}} J + JA)Y, \end{aligned}$$

so the matrix $Y^{\mathrm{tr}}JY$ *is constant if* A *is contained in the Lie-Algebra* $\{A \mid A^{\mathrm{tr}}J + JA = 0\}$ *corresponding to the symplectic group and the same kind of transformations* $Y \mapsto YC$ *as above can be applied to get a symplectic fundamental solution matrix.*

3.3 Lower Bounds

3.3.1 Setup for Specialization

In addition to the notation established in Chapter 2, we will use the following notation in this section.

d:	a fixed number $d \in \mathbb{N}$.
$(\mathfrak{o}, \mathfrak{p})$:	a valuation ring $\mathfrak{o}$ inside k with maximal ideal $\mathfrak{p}$ such that the residue field $\mathfrak{o}/\mathfrak{p}$ is isomorphic to $\mathbb{F}_{q^d}$. We do not assume $\mathfrak{o}$ to be discrete.
Γ:	the corresponding ordered abelian group $\Gamma = k^\times/\mathfrak{o}^\times$.
$(\mathcal{O}, \mathcal{P})$:	an extension of $(\mathfrak{o}, \mathfrak{p})$ to $\overline{k}^{\text{sep}}$.
Γ':	the corresponding ordered abelian group $\Gamma' := (\overline{k}^{\text{sep}})^\times/\mathcal{O}^\times$.
ν:	the corresponding valuation $\nu\colon \overline{k}^{\text{sep}} \to \Gamma' \cup \{\infty\}$. Note that ν restricts to $\nu\colon k \to \Gamma \cup \{\infty\}$.
κ:	the residue homomorphism $\kappa\colon \mathcal{O} \to \overline{\mathbb{F}}_q$. (We have $\mathcal{O}/\mathcal{P} \cong \overline{\mathbb{F}}_q$, as we assumed $\mathfrak{o}/\mathfrak{p} \cong \mathbb{F}_{q^d}$.) Note that κ restricts to $\kappa\colon \mathfrak{o} \to \mathbb{F}_{q^d}$.
ν_t:	the Gauss extension $\nu_t\colon k(t) \to \Gamma \cup \{\infty\}$ of ν, defined by $\nu_t(\sum_{i=0}^r a_i t^i) = \min\{\nu(a_i) \mid 0 \le i \le r\}$ for $a_i \in k$ and $r \in \mathbb{N}$ and extended to fractions of polynomials.
$(\mathfrak{o}_t, \mathfrak{p}_t)$:	the valuation ring $\mathfrak{o}_t$ of ν_t inside $k(t)$ with maximal ideal $\mathfrak{p}_t$. The residue class field equals $\mathfrak{o}_t/\mathfrak{p}_t \cong \mathbb{F}_{q^d}(t)$ (see [EP05, Cor. 2.2.2]).
$\mathcal{O}((t))$:	the ring of formal Laurent series over $\mathcal{O}$: $\mathcal{O}((t)) := \{\sum_{i=r}^\infty a_i t^i \mid r \in \mathbb{Z}, a_i \in \mathcal{O}\} = \mathcal{O}[[t]][t^{-1}]$.
$\mathcal{O}_t$:	the subring of $\overline{k}^{\text{sep}}((t))$ generated by $\mathfrak{o}_t$ and $\mathcal{O}((t))$, see Definition 3.3.6.
$(K((t)), \phi_q)$:	we define ϕ_q on $K((t))$ (and any subring thereof) by setting $\phi_q(\sum_{i=r}^\infty a_i t^i) = \sum_{i=r}^\infty \phi_q(a_i) t^i = \sum_{i=r}^\infty a_i^q t^i$ for $r \in \mathbb{Z}$ and $a_i \in K$. This is compatible with the definition on the subfield L of $K((t))$ made in Chapter 2.

Example 3.3.1. *Note that $\mathfrak{o}/\mathfrak{p} \cong \mathbb{F}_{q^d}$ includes restrictions on k which had been an arbitrary subfield of K, before. For instance k cannot equal $\overline{\mathbb{F}}_q(s)$ anymore, since $\overline{\mathbb{F}}_q$ can be embedded into the residue field of any valuation on $\overline{\mathbb{F}}_q(s)$. In all of our applications, $k = \mathbb{F}_q(s)$ with $\mathfrak{p}$ a place of degree d (in most cases actually $d = 1$). However the results from this chapter could also be applied in more general situations such as:*

- *k a finite extension of $\mathbb{F}_q(s)$ with $k \cap \overline{\mathbb{F}}_q \le \mathbb{F}_{q^d}$.*

- *$k = \mathbb{F}_q(s_1, \dots s_r)$ with $s_1, \dots, s_r$ algebraically independent. We give an example of a rank r valuation on k with $\mathfrak{o}/\mathfrak{p} \cong \mathbb{F}_q$ (i.e., $d = 1$): Choose $\alpha_1, \dots, \alpha_r \in \mathbb{F}_q$ and consider*

$$\nu : \ \mathbb{F}_q(s_1, \dots, s_l) \to \mathbb{Z}^l \cup \{\infty\}, \ 0 \neq f \mapsto (v_1(f), \dots, v_r(f)),$$

with $\mathbb{Z}^l$ ordered lexicographically and $\nu_1(f), \dots, \nu_r(f)$ defined as follows. The first component $\nu_1(f)$ is the $(s_1 - \alpha_1)$-adic valuation of f. Let $\mathfrak{o}_1 = \mathbb{F}_q[s_1, \dots, s_r]_{(s_1 - \alpha_1)}$ be the corresponding discrete valuation ring in k with valuation ideal $\mathfrak{p}_1 = (s_1 - \alpha_1)\mathfrak{o}_1$. Then we have $k_1 := \mathfrak{o}_1/\mathfrak{p}_1 \cong \mathbb{F}_q(s_2, \dots, s_l)$ with projection $\kappa_1 : \mathfrak{o}_1 \to k_1$. We can now define $\nu_2(f)$ to be the $(s_2 - \alpha_2)$-adic valuation of

$$\kappa_1(f \cdot (s_1 - \alpha_1)^{-\nu_1(f)})$$

inside k_1. Let $\mathfrak{o}_2$ and $\mathfrak{p}_2$ be the corresponding valuation ring and valuation ideal inside k_1. Then $k_2 := \mathfrak{o}_2/\mathfrak{p}_2 \cong \mathbb{F}_q(s_3, \dots, s_l)$. The components $\nu_3, \dots, \nu_l$ are defined inductively in the same way. Let $\mathfrak{o}$ be the (non-discrete) valuation ring inside k that corresponds to ν and $\mathfrak{p}$ the valuation ideal. By construction we have $\mathfrak{o}/\mathfrak{p} \cong \mathbb{F}_q$.

3.3.2 Specializing Fundamental Matrices

We start with a Lemma on the separability of solutions to systems of algebraic equations.

Lemma 3.3.2. *Let $n \in \mathbb{N}$ and let $K_1 \subseteq K_2$ be fields. Consider a system*

$$Ay^q + y + a = 0$$

of polynomial equations over K_1 for an $A = (A_{ij}) \in \mathrm{GL}_n(K_1)$ and $a = (a_1, \dots, a_n)^{\mathrm{tr}}$ contained in K_1^n, where $y = (y_1, \dots, y_n)^{\mathrm{tr}}$ consists of n indeterminates. Let $y \in K_2^n$ be a solution to $Ay^q + y + a = 0$. Then all coordinates of y are separable algebraic over K_1.

Proof. Let $f_1, \dots, f_n$ be the n polynomial equations in $y_1, \dots, y_n$ given by $Ay^q + y + a = 0$. Then we have

$$\frac{\partial f_i}{\partial y_j} = \frac{\partial(\sum_{i=1}^n A_{ij} y_j^q + y_i + a_i)}{\partial y_j} = \delta_{ij}. \tag{3.6}$$

Hence the Jacobian matrix $(\frac{\partial f_i}{\partial y_j})_{i,j}$ is constant and equals the identity matrix. It is therefore everywhere invertible and Proposition VIII.5.3. in [Lan02, Part II] implies that all solutions are separable and algebraic over K_1. □

The following proposition allows us to specialize a fundamental matrix Y in a compatible and well-defined way:

Proposition 3.3.3. *Let (M, Φ) be an n-dimensional ϕ_q-difference module over $k(t)$ with representing matrix $D \in \mathrm{GL}_n(k(t)) \subseteq \mathrm{GL}_n(k((t)))$ with respect to a fixed basis of M. Let further $\tilde{k}$ be a field containing $\overline{k}$. Assume that there exists a fundamental matrix $Y \in \mathrm{GL}_n(\tilde{k}((t)))$ for M. Then the following holds:*

a) If D is contained in $\mathrm{GL}_n(k[[t]])$, then Y is contained in $\mathrm{GL}_n(\overline{k}^{\mathrm{sep}}((t)))$.

b) If D is contained in $\mathrm{GL}_n(\mathfrak{o}[[t]])$, then Y is contained in $\mathrm{GL}_n(\mathcal{O}((t)))$.

c) If $D \in \mathrm{GL}_n(\mathfrak{o}[[t]])$ and if $Y \in \mathrm{GL}_n(\tilde{k}[[t]])$, then Y is contained in $\mathrm{GL}_n(\mathcal{O}[[t]])$.

Proof. We can write $D = \sum_{i=0}^{\infty} D_i t^i$ with

a): $D_0 \in \mathrm{GL}_n(k)$ and $D_i \in \mathrm{M}_n(k)$ for all $i > 0$

b), c): $D_0 \in \mathrm{GL}_n(\mathfrak{o})$ and $D_i \in \mathrm{M}_n(\mathfrak{o})$ for all $i > 0$.

and $Y = \sum_{i=l}^{\infty} Y_i t^i$ with

a), b): $l \in \mathbb{Z}$, all $Y_i \in \mathrm{M}_n(\tilde{k})$ and $Y_l \neq 0$.

c): $l = 0$, $Y_0 \in \mathrm{GL}_n(\tilde{k})$ and all $Y_i \in \mathrm{M}_n(\tilde{k})$ for $i > 0$.

Now Y is a fundamental matrix for M, hence $D\phi_q(Y) = Y$ holds, which implies

$$(D_0 + D_1 t + \dots)(Y_l^q t^l + Y_{l+1}^q t^{l+1} + \dots) = (Y_l t^l + Y_{l+1} t^{l+1} + \dots), \quad (3.7)$$

where Y_i^q denotes the coordinate-wise application of the ordinary Frobenius homomorphism.
Comparing the coefficients of the lowest term t^l in (3.7), we get

$$D_0 Y_l^q = Y_l.$$

We conclude that the entries of all columns of Y_l are separable algebraic over k by Lemma 3.3.2, hence $Y_l \in \mathrm{M}_n(\overline{k}^{\mathrm{sep}})$. In case b) and c), we moreover have $D_0 \in \mathrm{GL}_n(\mathfrak{o})$. Hence we have $Y_l^q = D_0^{-1} Y_l$ and it follows that $\mathfrak{o}[(Y_l)_{i,j} \mid 1 \leq i, j \leq n]$ is finitely generated as an $\mathfrak{o}$-module. Therefore, all entries of Y_l are integral over $\mathfrak{o}$ (see for Example [AM69, Prop. 5.1]). As they are also contained in $\overline{k}^{\mathrm{sep}}$, they are contained in the integral closure of $\mathfrak{o}$ inside $\overline{k}^{\mathrm{sep}}$, which is contained in $\mathcal{O}$. So all entries of Y_l are contained in $\mathcal{O}$, in these cases.
We can now use induction on i to see that Y_i has entries in $\overline{k}^{\mathrm{sep}}$ (and moreover in $\mathcal{O}$, in case b), c)) for all $i > l$. For an $i \geq l$, we evaluate the coefficients of t^{i+1} in (3.7) to get the following equation:

$$D_0 Y_{i+1}^q + D_1 Y_i^q + \dots + D_{i+1-l} Y_l^q = Y_{i+1}. \quad (3.8)$$

By induction hypothesis, $Y_l, \dots, Y_i$ have entries in $\overline{k}^{\mathrm{sep}}$ and so Lemma 3.3.2 (applied to $K_1 = \overline{k}^{\mathrm{sep}}$ and $A = -D_0$) implies $Y_{i+1} \in \mathrm{M}_n(\overline{k}^{\mathrm{sep}})$. Moreover, in case b) and c), $Y_l, \dots, Y_i$ have entries in $\mathcal{O}$ by induction and so we multiply Equation (3.8) by $D_0^{-1} \in \mathrm{GL}_n(\mathfrak{o}) \subseteq \mathrm{GL}_n(\mathcal{O})$ to get an equation of the form

$$Y_{i+1}^q = D_0^{-1} Y_{i+1} + \tilde{A}, \tag{3.9}$$

for $\tilde{A} = -D_0^{-1}(D_1 Y_i^q + \cdots + D_{i+1-l} Y_l^q) \in \mathrm{M}_n(\mathcal{O})$. As above, it follows that Y_{i+1} is contained in $\mathrm{M}_n(\mathcal{O})$. Altogether, we proved that Y is contained in $\mathrm{GL}_n(\overline{k}^{\mathrm{sep}}((t)))$ and moreover $Y \in \mathrm{GL}_n(\overline{k}^{\mathrm{sep}}((t))) \cap \mathrm{M}_n(\mathcal{O}((t)))$ in case b) and $Y \in \mathrm{GL}_n(\overline{k}^{\mathrm{sep}}[[t]]) \cap \mathrm{M}_n(\mathcal{O}[[t]])$ in case c).

For the cases b) and c), resp., it remains to show that $\det(Y) \in \mathcal{O}((t))^\times$ and $\det(Y) \in \mathcal{O}[[t]]^\times$, resp. We set $y = \det(Y)^{-1}$ and $d = \det(D)^{-1}$. Then the equality $Y = D\phi_q(Y)$ implies

$$y = d\phi_q(y).$$

The one-dimensional ϕ_q-difference module over $k(t)$ given by $d \in \mathrm{GL}_1(k(t))$ itself conforms to all assumptions of this Proposition. In fact, $d = \det(D)^{-1}$ is contained in $\mathfrak{o}[[t]]^\times = \mathrm{GL}_1(\mathfrak{o}[[t]])$ as D is contained in $\mathrm{GL}_n(\mathfrak{o}[[t]])$ and y is a fundamental matrix contained in $\tilde{k}((t))^\times = \mathrm{GL}_1(\tilde{k}((t)))$. In case c) we moreover have $y \in \tilde{k}[[t]]^\times = \mathrm{GL}_1(\tilde{k}[[t]])$, as Y is contained in $\mathrm{GL}_n(\tilde{k}[[t]]))$. By what we have proven above, we know that the fundamental matrix $y = \det(Y)^{-1}$ is contained in $\mathrm{M}_1(\mathcal{O}((t))) = \mathcal{O}((t))$ in case b) and $y = \det(Y)^{-1}$ is contained in $\mathrm{M}_1(\mathcal{O}[[t]]) = \mathcal{O}[[t]]$ in case c). Thus $\det(Y) = y^{-1}$ is invertible inside $\mathcal{O}((t))$ in case b) and $\det(Y) = y^{-1}$ is invertible inside $\mathcal{O}[[t]]$ in case c). □

Lemma 3.3.4. *The following holds:*

a) $\mathfrak{o}_t$ *and* $\mathcal{O}((t))$ *are* ϕ_q*-stable.*

b) $\mathfrak{o}_t \subseteq \mathrm{Quot}(\mathfrak{o}[t]) \subseteq \mathrm{Quot}(\mathcal{O}[[t]]) \subseteq \overline{k}^{\mathrm{sep}}((t))$.

c) $k(t) \cap \mathfrak{o}[[t]] \subseteq \mathfrak{o}_t$.

d) $\mathrm{GL}_n(k(t)) \cap \mathrm{GL}_n(\mathfrak{o}[[t]]) \subseteq \mathrm{GL}_n(\mathfrak{o}_t)$.

Proof. a) Since ϕ_q is just the ordinary Frobenius map on $\mathfrak{o} \subseteq k$, it follows that $\nu(\phi_q(a)) = q\nu(a)$ for all $a \in \mathfrak{o}$, and thus also $\nu_t(\phi_q(x)) = q\nu_t(x)$ for all $x \in \mathfrak{o}_t$. In particular, $\mathfrak{o}_t$ is stable under ϕ_q. Similarly $\mathcal{O}$ is ϕ_q-stable, so $\mathcal{O}((t))$ is also ϕ_q-stable, as ϕ_q acts coefficient-wise on $\mathcal{O}((t))$.

b) The valuation ring $\mathfrak{o}_t$ equals

$$\left\{ \frac{\sum_{i=0}^n a_i t^i}{\sum_{i=0}^m b_i t^i} \;\middle|\; a_i, b_i \in k : \; \min\{\nu(a_i) \mid i \le n\} \ge \min\{\nu(b_i) \mid i \le m\} \right\}.$$

Let $\frac{\sum_{i=0}^{n} a_i t^i}{\sum_{i=0}^{m} b_i t^i}$ be such an element. Let $j \leq m$ be such that $\nu(b_j)$ is minimal among $\nu(b_1), \ldots, \nu(b_m)$. Dividing both numerator and denominator by b_j, we obtain that $\mathfrak{o}_t$ equals

$$\left\{ \frac{\sum_{i=0}^{n} a_i t^i}{\sum_{i=0}^{m} b_i t^i} \;\middle|\; a_i, b_i \in \mathfrak{o} : \; \min\{\nu(a_i) \mid i \leq n\} \geq \min\{\nu(b_i) \mid i \leq m\} \right\}.$$

Thus $\mathfrak{o}_t \subseteq \mathrm{Quot}(\mathfrak{o}[t])$ and the other inclusions are immediate.

c) Now let $\frac{\sum_{i=0}^{n} a_i t^i}{\sum_{i=0}^{m} b_i t^i}$ be an element in $k(t) \cap \mathfrak{o}[[t]]$, i.e., there exist $\lambda_i \in \mathfrak{o}$ such that $\frac{\sum_{i=0}^{n} a_i t^i}{\sum_{i=0}^{m} b_i t^i} = \sum_{i=0}^{\infty} \lambda_i t^i$. Let $i \leq n$. Then $a_i = \lambda_i b_0 + \lambda_{i-1} b_1 + \cdots + \lambda_0 b_i$, where we set $b_j = 0$ for $j > m$. Since all λ_i are contained in $\mathfrak{o}$, we conclude that $\nu(a_i) \geq \min\{\nu(b_j) \mid 0 \leq j \leq i\} = \min\{\nu(b_j) \mid j \leq m\}$. Hence $\min\{\nu(a_i) \mid i \leq n\} \geq \min\{\nu(b_j) \mid j \leq m\}$ and so $\mathfrak{o}[[t]] \cap k(t) \subseteq \mathfrak{o}_t$ holds.

d) follows from the previous point, as $k(t) \cap \mathfrak{o}[[t]] \subseteq \mathfrak{o}_t$ implies $k(t)^\times \cap \mathfrak{o}[[t]]^\times \subseteq \mathfrak{o}_t^\times$.

□

Remark 3.3.5. *Note that $\mathfrak{o}_t$ is not contained in $\mathcal{O}((t))$. Indeed, $\frac{1}{a+t}$ is contained in $\mathfrak{o}_t$ but not in $\mathcal{O}((t))$, if $a \in \mathfrak{p} = \mathfrak{o} \backslash \mathfrak{o}^\times$.*

Definition 3.3.6. *From now on, we let $\mathcal{O}_t$ be the subring of $\overline{k}^{\mathrm{sep}}((t))$ generated by $\mathcal{O}((t)) \cup \mathfrak{o}_t$. Since both $\mathcal{O}((t))$ and $\mathfrak{o}_t$ are ϕ_q-stable inside $\overline{k}^{\mathrm{sep}}((t))$, $\mathcal{O}_t$ is ϕ_q-stable, as well. Also, note that $\mathbb{F}_q(t) \subseteq \mathcal{O}((t)) \subseteq \mathcal{O}_t$.*

Proposition 3.3.7. *There exists a homomorphism*

$$\kappa \colon \mathcal{O}_t \to \overline{\mathbb{F}}_q((t))$$

extending the residue class homomorphism $\kappa \colon \mathcal{O} \to \overline{\mathbb{F}}_q$ such that the following holds:

a) κ commutes with ϕ_q.

b) κ restricted to $\mathcal{O}((t))$ equals the coefficient-wise application of the residue map $\mathcal{O} \to \mathcal{O}/\mathcal{P} \cong \overline{\mathbb{F}}_q$ to a Laurent series over $\mathcal{O}$.

c) κ restricts to the residue map $\mathfrak{o}_t \to \mathfrak{o}_t/\mathfrak{p}_t \cong \mathbb{F}_{q^d}(t)$ on $\mathfrak{o}_t$.

d) κ induces specializations

- $\kappa(Y) \in \mathrm{GL}_n(\overline{\mathbb{F}}_q((t)))$ *of* $Y \in \mathrm{GL}_n(\mathcal{O}((t)))$
- $\kappa(Y) \in \mathrm{GL}_n(\overline{\mathbb{F}}_q[[t]])$ *of* $Y \in \mathrm{GL}_n(\mathcal{O}[[t]])$
- $\kappa(D) \in \mathrm{GL}_n(\mathbb{F}_{q^d}[t]_{(t)})$ *of* $D \in \mathrm{GL}_n(k(t) \cap \mathfrak{o}[[t]])$.

Proof. As the residue class homomorphism $\kappa\colon \mathcal{O} \to \overline{\mathbb{F}}_q$ is a homomorphism, it commutes with ϕ_q which is the ordinary Frobenius homomorphism on $\mathcal{O}$. We can extend κ to a ring homomorphism

$$\kappa\colon \mathcal{O}((t)) \to \overline{\mathbb{F}}_q((t))$$

by applying κ to the coefficients of the Laurent series over $\mathcal{O}$. Since ϕ_q acts on $\mathcal{O}$ coefficient-wise as well, we find that κ commutes with ϕ_q on $\mathcal{O}((t))$.

On $\mathfrak{o}_t$, we let $\tilde{\kappa}$ be the residue map $\mathfrak{o}_t \to \mathfrak{o}_t/\mathfrak{p}_t \cong \mathbb{F}_{q^d}(t)$ on $\mathfrak{o}_t$. We have seen in the proof of Lemma 3.3.4 that an element in $\mathfrak{o}_t$ can be written as $x = \frac{\sum_{i=0}^{n} a_i t^i}{\sum_{i=0}^{m} b_i t^i}$ for some $a_i, b_i \in \mathfrak{o}$ such that $\min\{\nu(a_i) \mid i \leq n\} \geq \min\{\nu(b_i) \mid i \leq m\}$. Now $\tilde{\kappa}|_{\mathfrak{o}} = \kappa|_{\mathfrak{o}}$ and thus

$$\tilde{\kappa}(x) = \frac{\sum_{i=0}^{n} \tilde{\kappa}(a_i) t^i}{\sum_{i=0}^{m} \tilde{\kappa}(b_i) t^i} = \frac{\sum_{i=0}^{n} \kappa(a_i) t^i}{\sum_{i=0}^{m} \kappa(b_i) t^i}, \tag{3.10}$$

and we conclude that $\tilde{\kappa}$ commutes with ϕ_q. It is also immediate from Equation (3.10), that κ and $\tilde{\kappa}$ agree on $\mathcal{O}((t)) \cap \mathfrak{o}_t$ and that we can glue κ and $\tilde{\kappa}$ to a homomorphism on $\mathcal{O}_t$ satisfying a),b) and c).

For the last part, note that κ restricts to $\mathfrak{o}[[t]] \to \mathbb{F}_{q^d}[[t]]$ and thus also to $\mathfrak{o}[[t]]^\times \to \mathbb{F}_{q^d}[[t]]^\times$. If $Y \in \mathrm{GL}_n(\mathcal{O}((t)))$ (or $Y \in \mathrm{GL}_n(\mathcal{O}[[t]])$) and $D \in \mathrm{GL}_n(\mathfrak{o}[[t]])$, we get well-defined matrices $\kappa(Y) \in \mathrm{GL}_n(\overline{\mathbb{F}}_q((t)))$ (or $\kappa(Y) \in \mathrm{GL}_n(\overline{\mathbb{F}}_q[[t]])$) and $\kappa(D) \in \mathrm{GL}_n(\mathbb{F}_{q^d}[[t]])$, by applying κ coordinate-wise. □

Remark 3.3.8. *In Section 3.1 we constructed fundamental matrices $Y \in \mathrm{GL}_n(L) \subseteq \mathrm{GL}_n(K((t)))$. If we set $\tilde{k} = K$, then $Y \in \mathrm{GL}_n(\tilde{k}((t)))$ and also $YC \in \mathrm{GL}_n(\tilde{k}((t)))$ for all $C \in \mathrm{GL}_n(\mathbb{F}_q(t))$ (C will be chosen such that YC is contained in a given group, see Chapter 3.2). If the corresponding difference module (M, Φ) is given by a representing matrix $D \in \mathrm{GL}_n(k(t) \cap \mathfrak{o}[[t]])$, we can thus apply Proposition 3.3.3 and 3.3.7 to specialize YC.*

3.3.3 A Lower Bound Theorem

The Chevalley Theorem 3.2.1 has played an important role in solving the inverse problem in differential Galois theory (with algebraically closed constants). It has been used in characteristic zero (see [MS96]) as well as in the iterative differential case (see [Mat01]).
We will apply Theorem 3.2.1 to difference Galois group schemes $\mathcal{H}$ and get the following lemma as a consequence for the module structure:

Lemma 3.3.9. *Let (M, Φ) be an m-dimensional difference module over a difference field (F, ϕ), with Picard-Vessiot extension E, fundamental matrix*

$Y \in \mathrm{GL}_m(E)$ and Galois group scheme $\mathcal{H} \leq \mathrm{GL}_m$. Suppose that there exists a $0 \neq w \in C_F^m$ that spans an $\mathcal{H}$-stable line, i.e., for any C_F-algebra S, we have $\mathcal{H}(S) \cdot w \subseteq S \cdot w$. Then there exists an $\alpha \in E^\times$ such that $v := \alpha Y \cdot w \in F^m \cong M$ and $N := F \cdot v$ defines a Φ-stable submodule of M.

Proof. Note that M has been identified with F^m by fixing a basis.
Let $y_1, \ldots, y_m \in E^m$ be the columns of Y. Then $\mathrm{Sol}_E^\Phi(M)$ is spanned by $y_1, \ldots, y_m$ as a C_F-vector space and $Y \cdot w$ is contained in $\mathrm{Sol}_E^\Phi(M) \leq E^m$. We fix an $i \leq m$ such that the i-th coordinate of $Y \cdot w$ is non-zero and we set $\alpha = (Y \cdot w)_i^{-1} \in E^\times$. We first show that $v := \alpha Y \cdot w$ is contained in F^m. Let $R = F[Y, Y^{-1}] \subseteq E$ be the Picard-Vessiot ring inside E (see Theorem 1.2.11). Let S be any C_F-algebra and let σ be an element in $\mathrm{Aut}^\phi(R \otimes_{C_F} S, F \otimes_{C_F} S)$. We have $\mathcal{H}(S) \cdot w \subseteq S \cdot w$, hence there exists a $\lambda_\sigma \in S$ such that $Y^{-1}\sigma(Y) \cdot w = \lambda_\sigma w$, by Proposition 1.3.11. For any $j \leq m$, $(Y \cdot w)_j$ is contained in $R \subseteq R \otimes_{C_F} S$ and we have $\sigma((Y \cdot w)_j) = (\sigma(Y)w)_j = \lambda_\sigma \cdot (Y \cdot w)_j$. Therefore,

$$\sigma((Yw)_j)(Yw)_i = \lambda_\sigma (Yw)_j (Yw)_i = (Yw)_j \sigma((Yw)_i)$$

holds for all $j \leq m$. The j-th coordinate of v equals $v_j = \frac{(Yw)_j}{(Yw)_i}$, so Proposition 1.3.13 implies that v_j is contained in F.
To see that $\Phi(N) \subseteq N$ holds, recall that Yw is a solution. Thus $\Phi(Yw) = Yw$ holds, where $D \in \mathrm{GL}_m(F)$ denotes the representing matrix of M. Hence $\Phi(v) = \phi(\alpha)\Phi(Yw) = \phi(\alpha)\alpha^{-1}v$. Now $\phi(\alpha)\alpha^{-1} = \frac{(Yw)_i}{\phi((Yw)_i)}$ and another application of Proposition 1.3.11 yields that $\phi(\alpha)\alpha^{-1}$ is contained in F, hence $\Phi(v)$ is contained in $Fv = N$. □

For difference modules over (k, ϕ_q) (so-called finite Frobenius modules) there exists a lower bound criterion due to Matzat (see Theorem 4.5. in [Mat04]), leading to finite Galois extensions over k. This criterion asserts that conjugates of specializations of certain twists of the representing matrix are contained in the Galois group. The following theorem generalizes this criterion to difference modules over $(k(t), \phi_q)$.

Theorem 3.3.10. *Let $\mathcal{G} \leq \mathrm{GL}_n$ be a linear algebraic group defined over $\mathbb{F}_q(t)$. Let (M, Φ) be an n-dimensional ϕ_q-module over $k(t)$ with representing matrix $D \in \mathcal{G}(k(t) \cap \mathfrak{o}[[t]])$ and let $\tilde{k}$ be a field containing $\overline{k}^{\mathrm{sep}}$. Assume that there exists a fundamental matrix $Y \in \mathcal{G}(\tilde{k}((t)))$ for M generating a separable Picard-Vessiot extension $E/k(t)$ of M. Let $\mathcal{H} \leq \mathcal{G}$ be the Galois group-scheme of M corresponding to the Picard-Vessiot ring $R := k(t)[Y, Y^{-1}] \subseteq E$ (see Theorem 1.2.11). Then $\mathcal{H}(\mathbb{F}_q((t)))$ contains a $\mathcal{G}(\overline{\mathbb{F}}_q((t)))$-conjugate of $\kappa(D\phi_q(D) \ldots \phi_{q^{d-1}}(D))$.*
(More precisely, the conjugating matrix can be chosen as $\kappa(Y) \in \mathcal{G}(\overline{\mathbb{F}}_q((t)))$).

Proof. We abbreviate $F := k(t)$ throughout this proof.
First of all, note that Y is actually contained in $\mathcal{G}(\overline{k}^{\mathrm{sep}}((t)))$, by Proposition

3.3.3, hence the Picard-Vessiot extension E, which is generated over F by the entries of Y, is contained in $\overline{k}^{\mathrm{sep}}((t))$.

By Theorem 1.3.10, $\mathcal{H}$ is a linear algebraic group and it is a subgroup of $\mathcal{G}$ by Proposition 1.3.11. We apply Theorem 3.2.1 to $\mathcal{G}$ and get a closed embedding

$$\rho\colon \mathcal{G} \to \mathrm{GL}_m$$

defined over $\mathbb{F}_q(t)$ and a non-zero $w \in \mathbb{F}_q(t)^m$ such that $\mathcal{H}(\overline{\mathbb{F}_q(t)}) = \{g \in \mathcal{G}(\overline{\mathbb{F}_q(t)}) \mid \rho(g)w \in \overline{\mathbb{F}_q(t)} \cdot w\}$ holds. The stabilizer of the line spanned by w defines a closed subvariety of $\mathcal{G}$ defined over $\mathbb{F}_q(t)$ and it follows that

$$\mathcal{H}(S) = \{g \in \mathcal{G}(S) \mid \rho(g)w \in S \cdot w\} \tag{3.11}$$

also holds for all $\mathbb{F}_q(t)$-algebras S. We now blow up M to an m-dimensional version $\tilde{M}$ in order to be able to apply Lemma 3.3.9. Let $\tilde{M}$ be an m-dimensional difference module over F such that its representing matrix with respect to a fixed basis is given by $\rho(D) \in \mathrm{GL}_m(F)$. Then $\tilde{Y} := \rho(Y)$ is a fundamental solution matrix for $\tilde{M}$, since ρ is defined over $\mathbb{F}_q(t)$ and thus $\phi_q(\rho(Y)) = \rho(\phi_q(Y))$. All entries of $\tilde{Y}$ are contained in R and furthermore, the entries of Y are contained in $F[\tilde{Y}, \tilde{Y}^{-1}]$, since ρ is a closed embedding defined over $\mathbb{F}_q(t) \subseteq F$. Hence $R = F[\tilde{Y}, \tilde{Y}^{-1}]$ is also Picard-Vessiot ring for $\tilde{M}$ and the Galois group scheme $\mathcal{G}_{\tilde{M},R}$ is $\rho(\mathcal{H}) \leq \mathrm{GL}_m$ in its natural representation as given in Proposition 1.3.11. By construction, w spans a $\mathcal{G}_{\tilde{M},R}$-stable line (see Equation (3.11)) and thus there exists an $\alpha \in E^\times$ such that

$$v = \alpha \tilde{Y} w \tag{3.12}$$

is contained in F^m and $N = Fv$ is a Φ-submodule of $\tilde{M}$, by Lemma 3.3.9. This means that there exists a $\lambda \in F$ such that $\rho(D)\phi_q(v) = \lambda v$.
The third part of Lemma 3.3.4 asserts that D is contained in $\mathrm{GL}_n(\mathfrak{o}_t)$. Since ρ is defined over $\mathbb{F}_q(t) \subseteq \mathfrak{o}_t$, $\rho(D)$ and $\rho(D^{-1})$ both have coefficients in $\mathfrak{o}_t$ and thus $\rho(D)$ is contained in $\mathrm{GL}_m(\mathfrak{o}_t)$.
Now fix an $i \leq m$ such that the i-th coordinate v_i of v has minimal valuation among all coordinates of v (with respect to ν_t and the order on Γ). Recall that $v \neq 0$, thus $v_i \neq 0$ and we can define $v' = \frac{1}{v_i} v$. Then $v' = (v'_1, \ldots, v'_m)$ is contained in $\mathfrak{o}_t^m$ with $v'_i = 1$. Note that $\rho(D) \cdot \phi_q(v') = \phi_q(v_i)^{-1} v_i \lambda v'$, so we define $\lambda' = \phi_q(v_i)^{-1} v_i \lambda \in F$ and we get

$$\rho(D)\phi_q(v') = \lambda' v'. \tag{3.13}$$

Thus $\lambda' = \lambda' \cdot v'_i = (\rho(D)\phi_q(v'))_i$ is contained in $\mathfrak{o}_t$ since $\mathfrak{o}_t$ is ϕ_q-stable (see Lemma 3.3.4). Also, $(\lambda')^{-1} = (\lambda')^{-1}\phi_q(v')_i = (\rho(D^{-1})v')_i$ is contained in $\mathfrak{o}_t$, so λ' is in fact contained in $\mathfrak{o}_t^\times$. Overall, we got $\rho(D) \in \mathrm{GL}_m(\mathfrak{o}_t)$, $v' \in \mathfrak{o}_t^m$ and $\lambda' \in \mathfrak{o}_t^\times$, hence we may specialize them to $\kappa(\rho(D)) \in \mathrm{GL}_m(\mathbb{F}_{q^d}(t))$,

$\kappa(v') \in \mathbb{F}_{q^d}(t)^m$ and $\kappa(\lambda') \in \mathbb{F}_{q^d}(t)^\times$, by Proposition 3.3.7. We apply κ to both sides of Equation (3.13) coordinate-wise:

$$\kappa(\rho(D))\kappa(\phi_q(v')) = \kappa(\lambda')\kappa(v'). \tag{3.14}$$

We denote from now on the (coordinate-wise) application of κ to a matrix A with entries in $\mathcal{O}_t$ by $\overline{A}$ and similarly for vectors with entries in $\mathcal{O}_t$ and scalars in $\mathcal{O}_t$. Hence Equation (3.14) translates to

$$\overline{\rho(D)}\phi_q(\overline{v'}) = \overline{\lambda'} \cdot \overline{v'}, \tag{3.15}$$

where we used that κ and ϕ_q commute (see Proposition 3.3.7) to get $\overline{\phi_q(v')} = \phi_q(\overline{v'})$. Note that ρ commutes with the coordinate-wise application of κ to an element in $\mathcal{G}(\mathcal{O}_t)$, since ρ is defined over $\mathbb{F}_q(t)$ and κ restricts to the identity on $\mathbb{F}_q(t)$. In particular, $\overline{\rho(D)} = \rho(\overline{D})$ holds and we get

$$\rho(\overline{D}) \cdot \phi_q(\overline{v'}) = \overline{\lambda'} \cdot \overline{v'}.$$

Inductively, we get

$$\rho(\overline{D})\phi_q(\rho(\overline{D})) \cdots \phi_{d-1}(\rho(\overline{D})) \cdot \overline{v'} = \overline{\lambda'}\phi_q(\overline{\lambda'}) \cdots \phi_{q^{d-1}}(\overline{\lambda'}) \cdot \overline{v'}, \tag{3.16}$$

where we used $\phi_{q^d}(\overline{v'}) = \overline{v'}$. We set $\mu = \frac{\alpha}{v_i} \in E \subseteq \overline{k}^{\mathrm{sep}}((t))$ and get

$$v' = \mu \cdot \rho(Y) \cdot w \tag{3.17}$$

(see Equation (3.12)). Proposition 3.3.3 implies that Y has entries in $\mathcal{O}((t))$, hence $\rho(Y)$ is contained in $\mathrm{GL}_m(\mathcal{O}((t))) \subseteq \mathrm{GL}_m(\mathcal{O}_t)$, as ρ is defined over $\mathbb{F}_q(t) \subseteq \mathcal{O}((t))$. Recall that $v' \in \mathfrak{o}_t^m \subseteq \mathcal{O}_t^m$, $v'_i = 1$ and $0 \neq w \in \mathbb{F}_q(t)^m$ holds, hence there exists a $j \leq m$ such that $w_j \in \mathbb{F}_q(t)^\times \subseteq \mathcal{O}_t^\times$. Then Equation (3.17) implies

$$1 = v'_i = \mu \cdot (\rho(Y) \cdot w)_i$$

and

$$(\rho(Y)^{-1} \cdot v')_j = \mu \cdot w_j$$

and we deduce that μ is contained in $\mathcal{O}_t^\times$. It can thus be specialized to an element $\overline{\mu} = \kappa(\mu) \in \overline{\mathbb{F}}_q((t))^\times$. We may apply κ to both sides of Equation (3.17) to get

$$\overline{v'} = \overline{\mu} \cdot \overline{\rho(Y)} \cdot \overline{w} = \overline{\mu} \cdot \rho(\overline{Y}) \cdot w. \tag{3.18}$$

(Note that at this point we applied κ simultaneously to elements in $\mathcal{O}((t))$ and $\mathfrak{o}_t$ which is why we had to construct κ on the somewhat peculiar ring $\mathcal{O}_t$ in Proposition 3.3.7.)

Abbreviate $\hat{D} = D\phi_q(D) \cdots \phi_{q^{d-1}}(D)$ and $\hat{\lambda}' = \lambda'\phi_q(\lambda') \cdots \phi_{q^{d-1}}(\lambda')$. Then Equation (3.16) translates to

$$\rho(\overline{\hat{D}})\overline{v'} = \overline{\hat{\lambda}'}\overline{v'}. \tag{3.19}$$

We now consider $\overline{Y}^{-1} \cdot \overline{\hat{D}} \cdot \overline{Y} = \kappa(Y^{-1}\hat{D}Y)$ which is contained in $\mathcal{G}(\overline{\mathbb{F}}_q((t)))$, since $\mathcal{G}$ is defined over $\mathbb{F}_q(t)$ and κ acts trivially on $\mathbb{F}_q(t)$. We use Equation (3.18) and (3.19) to compute

$$\begin{aligned}\rho(\overline{Y}^{-1} \cdot \overline{\hat{D}} \cdot \overline{Y}) \cdot w &= \rho(\overline{Y^{-1}})\rho(\overline{\hat{D}})\rho(\overline{Y})w \\ &= \overline{\mu}^{-1}\rho(\overline{Y}^{-1})\rho(\overline{\hat{D}})\overline{v'} \\ &= \overline{\mu}^{-1}\overline{\hat{\lambda}'}\rho(\overline{Y}^{-1})\overline{v'} \\ &= \overline{\hat{\lambda}'} \cdot w.\end{aligned}$$

It follows that $\overline{Y}^{-1} \cdot \overline{\hat{D}} \cdot \overline{Y}$ is contained in $\mathcal{H}(\overline{\mathbb{F}}_q((t)))$ (see (3.11)). It remains to show that $\overline{Y}^{-1} \cdot \overline{\hat{D}} \cdot \overline{Y}$ has entries in $\mathbb{F}_q((t))$. To see this, recall that $D\phi_q(Y) = Y$ holds, hence $\overline{D}\phi_q(\overline{Y}) = \overline{Y}$ and $\phi_q(\overline{Y})^{-1} = \overline{Y}^{-1} \cdot \overline{D}$. We compute

$$\begin{aligned}\phi_q(\overline{Y}^{-1}\overline{\hat{D}}\overline{Y}) &= \phi_q(\overline{Y}^{-1})\phi_q(\overline{D}) \cdots \phi_{q^d}(\overline{D})\phi_q(\overline{Y}) \\ &= \phi_q(\overline{Y}^{-1})\phi_q(\overline{D}) \cdots \phi_{q^{d-1}}(\overline{D})\overline{D}\phi_q(\overline{Y}) \\ &= \overline{Y}^{-1}\overline{D}\phi_q(\overline{D}) \cdots \phi_{q^{d-1}}(\overline{D})\overline{Y} \\ &= \overline{Y}^{-1} \cdot \overline{\hat{D}} \cdot \overline{Y},\end{aligned}$$

where we used that $\overline{D} \in \mathrm{GL}_n(\mathbb{F}_{q^d}(t))$. Hence $\overline{Y}^{-1} \cdot \overline{\hat{D}} \cdot \overline{Y}$ has entries in $\overline{\mathbb{F}}_q((t))^{\phi_q} = \mathbb{F}_q((t))$. □

We immediately get the following power series version of Theorem 3.3.10 under the further assumption that Y is contained in $\mathcal{G}(\tilde{k}[[t]])$.

Corollary 3.3.11. *Let $\mathcal{G} \leq \mathrm{GL}_n$ be a linear algebraic group defined over $\mathbb{F}_q(t)$. Let (M, Φ) be an n-dimensional ϕ_q-module over $k(t)$ with representing matrix $D \in \mathcal{G}(k(t) \cap \mathfrak{o}[[t]])$ and let $\tilde{k}$ be a field containing $\overline{k}^{\mathrm{sep}}$. Assume that there exists a fundamental matrix $Y \in \mathcal{G}(\tilde{k}[[t]])$ for M generating a separable Picard-Vessiot extension $E/k(t)$ of M. Let $\mathcal{H} \leq \mathcal{G}$ be the Galois group-scheme of M corresponding to the Picard-Vessiot ring $R := k(t)[Y, Y^{-1}] \subseteq E$. Then $\mathcal{H}(\mathbb{F}_q[[t]])$ contains a $\mathcal{G}(\overline{\mathbb{F}}_q[[t]])$-conjugate of $\kappa(D\phi_q(D) \dots \phi_{q^{d-1}}(D))$.*
(More precisely, the conjugating matrix inside $\mathcal{G}(\overline{\mathbb{F}}_q[[t]])$ can be chosen as $\kappa(Y)$.)

Proof. It follows from the third part of Proposition 3.3.7 (together with Proposition 3.3.3) that $\overline{Y} = \kappa(Y)$ is contained in $\mathrm{GL}_n(\overline{\mathbb{F}}_q[[t]])$. On the other hand, $\overline{Y}$ is still contained in $\mathcal{G}$, since $\mathcal{G}$ is defined over $\mathbb{F}_q(t)$. Hence $\overline{Y}$ is contained in $\mathcal{G}(\overline{\mathbb{F}}_q[[t]])$. Also, D is contained in $\mathrm{GL}_n(\mathfrak{o}[[t]])$, hence $\overline{D} = \kappa(D)$ is contained in $\mathrm{GL}_n(\mathbb{F}_{q^d}[[t]])$ and we just proved in Theorem 3.3.10 that $\mathcal{H}(\mathbb{F}_q((t)))$ contains $\overline{Y}^{-1} \cdot \overline{\hat{D}} \cdot \overline{Y}$, which has entries in $\mathbb{F}_q((t)) \cap \overline{\mathbb{F}}_q[[t]] = \mathbb{F}_q[[t]]$ and is a $\mathcal{G}(\overline{\mathbb{F}}_q[[t]])$ conjugate of $\overline{\hat{D}} = \kappa(D\phi_q(D) \dots \phi_{q^{d-1}}(D))$. □

Example 3.3.12. *If $k = \mathbb{F}_q(s)$ and $\mathfrak{p} = (s - \alpha)$ is a finite place of degree 1 ($\alpha \in \mathbb{F}_q$), then the Galois group scheme $\mathcal{H}$ contains a conjugate of the specialized matrix D_α obtained by replacing each s by α.*

Chapter 4

Generating Reductive Groups

Using the lower bound criterion Corollary 3.3.11, we obtain elements contained in the Galois group up to conjugacy over $\overline{\mathbb{F}}_q[[t]]$. Therefore, we need to find generators such that any conjugates thereof still generate the given group $\mathcal{G}$ that we would like to realize as difference Galois group. For the classical groups, we make use of known results on generators of the finite parts $\mathcal{G}(\mathbb{F}_q)$ due to Malle, Saxl and Weigel ([MSW94]).

4.1 Finite Groups of Lie Type

We start with some basic facts on maximal tori in the finite parts of a linear algebraic group. Let $\mathcal{G}$ be a linear algebraic group defined over a finite field $\mathbb{F}_q$. Then $\mathcal{G}(\mathbb{F}_q)$ is a so-called *finite group of Lie type*. Let further T be a maximal torus of $\mathcal{G}$ that is defined over $\mathbb{F}_q$. Then $T(\mathbb{F}_q)$ is called a *maximal torus* of $\mathcal{G}(\mathbb{F}_q)$. Two maximal tori $T(\mathbb{F}_q)$ and $T_0(\mathbb{F}_q)$ in $\mathcal{G}(\mathbb{F}_q)$ are usually not conjugate but we can use the fact that T and T_0 are conjugate over $\mathcal{G}(\overline{\mathbb{F}}_q)$ to identify $T(\mathbb{F}_q)$ with some subgroup of $T_0(\overline{\mathbb{F}}_q)$. We think of T_0 as a fixed, well known maximal torus such as the diagonal torus in GL_n.

Proposition 4.1.1. *Let $\mathcal{G}$ be a linear algebraic group defined over $\mathbb{F}_q$ and let T_0 be a fixed maximal torus defined over $\mathbb{F}_q$. Then a maximal torus $T = T_0^g$ for a $g \in \mathcal{G}(\overline{\mathbb{F}}_q)$ is defined over $\mathbb{F}_q$ if and only if $w := g\phi_q(g)^{-1}$ is contained in the normalizer $\mathcal{N}_{\mathcal{G}}(T_0)$ of T_0. In this case, we have*

$$T(\mathbb{F}_q) = \{t_0 \in T_0(\overline{\mathbb{F}}_q) \mid \phi_q(t_0) = t_0^w\}^g.$$

Proof. All of this is well known. However, for the convenience of the reader, we state the proof:
As g is contained in $\mathcal{G}(\overline{\mathbb{F}}_q)$ and $\mathbb{F}_q$ is perfect, T is defined over the separable

closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$. Let Γ be the absolute Galois group of $\overline{\mathbb{F}}_q/\mathbb{F}_q$. Then T is defined over $\mathbb{F}_q$ if and only if $T(\overline{\mathbb{F}}_q)$ is Γ-stable (see [Bor91, AG.14.4]). Since Γ is generated by the Frobenius automorphism ϕ_q, we know that T is defined over $\mathbb{F}_q$ if and only if $\phi_q(T(\overline{\mathbb{F}}_q)) = T(\overline{\mathbb{F}}_q)$ holds. Now $\phi_q(T(\overline{\mathbb{F}}_q)) = \phi_q(T_0(\overline{\mathbb{F}}_q))^{\phi_q(g)}$ and $\phi_q(T_0(\overline{\mathbb{F}}_q)) = T_0(\overline{\mathbb{F}}_q)$, as T_0 is defined over $\mathbb{F}_q$. We conclude that T is defined over $\mathbb{F}_q$ if and only if

$$T_0(\overline{\mathbb{F}}_q)^{\phi_q(g)} = T_0(\overline{\mathbb{F}}_q)^g$$

holds which is the case if and only if $w = g\phi_q(g)^{-1}$ normalizes T_0. For the second part of the statement, we compute

$$\begin{aligned} T(\mathbb{F}_q) &= \{t_0^g \mid t_0 \in T_0(\overline{\mathbb{F}}_q),\ \phi_q(t_0^g) = t_0^g\} \\ &= \{t_0^g \mid t_0 \in T_0(\overline{\mathbb{F}}_q),\ \phi_q(t_0) = t_0^{g\phi_q(g^{-1})}\} \\ &= \{t_0 \in T_0(\overline{\mathbb{F}}_q) \mid \phi_q(t_0) = t_0^w\}^g. \end{aligned}$$

□

Example 4.1.2. *Let $\mathcal{G} = \mathrm{SL}_2$ and let T_0 be the diagonal torus. Set*

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

The Lang-isogeny (see [Bor91, V.16.4]) assures that there exists a $g \in \mathcal{G}(\overline{\mathbb{F}}_q)$ such that $g\phi_q(g)^{-1} = w$ holds. As w normalizes T_0, we have that $T = T_0^g$ is defined over $\mathbb{F}_q$. Let $t_0 = \mathrm{diag}(\lambda, \lambda^{-1})$ be an element in $T_0(\overline{\mathbb{F}}_q)$. Then t_0^g is contained in $T(\mathbb{F}_q)$ if and only if

$$\mathrm{diag}(\lambda^q, \lambda^{-q}) = \phi_q(t_0) = t_0^w = \mathrm{diag}(\lambda^{-1}, \lambda)$$

holds, that is, if and only if λ is a $(q+1)$-th root of unity. We conclude that $T(\mathbb{F}_q)$ is cyclic of order $q+1$, generated by $(\mathrm{diag}(\zeta, \zeta^{-1}))^g$ for a primitive $(q+1)$-th root of unity $\zeta \in \mathbb{F}_{q^2}$.

A semisimple element g in a linear algebraic group $\mathcal{G}$ of rank r is called *regular* if its centralizer is of minimal dimension (that is, of dimension r). This means that the connected component of the centralizer consists only of the maximal torus that g is contained in (which in this case is unique).

$\mathcal{G}$	$n_1(q)$	$n_2(q)$
SL_n	$\frac{q^n-1}{q-1}$	$q^{n-1}-1$
Sp_{2d}	q^d+1	q^d-1
SO_{2d+1}	q^d+1	q^d-1
SO_{2d}, d odd	$(q^{d-1}+1)(q+1)$	q^d-1
SO_{2d}, d even	$(q^{d-1}+1)(q+1)$	$(q^{d/2}+(-1)^{d/2})^2$

Table 4.1: Definition of $n_1(q)$ and $n_2(q)$

In [MSW94] it is shown that any finite group of Lie type can be generated by any two regular elements that are contained in maximal tori of prescribed order. As the order is invariant under conjugation over $\mathcal{G}(\mathbb{F}_q)$, any $\mathcal{G}(\mathbb{F}_q)$-conjugates of these elements still generate $\mathcal{G}(\mathbb{F}_q)$. For the groups that are of interest to us, we collect these prescribed orders $n_i(q)$ in Table 4.1.

Theorem 4.1.3 (Malle, Saxl, Weigel)**.** *Let $\mathcal{G}$ be one of the following groups*

- SL_n, $n \geq 3$
- Sp_{2d}, $d \geq 2$ *such that* $(d, q) \neq (2, 2)$
- SO_n, $n \geq 7$

and assume that T_1 and T_2 are maximal tori of $\mathcal{G}$ defined over $\mathbb{F}_q$ such that $|T_i(\mathbb{F}_q)| = n_i(q)$ holds for $i = 1, 2$, where n_i is as defined above. Then for any elements $A_1, A_2 \in \mathcal{G}(\mathbb{F}_q)$ we have

$$< T_1(\mathbb{F}_q)^{A_1}, T_2(\mathbb{F}_q)^{A_2} >= \mathcal{G}(\mathbb{F}_q).$$

Proof. In [MSW94], the authors prove that any finite group of Lie type can be generated by three involutions. In the course of the proof, they show that for any two regular elements x_1 and x_2 contained in $T_1(\mathbb{F}_q)$ and $T_2(\mathbb{F}_q)$, resp., the conjugates $x_1^{A_1}$ and $x_2^{A_2}$ generate $\mathcal{G}(\mathbb{F}_q)$. This clearly implies that $T_1(\mathbb{F}_q)^{A_1}$ and $T_2(\mathbb{F}_q)^{A_2}$ generate $\mathcal{G}(\mathbb{F}_q)$, as $T_1(\mathbb{F}_q)$ and $T_2(\mathbb{F}_q)$ always contain regular elements. (See Proposition 4.1.8 and its proof for explicit regular elements $x_1 \in T_1(\mathbb{F}_q)$ and $x_2 \in T_2(\mathbb{F}_q)$.)

We now give further instructions on how to find the desired results in [MSW94]. Starting on page 96, the authors treat each group separately. To be precise, for $\mathcal{G} = \mathrm{SL}_n$ and $\mathcal{G} = \mathrm{Sp}_{2d}$ they prove the statement for the simple counterpart $\overline{\mathcal{G}} = \mathcal{G}/Z(\mathcal{G})$ of $\mathcal{G}$ with maximal tori $\overline{T_1} = T_1/Z(\mathcal{G})$ and $\overline{T_2} = T_2/Z(G)$. But as $Z(\mathcal{G})$ is contained in $T_1(\mathbb{F}_q)^{A_1}$, this implies that $< T_1(\mathbb{F}_q)^{A_1}, T_2(\mathbb{F}_q)^{A_2} >= \mathcal{G}(\mathbb{F}_q)$. Now for $\mathcal{G} = \mathrm{SO}_n$, they consider the commutator subgroups $\mathcal{G}(\mathbb{F}_q)'$ with maximal tori $T_i(\mathbb{F}_q)' := T_i(\mathbb{F}_q) \cap \mathcal{G}(\mathbb{F}_q)'$. Then they prove the statement for the simple counterpart of $\mathcal{G}(\mathbb{F}_q)'$ which in turn implies that any $\mathcal{G}(\mathbb{F}_q)'$-conjugates of $T_1(\mathbb{F}_q)'$ and $T_2(\mathbb{F}_q)'$ generate $\mathcal{G}(\mathbb{F}_q)'$. As $\mathcal{G}(\mathbb{F}_q)'$ is normal in $\mathcal{G}(\mathbb{F}_q)$, this is in fact also true for any $\mathcal{G}(\mathbb{F}_q)$-conjugate of $T_1(\mathbb{F}_q)'$ and $T_2(\mathbb{F}_q)'$ (as these are maximal tori contained in $\mathcal{G}(\mathbb{F}_q)'$ of the same order). It follows that $< T_1(\mathbb{F}_q)^{A_1}, T_2(\mathbb{F}_q)^{A_2} >$ contains $\mathcal{G}(\mathbb{F}_q)'$ which is a normal subgroup of $\mathcal{G}(\mathbb{F}_q)$ of index at most two. It is therefore sufficient to show that $< T_1(\mathbb{F}_q)^{A_1}, T_2(\mathbb{F}_q)^{A_2} >$ is bigger than $\mathcal{G}(\mathbb{F}_q)'$ if $\mathcal{G}(\mathbb{F}_q) \neq \mathcal{G}(\mathbb{F}_q)'$. Assume that $< T_1(\mathbb{F}_q)^{A_1}, T_2(\mathbb{F}_q)^{A_2} >= \mathcal{G}(\mathbb{F}_q)' \subsetneq \mathcal{G}(\mathbb{F}_q)$ holds. This implies $T_1(\mathbb{F}_q) = T_1(\mathbb{F}_q)'$ which can not be the case by Table I in [MSW94]. □

Remark 4.1.4. *Note that the Dynkin diagram of* SO_5 *(type B_2) is the same as that of* Sp_4 *(type C_2) and that of* SO_6 *(type D_3) is the same as that of*

SL_4 *(type* A_3*). Therefore, the restriction* $n \geq 7$ *for* SO_n *is not essential. The group* SL_2 *will be treated separately in Chapter 5.4.*

Before we can construct the maximal tori of order $n_1(q)$ and $n_2(q)$ we need to examine the normalizer of the fixed maximal torus T_0 of $\mathcal{G} \in \{\mathrm{SL}_n, \mathrm{Sp}_{2d}, \mathrm{SO}_n\}$. For these groups, we let T_0 be the torus consisting of the diagonal matrices contained in $\mathcal{G}$. It is well known that its normalizer is the group of all monomial matrices that are contained in $\mathcal{G}$.

Lemma 4.1.5. *Let* $\sigma \in S_n$ *be a permutation.*

a) Let $n = 2d$ *be even and* $\mathcal{G} = \mathrm{Sp}_{2d}$*. Then there exists a monomial matrix* $A = (A_{ij}) \in \mathcal{G}(\mathbb{F}_q)$ *corresponding to* σ *(i.e.,* A_{ij} *is non-zero iff* $i = \sigma(j)$*) if and only if*

$$\sigma(n+1-i) = n+1-\sigma(i)$$

holds for all $i \leq n$*.*

b) Let $n = 2d+1$ *be odd and* $\mathcal{G} = \mathrm{SO}_{2d+1}$*. Then there exists a monomial matrix* $A \in \mathcal{G}(\mathbb{F}_q)$ *corresponding to* σ *if and only if*

$$\sigma(n+1-i) = n+1-\sigma(i)$$

holds for all $i \leq n$*.*

c) Let $n = 2d$ *be even and* $\mathcal{G} = \mathrm{SO}_{2d}$*. Then there exists a monomial matrix* $A \in \mathcal{G}(\mathbb{F}_q)$ *corresponding to* σ *if and only if the sign of* σ *equals one and*

$$\sigma(n+1-i) = n+1-\sigma(i)$$

holds for all $i \leq n$*.*

Proof. In all three cases, let $\tau = (1,n)(2,n-2)\cdots(d,n-d)$. Recall that the matrices J defining the symplectic and orthogonal forms were chosen monomial with corresponding permutation τ. If A is monomial with corresponding permutation σ and $A^{\mathrm{tr}}JA = J$ then $\sigma^{-1}\tau\sigma = \tau$. We conclude that $\sigma(n+1-i) = \sigma(\tau(i)) = \tau(\sigma(i)) = n+1-\sigma(i)$ for all $1 \leq i \leq n$ is a necessary condition.

a) Let $\sigma \in S_n$ be a permutation such that $\sigma(n+1-i) = n+1-\sigma(i)$ for all $i \leq n$ and let $B \in \mathrm{GL}_n(\mathbb{F}_q)$ be the permutation matrix corresponding to σ, i.e., $B_{ij} = \delta_{\sigma(j),i}$ for $1 \leq i,j \leq 2d$. We set $A = B \cdot \mathrm{diag}(x_1, \ldots, x_n)$, where we will later specify $x_i = \pm 1$ in such a way that A becomes symplectic. Recall that $J_{ij} = -\delta_{2d+1-i,j}$ for $1 \leq i \leq d$ and $J_{ij} = \delta_{2d+1-i,j}$ for $d+1 \leq i \leq 2d$. Hence $(JA)_{ij} = -A_{2d+1-i,j} =$

$-x_j\delta_{\sigma(2d+1-j),i}$ if $i \leq d$ and $(JA)_{ij} = x_j\delta_{\sigma(2d+1-j),i}$, otherwise. We compute

$$\begin{aligned}(A^{\mathrm{tr}}JA)_{ij} &= (A^{\mathrm{tr}})_{i,\sigma(i)}(JA)_{\sigma(i),j} = A_{\sigma(i),i}(JA)_{\sigma(i),j} \\ &= \begin{cases} -x_ix_j\delta_{\sigma(2d+1-j),\sigma(i)}, & \text{if } \sigma(i) \leq d \\ x_ix_j\delta_{\sigma(2d+1-j),\sigma(i)}, & \text{if } \sigma(i) \geq d+1 \end{cases} \\ &= \begin{cases} -x_ix_{2d+1-i}, & \text{if } \sigma(i) \leq d,\ j = 2d+1-i \\ x_ix_{2d+1-i}, & \text{if } \sigma(i) \geq d+1,\ j = 2d+1-i \\ 0, & \text{if } j \neq 2d+1-i. \end{cases}\end{aligned}$$

Taking into account that $\sigma(i) \leq d$ holds if and only if $\sigma(2d+1-i) \geq d+1$ holds, it is now easy to see that $A^{\mathrm{tr}}JA = J$ holds if we set

$$x_i = \begin{cases} -1, & \text{if } i \leq d \text{ and } \sigma(i) > d \\ 1, & \text{if } i \leq d \text{ and } \sigma(i) \leq d \\ 1, & \text{if } i > d. \end{cases}$$

b), c) For both cases $\mathcal{G} = \mathrm{SO}_n$ with $n = 2d$ or $n = 2d+1$, let σ be a permutation such that $\sigma(n+1-i) = n+1-\sigma(i)$ for all $1 \leq i \leq n$. Again, we start with a generic monomial matrix $A = B \cdot \mathrm{diag}(x_1, \ldots, x_n)$ associated to σ (with $B_{ij} = \delta_{\sigma(j),i}$). Now we have $J_{ij} = \delta_{n+1-i,j}$ for all $i, j \leq n$ and so we compute

$$(A^{\mathrm{tr}}JA)_{ij} = x_ix_j\delta_{n+1-i,j},$$

hence $A^{tr}JA = J$ holds if and only if

$$x_ix_{n+1-i} = 1$$

holds for all $1 \leq i \leq n$. The determinant of A equals $\det(A) = \mathrm{sign}(\sigma) \cdot x_1 \ldots x_n$. If $x_ix_{n+1-i} = 1$ holds for all i, we have

$$\det(A) = \begin{cases} \mathrm{sign}(\sigma)x_{d+1} & \text{if } n = 2d+1 \\ \mathrm{sign}(\sigma) & \text{if } n = 2d. \end{cases}$$

If the sign of σ equals one, we are done by setting $x_1 = \cdots = x_n = 1$, i.e., $A = B$ is already contained in $\mathcal{G}$. If the sign of σ equals -1 and $n = 2d$, it is immediate that there cannot exist a monomial matrix of determinant 1 that is orthogonal. Now if $n = 2d+1$ and σ is of sign -1, we can set $x_{d+1} = -1$ and all other $x_i = 1$. Then $x_{d+1}^2 = 1$, hence $A^{\mathrm{tr}}JA = J$ holds and A is of determinant 1.

□

Corollary 4.1.6. *There exist monomial matrices w_1 and w_2 contained in $\mathcal{G}(\mathbb{F}_q)$ corresponding to the following permutations:*

SL_n	$\sigma_1 = (1, 2, \ldots, n)$ $\sigma_2 = (1, \ldots, n-1)$
Sp_{2d}	$\sigma_1 = (1, \ldots, d, 2d, \ldots, d+1)$ $\sigma_2 = (1, \ldots, d)(2d, \ldots, d+1)$
SO_{2d+1}	$\sigma_1 = (1, \ldots, d, 2d, \ldots, d+2)$ $\sigma_2 = (1, \ldots, d)(2d, \ldots, d+2)$
SO_{2d}, *d odd*	$\sigma_1 = (d, d+1)(1, \ldots, d-1, 2d, \ldots, d+2)$ $\sigma_2 = (1, \ldots, d)(2d, \ldots, d+1)$
SO_{2d}, $d = 2m$, *m odd*	$\sigma_1 = (d, d+1)(1, \ldots, d-1, 2d, \ldots, d+2)$ $\sigma_2 = (1, \ldots, m)(m+1, \ldots, 2m)(3m, \ldots, 2m+1)(4m, \ldots, 3m+1)$
SO_{2d}, $d = 2m$, *m even*	$\sigma_1 = (d, d+1)(1, \ldots, d-1, 2d, \ldots, d+2)$ $\sigma_2 = (1, \ldots, m, 4m, \ldots, 3m+1)(m+1, \ldots, 2m, 3m, \ldots, 2m+1)$

Table 4.2: Definition of σ_1, σ_2

Proof. For $\mathcal{G} = \mathrm{SL}_n$, there is nothing to show as there exists a monomial matrix $w_\sigma \in \mathrm{SL}_n$ for any element $\sigma \in S_n$. For all other groups this is an immediate consequence of Lemma 4.1.5. Indeed, it is readily checked that $\sigma_j(n+1-i) = n+1-\sigma_j(i)$ holds for all $1 \leq i \leq n$ and $j = 1, 2$. In case $\mathcal{G} = \mathrm{SO}_{2d}$, σ_1 and σ_2 are moreover both of positive sign. □

Definition 4.1.7. *Let $\mathcal{G}$ be one of the groups SL_n, Sp_{2d} or SO_n and fix monomial matrices $w_1, w_2 \in \mathcal{G}(\mathbb{F}_q)$ with respect to σ_1, σ_2 as described in Corollary 4.1.6. Fix $g_i \in \mathcal{G}(\overline{\mathbb{F}}_q)$ such that $g_i \phi_q(g_i)^{-1} = w_i$ holds for $i = 1, 2$ (the Lang isogeny assures that such elements exist). Then we set $T_i = T_0^{g_i}$, $i = 1, 2$, where T_0 denotes the diagonal torus inside $\mathcal{G}$.*

Proposition 4.1.8. *Let $\mathcal{G}$, T_1 and T_2 be as in Definition 4.1.7. Then T_1 and T_2 are defined over $\mathbb{F}_q$ and we have*

$$|T_i(\mathbb{F}_q)| = n_i(q), \ i = 1, 2.$$

Proof. As w_1 and w_2 normalize T_0, it follows from Proposition 4.1.1 that T_1 and T_2 are defined over $\mathbb{F}_q$ with $\mathbb{F}_q$-rational points

$$\begin{aligned} T_i(\mathbb{F}_q) &= \{t_0 \in T_0(\overline{\mathbb{F}}_q) \mid \phi_q(t_0) = t_0^{w_i}\}^{g_i} \\ &= \{\mathrm{diag}(\lambda_1, \ldots, \lambda_n) \mid \mathrm{diag}(\lambda_1^q, \ldots, \lambda_n^q) = \mathrm{diag}(\lambda_{\sigma_i(1)}, \ldots, \lambda_{\sigma_i(n)})\}^{g_i}. \end{aligned}$$

a) Let $\mathcal{G} = \mathrm{SL}_n$ and let $\mathrm{diag}(\lambda_1, \ldots, \lambda_n) \in T_0(\overline{\mathbb{F}}_q)$. Then

$$\mathrm{diag}(\lambda_{\sigma_1(1)}, \ldots, \lambda_{\sigma_1(n)}) = \mathrm{diag}(\lambda_2, \ldots, \lambda_n, \lambda_1),$$

hence $\mathrm{diag}(\lambda_1^q, \ldots, \lambda_n^q) = \mathrm{diag}(\lambda_{\sigma_1(1)}, \ldots, \lambda_{\sigma_1(n)})$ holds if and only if we have $\mathrm{diag}(\lambda_1, \ldots, \lambda_n) = \mathrm{diag}(\lambda_1, \lambda_1^q, \ldots, \lambda_1^{q^{n-1}})$ and $\lambda_1^{q^n} = \lambda_1$, that is, $\lambda_1 \in \mathbb{F}_{q^n}$. Additionally, we need that $\mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ has determinant one, which is the case if and only if $1 = \lambda_1^{1+q+\cdots+q^{n-1}} = \lambda_1^{\frac{q^n-1}{q-1}}$ holds. Overall, we conclude

$$T_1(\mathbb{F}_q) = \{\mathrm{diag}(\zeta, \zeta^q, \ldots, \zeta^{q^{n-1}}) \mid \zeta^{\frac{q^n-1}{q-1}} = 1\}^{g_1}.$$

In particular, $T_1(\mathbb{F}_q)$ is cyclic of order $\frac{q^n-1}{q-1} = n_1(q)$.
For $i = 2$, we have $\mathrm{diag}(\lambda_{\sigma_2(1)}, \ldots, \lambda_{\sigma_2(n)}) = \mathrm{diag}(\lambda_2, \ldots, \lambda_{n-1}, \lambda_1, \lambda_n)$, hence $\mathrm{diag}(\lambda_1^q, \ldots, \lambda_n^q) = \mathrm{diag}(\lambda_{\sigma_2(1)}, \ldots, \lambda_{\sigma_2(n)})$ holds if and only if we have $\mathrm{diag}(\lambda_1, \ldots, \lambda_n) = \mathrm{diag}(\lambda_1, \lambda_1^q, \ldots, \lambda_1^{q^{n-2}}, \lambda_n)$ and $\lambda_1^{q^{n-1}} = \lambda_1$ (that is, $\lambda_1 \in \mathbb{F}_{q^{n-1}}$) as well as $\lambda_n^q = \lambda_n$ (that is, $\lambda_n \in \mathbb{F}_q$). Additionally, to ensure that $\mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ has determinant one, we need $\lambda_n = \lambda_1^{-1-q-\cdots-q^{n-2}} = \lambda_1^{-\frac{q^{n-1}-1}{q-1}}$. Note that for any $\lambda_1 \in \mathbb{F}_{q^{n-1}}^\times$, we have $\lambda_1^{-\frac{q^{n-1}-1}{q-1}} \in \mathbb{F}_q^\times$. Therefore, we get

$$T_2(\mathbb{F}_q) = \{\mathrm{diag}(\zeta, \zeta^q, \ldots, \zeta^{q^{n-2}}, \zeta^{-\frac{q^{n-1}-1}{q-1}}) \mid \zeta^{q^n-1} = 1\}^{g_2}.$$

In particular, $T_2(\mathbb{F}_q)$ is cyclic of order $q^{n-1} - 1 = n_2(q)$.

b) If $\mathcal{G} = \mathrm{Sp}_{2d}$, $T_0(\overline{\mathbb{F}}_q)$ consist of all diagonal matrices of the form $\mathrm{diag}(\lambda_1, \ldots, \lambda_d, \lambda_d^{-1}, \ldots, \lambda_1^{-1})$ with $\lambda_i \in \overline{\mathbb{F}}_q^\times$. For such an element we have $\mathrm{diag}(\lambda_1^q, \ldots, \lambda_n^q) = \mathrm{diag}(\lambda_{\sigma_1(1)}, \ldots, \lambda_{\sigma_1(n)})$ if and only if $\mathrm{diag}(\lambda_1^q, \ldots, \lambda_d^q, \lambda_d^{-q}, \ldots, \lambda_1^{-q}) = \mathrm{diag}(\lambda_2, \ldots, \lambda_d, \lambda_1^{-1}, \lambda_1, \lambda_d^{-1} \ldots, \lambda_2^{-1})$. We conclude

$$T_1(\mathbb{F}_q) = \{\mathrm{diag}(\zeta, \zeta^q, \ldots, \zeta^{q^{d-1}}, \zeta^{-q^{d-1}}, \ldots, \zeta^{-q}, \zeta^{-1}) \mid \zeta^{q^d+1} = 1\}^{g_1}.$$

In particular, $T_1(\mathbb{F}_q)$ is cyclic of order $q^d + 1 = n_1(q)$. Similarly, we compute

$$T_2(\mathbb{F}_q) = \{\mathrm{diag}(\zeta, \zeta^q, \ldots, \zeta^{q^{d-1}}, \zeta^{-q^{d-1}}, \ldots, \zeta^{-q}, \zeta^{-1}) \mid \zeta^{q^d-1} = 1\}^{g_2}.$$

In particular, $T_2(\mathbb{F}_q)$ is cyclic of order $q^d - 1 = n_2(q)$.

c) For $\mathcal{G} = SO_{2d+1}$, the diagonal torus T_0 consists of all elements of the form $\mathrm{diag}(\lambda_1, \ldots, \lambda_d, 1, \lambda_d^{-1}, \ldots \lambda_1^{-1})$. Then $T_1(\mathbb{F}_q)$ and $T_2(\mathbb{F}_q)$ can be computed in the very same way as for $\mathcal{G} = \mathrm{Sp}_{2d}$:

$$\begin{aligned} T_1(\mathbb{F}_q) &= \{\mathrm{diag}(\zeta, \zeta^q, \ldots, \zeta^{q^{d-1}}, 1, \zeta^{-q^{d-1}}, \ldots, \zeta^{-q}, \zeta^{-1}) \mid \zeta^{q^d+1} = 1\}^{g_1} \\ T_2(\mathbb{F}_q) &= \{\mathrm{diag}(\zeta, \zeta^q, \ldots, \zeta^{q^{d-1}}, 1, \zeta^{-q^{d-1}}, \ldots, \zeta^{-q}, \zeta^{-1}) \mid \zeta^{q^d-1} = 1\}^{g_2}. \end{aligned}$$

In particular, $T_1(\mathbb{F}_q)$ and $T_2(\mathbb{F}_q)$ are both cyclic of order $q^d + 1 = n_1(q)$ and $q^d - 1 = n_2(q)$, resp.

d) Now assume $\mathcal{G} = \mathrm{SO}_{2d}$ for an odd d. The diagonal torus T_0 consists of all elements of the form $\mathrm{diag}(\lambda_1, \ldots, \lambda_d, \lambda_d^{-1}, \ldots, \lambda_1^{-1})$. The torus $T_1(\mathbb{F}_q)$ can be computed similarly to the first torus for the symplectic group Sp_{2d-2}, only that we have an extra transposition in the middle. We deduce that $T_1(\mathbb{F}_q)$ consists of all elements of the form

$$\mathrm{diag}(\zeta, \zeta^q, \ldots, \zeta^{q^{d-2}}, \mu, \mu^{-1}, \zeta^{-q^{d-2}}, \ldots, \zeta^{-q}, \zeta^{-1})^{g_1}$$

such that $\zeta^{q^{d-1}+1} = 1$ and $\mu^{q+1} = 1$, so this time $T_1(\mathbb{F}_q)$ is not cyclic. Its order equals $(q^{d-1}+1)(q+1) = n_1(q)$. Similarly to the symplectic case, we get

$$T_2(\mathbb{F}_q) = \{\mathrm{diag}(\zeta, \zeta^q, \ldots, \zeta^{q^{d-1}}, \zeta^{-q^{d-1}}, \ldots, \zeta^{-q}, \zeta^{-1}) \mid \zeta^{q^d-1} = 1\}^{g_2}$$

In particular, $T_2(\mathbb{F}_q)$ is cyclic of order $q^d - 1 = n_2(q)$.

e) If $\mathcal{G} = \mathrm{SO}_{2d}$ for an even $d = 2m$, the first torus is the same is in the previous case so its order equals $(q^{d-1}+1)(q+1) = n_1(q)$. If m is odd, similar computations as before yield that $T_2(\mathbb{F}_q)$ consists of all elements of the form

$$\mathrm{diag}(\zeta, \zeta^q, \ldots, \zeta^{q^{m-1}}, \mu, \mu^q, \ldots, \mu^{q^{m-1}}, \mu^{-q^{m-1}}, \ldots, \mu^{-1}, \zeta^{-q^{m-1}}, \ldots, \zeta^{-1})^{g_2}$$

with $\zeta^{q^m-1} = 1 = \mu^{q^m-1}$, if m. If m is even, $T_2(\mathbb{F}_q)$ consists of all elements of the form

$$\mathrm{diag}(\zeta, \zeta^q, \ldots, \zeta^{q^{m-1}}, \mu, \mu^q, \ldots, \mu^{q^{m-1}}, \mu^{-q^{m-1}}, \ldots, \mu^{-1}, \zeta^{-q^{m-1}}, \ldots, \zeta^{-1})^{g_2}$$

with $\zeta^{q^m+1} = 1 = \mu^{q^m+1}$. We conclude $T_2(\mathbb{F}_q) = (q^m + (-1)^m)^2 = n_2(q)$.

□

4.2 Generating Classical Groups

We start with a more or less obvious statement, that will be used repeatedly.

Lemma 4.2.1. *a) Let $\mathcal{G} \leq \mathrm{GL}_n$ be a linear algebraic group defined over $\overline{\mathbb{F}}_q$ and let A be contained in $\mathcal{G}(\overline{\mathbb{F}}_q[[t]])$. Then the constant part $A_0 \in \mathrm{M}_n(\overline{\mathbb{F}}_q)$ is contained in $\mathcal{G}(\overline{\mathbb{F}}_q)$.*

b) Let A, B be elements contained in $\mathrm{GL}_n(\overline{\mathbb{F}}_q[[t]])$ with constant parts A_0, $B_0 \in \mathrm{GL}_n(\overline{\mathbb{F}}_q)$. Then the constant part of the conjugate B^A equals $B_0^{A_0}$.

Proof. a) This is true for any affine variety $V \subseteq \mathbb{A}^m$ defined over $\overline{\mathbb{F}}_q$ where in our case, $m = n^2+1$, as GL_n is an affine subset of $\mathbb{A}^{n^2+1}$. Indeed, let $a = (a_1, \ldots, a_m)$ be contained in $V(\overline{\mathbb{F}}_q[[t]])$ and let $a_{10}, \ldots, a_{m0} \in \overline{\mathbb{F}}_q$ denote the constant parts of $a_1, \ldots, a_m$. Then for any $f \in \overline{\mathbb{F}}_q[X_1, \ldots, X_m]$ contained in the vanishing ideal of V, the constant part of $f(a_1, \ldots, a_m)$ equals $f(a_{10}, \ldots, a_{m0})$ which is thus zero. We conclude that $(a_{10}, \ldots, a_{m0})$ is contained in V.

b) The constant part of A^{-1} equals A_0^{-1} and as the constant part of a product of matrices equals the product of their constant parts, hence the constant part of $A^{-1}BA$ equals $A_0^{-1}B_0A_0$.

□

The objective of this section is to prove that certain conjugates of the maximal tori T_1 and T_2 constructed in the previous section generate $\mathcal{G}$. The key ingredient is the following proposition.

Proposition 4.2.2. *Let K_1 be an infinite field and let $\mathcal{G} \leq \mathrm{GL}_n$ be a connected linear algebraic group defined over K_1 such that either K_1 is perfect or $\mathcal{G}$ is reductive. Let further K_2/K_1 be a field extension and consider the field of formal Laurent series $K_2((t))$ over K_2. If $\mathcal{H} \subset \mathcal{G}$ is a closed subvariety defined over $K_2((t))$ such that for all $g \in \mathcal{G}(K_1)$ there exists an $h \in \mathcal{H}(K_2[[t]])$ of the form $h = g + M_1 t + M_2 t^2 + \dots$ for some $M_i \in M_n(K_2)$, then $\mathcal{H} = \mathcal{G}$ holds.*

Proof. First of all, note that $\mathcal{G}(K_1)$ is dense in $\mathcal{G}$, as we assumed that either K_1 is perfect or $\mathcal{G}$ is reductive (see [Bor91, 18.3]).
Set $m = n^2 + 1$. Then $\mathcal{G}$ is a closed subvariety of affine m-space, since $\mathcal{G} \leq \mathrm{GL}_n$ holds. Let $K_t := \overline{K_2((t))}$ be an algebraic closure of $K_2((t))$. We consider the vanishing ideals $I(\mathcal{G})$ and $I(\mathcal{H})$ of $\mathcal{G}$ and $\mathcal{H}$ inside $K_t[X_1, \dots, X_m]$. Assume that $\mathcal{H}$ is strictly contained in $\mathcal{G}$, i.e., $I(\mathcal{H}) \supsetneq I(\mathcal{G})$. Now $I(\mathcal{H})$ is generated by finitely many elements inside $K_2((t))[X_1, \dots, X_m]$ and we conclude that at least one of them cannot be contained in $I(\mathcal{G})$. Let $f \in K_2((t))[X_1, \dots, X_m]$ be such an element, i.e., $f \in I(\mathcal{H}) \backslash I(\mathcal{G})$. After multiplying by a suitable power of t, we may assume that f is contained in $K_2[[t]][X_1, \dots, X_m] \subset K_2[X_1, \dots, X_m][[t]]$. Hence there exist elements $f_j \in K_2[X_1, \dots, X_m]$ such that

$$f = \sum_{j=0}^{\infty} f_j t^j.$$

As $\mathcal{G}(K_1)$ is dense in $\mathcal{G}$, there exists a $g \in \mathcal{G}(K_1)$ with $f(g) \neq 0$. It follows that there exists a $j \in \mathbb{N}$ such that $f_j(g) \neq 0$. Let $j_0 \in \mathbb{N}$ be minimal such that there exists a $g \in \mathcal{G}(K_1)$ with $f_{j_0}(g) \neq 0$. Hence $f_0, \dots, f_{j_0 - 1}$ vanish on all $\mathcal{G}(K_1)$ and are thus contained in $I(\mathcal{G})$. Now consider

$$f' := t^{-j_0}(f - \sum_{j=0}^{j_0 - 1} f_j t^j) = f_{j_0} + f_{j_0+1} t + f_{j_0+2} t^2 + \cdots .$$

As $f \in I(\mathcal{H}) \backslash I(\mathcal{G})$ and $\sum_{j=0}^{j_0-1} f_j t^j \in I(\mathcal{G})$, we have $f' \in I(\mathcal{H}) \backslash I(\mathcal{G})$, as well. By definition of j_0, there exists a $g \in \mathcal{G}(K_1)$ such that $f_{j_0}(g) \neq 0$. By assumptions, there exists an $h = g + M_1 t + M_2 t^2 + \cdots \in \mathcal{H}(K_2[[t]])$ for some $M_i \in M_n(K_2)$, i.e., g occurs as the constant term of an element contained in $\mathcal{H}$. We compute

$$0 = f'(h) = \sum_{j=0}^{\infty} f_{j+j_0}(h) t^j \in K_2[[t]]$$

and compare the constant terms of both sides. The constant term of the right hand side equals the constant term of $f_{j_0}(h)$ which in turn equals $f_{j_0}(g)$,

hence $0 = f_{j_0}(g)$, a contradiction. Hence $\mathcal{H}$ cannot be strictly contained in $\mathcal{G}$. □

In order to be able to apply this proposition, we first have to generalize the result $\mathcal{G}(\mathbb{F}_q) =< T_1(\mathbb{F}_q)^{A_1}, T_2(\mathbb{F}_q)^{A_2} >$ (Theorem 4.1.3) from $\mathbb{F}_q$ to an infinite field $\mathbb{F}$.

Lemma 4.2.3. *Let $l_0 \in \mathbb{N}$ and consider*

$$\mathbb{F} := \bigcup_{l \in \mathbb{N}:\ l \equiv 1 \bmod l_0} \mathbb{F}_{q^l} \subseteq \overline{\mathbb{F}}_q.$$

Then $\mathbb{F}$ is a field of infinite order.

Proof. For any $i, j \in \mathbb{N}$, the compositum of $\mathbb{F}_{q^{il_0+1}}$ and $\mathbb{F}_{q^{jl_0+1}}$ inside $\overline{\mathbb{F}}_q$ equals $\mathbb{F}_{q^{\mathrm{lcm}(il_0+1, jl_0+1)}} \subseteq \mathbb{F}_{q^{(il_0+1)(jl_0+1)}} = \mathbb{F}_{q^{(ijl_0+i+j)l_0+1}}$. Hence $\mathbb{F}_{q^{il_0+1}}$ and $\mathbb{F}_{q^{jl_0+1}}$ are both contained in another field $\mathbb{F}_{q^l}$ with $l \equiv 1 \pmod{l_0}$ which is therefore contained in $\mathbb{F}$. It follows that $\mathbb{F}$ is a field and as $\mathbb{F}$ contains $\mathbb{F}_{q^{il_0+1}}$ for all $i \in \mathbb{N}$, $\mathbb{F}$ cannot be finite. □

Proposition 4.2.4. *Let $\mathcal{G}$ be one of the following classical groups*

- SL_n, $n \geq 3$
- Sp_{2d}, $d \geq 2$
- SO_n, $n \geq 7$

and let the monomial matrices $w_1, w_2 \in \mathcal{G}(\mathbb{F}_q)$ (corresponding to the permutations σ_1, σ_2) and the maximal tori T_1, T_2 be as defined in Definition 4.1.7. Let l_0 be the least common multiple of the order of σ_1 and σ_2. Then for $\mathbb{F} := \bigcup_{l \in \mathbb{N}:\ l \equiv 1 \bmod l_0} \mathbb{F}_{q^l} \subseteq \overline{\mathbb{F}}_q$ as in 4.2.3 and any $A_1, A_2 \in \mathcal{G}(\mathbb{F}_q)$, we have

$$< T_1(\mathbb{F})^{A_1}, T_2(\mathbb{F})^{A_2} >= \mathcal{G}(\mathbb{F}).$$

Proof. Recall that g_1 and g_2 where chosen in such a way that $\phi_q(g_i)g_i^{-1} = w_i$ holds. Hence for an l with $l \equiv 1 \mod l_0$ we have $\phi_{q^l}(g_i) = \phi_{q^{l-1}}(w_i g_i) = \cdots = w_i^l \cdot g_i$, where we used that w_i is contained in $\mathcal{G}(\mathbb{F}_q)$, for $i = 1, 2$. Now w_i^l is again monomial with respect to $\sigma_i^l = \sigma_i$. It thus follows from Proposition 4.1.8 that

$$|T_i(\mathbb{F}_{q^l})| = n_i(q^l)$$

holds for $i = 1, 2$. Let A_1 and A_2 be contained in $\mathcal{G}(\mathbb{F}_q)$. Then Theorem 4.1.3 implies that

$$< T_1(\mathbb{F}_{q^l})^{A_1}, T_2(\mathbb{F}_{q^l})^{A_2} >= \mathcal{G}(\mathbb{F}_{q^l})$$

holds for all l with $l \equiv 1 \mod l_0$. Now let $g = (g_{rs})$ be contained in $\mathcal{G}(\mathbb{F})$. Then there exist numbers $i_{rs} \in \mathbb{N}$ such that g_{rs} is contained in $\mathbb{F}_{q^{i_{rs}l_0+1}}$ for

all $1 \leq r, s \leq n$ (where we set $n = 2d$ in case $\mathcal{G} = \mathrm{Sp}_{2d}$). Let l be the product of $(i_{rs} l_0 + 1)$ over all $1 \leq r, s \leq n$. Then $l \equiv 1 \mod l_0$ holds and all entries g_{rs} are contained in $\mathbb{F}_{q^l}$. Hence

$$g \in \mathcal{G}(\mathbb{F}_{q^l}) =< T_1(\mathbb{F}_{q^l})^{A_1}, T_2(\mathbb{F}_{q^l})^{A_2} > \subseteq < T_1(\mathbb{F})^{A_1}, T_2(\mathbb{F})^{A_2} >$$

and we conclude $\mathcal{G}(\mathbb{F}) \subseteq < T_1(\mathbb{F})^{A_1}, T_2(\mathbb{F})^{A_2} >$. □

Theorem 4.2.5. *Let $\mathcal{G}$ be one of the following classical groups*

- SL_n, $n \geq 3$
- Sp_{2d}, $d \geq 2$
- SO_n, $n \geq 7$

and let the maximal tori T_1, T_2 be as defined in Definition 4.1.7. Then for any $A, B \in \mathcal{G}(\mathbb{F}_q + t\overline{\mathbb{F}}_q[[t]])$ (i.e., A and B are contained in $\mathcal{G}(\overline{\mathbb{F}}_q[[t]])$ such that the constant term of any coordinate is contained in $\mathbb{F}_q$), we have

$$< T_1^A, T_2^B >= \mathcal{G}.$$

Proof. As T_1^A and T_2^B are closed, connected subgroups of $\mathcal{G}$ that are defined over $\overline{\mathbb{F}}_q((t))$, we have that $\mathcal{H} :=< T_1^A, T_2^B >$ is a closed subgroup of $\mathcal{G}$ that is defined over $\overline{\mathbb{F}}_q((t))$ (see [Spr09, 2.2.7]). Let $\mathbb{F} \subseteq \overline{\mathbb{F}}_q$ be as defined in Proposition 4.2.4. By Proposition 4.2.2 (with $K_1 = \mathbb{F}$ and $K_2 = \overline{\mathbb{F}}_q$), it is sufficient to show that for any $g \in \mathcal{G}(\mathbb{F})$ there exist an element $h \in \mathcal{H}(\overline{\mathbb{F}}_q[[t]])$ with constant part g. Let $A_0, B_0 \in \mathrm{GL}_n(\mathbb{F}_q)$ be the constant parts of A, B, resp. As $\mathcal{G}$ is defined over $\mathbb{F}_q$ and A, B are contained in $\mathcal{G}$, it follows that A_0 and B_0 are contained in $\mathcal{G}(\mathbb{F}_q)$, by the first part of Lemma 4.2.1. By Proposition 4.2.4, we thus have $\mathcal{G}(\mathbb{F}) =< T_1(\mathbb{F})^{A_0}, T_2(\mathbb{F})^{B_0} >$. Let $g \in \mathcal{G}(\mathbb{F})$. Then there exist an $r \in \mathbb{N}$ and elements $x_i \in T_1(\mathbb{F})$ and $y_i \in T_2(\mathbb{F})$ such that

$$g = x_1^{A_0} y_1^{B_0} \dots x_r^{A_0} y_r^{B_0}.$$

Then

$$h := x_1^A y_1^B \dots x_r^A y_r^B \in < T_1(\mathbb{F})^A, T_2(\mathbb{F})^B > \subseteq \mathcal{H}(\overline{\mathbb{F}}_q[[t]])$$

has constant term g (by Lemma 4.2.1, b)) which concludes the proof. □

In order to show that a closed subgroup $\mathcal{H}$ of $\mathcal{G}$ (e.g. the Galois group of a difference module) is all of $\mathcal{G}$, we may thus show that certain conjugates of the maximal tori T_1 and T_2 are contained in $\mathcal{H}$. It is therefore sufficient to show that $\mathcal{H}$ contains elements that are dense in T_1 and T_2, resp. Fortunately, a maximal torus contains quite a lot of dense elements, as the following (well-known) lemma demonstrates.

Lemma 4.2.6. *Let $\mathcal{G}$ be a linear algebraic group over the algebraically closed field K. Let $T \leq \mathcal{G}$ be a torus of $\mathcal{G}$. Assume that there exists an element $s \in T$ such that $\chi(s) \neq 1$ holds for all non-trivial characters $\chi \in X^*(T)$. Then s generates a dense subgroup of T.*

Proof. Let $S \leq T$ be the closure of the cyclic group generated by s. Its coordinate ring $K[S]$ is a quotient space of $K[T]$. As T is diagonizable, its characters $X^*(T)$ form a K-basis of the coordinate ring T (see [Spr09, Thm. 3.2.3]). Let χ, χ' be two distinct characters of T. Then $\chi^{-1}\chi'$ is non-trivial and thus $\chi(s) \neq \chi'(s)$, by assumptions. It follows that $X^*(T)$ injects into $X^*(S)$ via restriction. As S is also diagonizable, we have that its characters form a K-basis of $K[S]$. In particular, the basis $X^*(T)$ of $K[T]$ projects on a system of linearly independent elements in the quotient space $K[S]$. It follows that $K[S] = K[T]$ and thus $S = T$ holds. □

Example 4.2.7. *Let $\mathcal{G} = \mathrm{SL}_3$ and T the diagonal torus inside $\mathcal{G}$. Its characters are generated by the standard characters χ_1 and χ_2 that project diagonal matrices on the first or second diagonal entry, resp. Then a diagonal matrix $s = \mathrm{diag}(\lambda_1, \lambda_2, (\lambda_1\lambda_2)^{-1})$ generates a dense subgroup of T if for all $(e_1, e_2) \in \mathbb{Z}^2 \backslash \{(0,0)\}$ we have $\chi_1^{e_1}\chi_2^{e_2}(s) \neq 1$, that is, if $\lambda_1^{e_1}\lambda_2^{e_2} \neq 1$. Over $\mathbb{C}$, any element $s = \mathrm{diag}(p_1, p_2, \frac{1}{p_1 p_2})$ with distinct prime numbers p_1 and p_2 is thus dense in T. Similarly, over $\overline{\mathbb{F}_q(t)}$, every element $s = \mathrm{diag}(p_1, p_2, \frac{1}{p_1 p_2})$ with coprime polynomials $p_1, p_2 \in \mathbb{F}_q[t]$ generates a dense subgroup of T.*

4.3 Generating Split Reductive Groups

We proceed with another application of Proposition 4.2.2 leading to a result on generating arbitrary connected reductive linear algebraic groups in positive characteristic.

Theorem 4.3.1. *Let $\mathcal{G}$ be a connected and reductive linear algebraic group defined over $\mathbb{F}_q$. Assume further that $\mathcal{G}$ splits over $\mathbb{F}_q$, i.e., there exists a maximal torus T of $\mathcal{G}$ that is defined over $\mathbb{F}_q$ and splits over $\mathbb{F}_q$. Let $\mathcal{H}$ be a closed subgroup of $\mathcal{G}$ defined over $\overline{\mathbb{F}}_q((t))$ that contains T^A for some $A \in \mathcal{G}(\mathbb{F}_q + t\overline{\mathbb{F}}_q[[t]])$ and such that every $g \in \mathcal{G}(\mathbb{F}_q)$ occurs as the constant part of an element inside $\mathcal{H}(\overline{\mathbb{F}}_q[[t]])$. Then $\mathcal{H} = \mathcal{G}$. In particular, $< T^A, \mathcal{G}(\mathbb{F}_q) >$ is dense in $\mathcal{G}$ for any $A \in \mathcal{G}(\mathbb{F}_q + t\overline{\mathbb{F}}_q[[t]])$.*

Proof. By Proposition 4.2.2 (applied to $K_1 = K_2 = \overline{\mathbb{F}}_q$), it is sufficient to show that for any $g \in \mathcal{G}(\overline{\mathbb{F}}_q)$, there exists an element $h \in \mathcal{H}(\overline{\mathbb{F}}_q[[t]])$ with constant part g.

As the constant part A_0 of A is contained in $\mathcal{G}(\mathbb{F}_q)$, the maximal torus T^{A_0} is defined over $\mathbb{F}_q$ and also splits over $\mathbb{F}_q$. Let $\Phi(\mathcal{G}, T^{A_0})$ denote the set of roots with respect to T^{A_0} and for $\alpha \in \Phi(\mathcal{G}, T^{A_0})$, let U_α be the root

subgroup corresponding to α. Since T^{A_0} splits over $\mathbb{F}_q$, all root subgroups are defined over $\mathbb{F}_q$ and we moreover have isomorphisms

$$u_\alpha \colon \mathbb{G}_a \to U_\alpha$$

defined over $\mathbb{F}_q$ for all $\alpha \in \Phi(\mathcal{G}, T^{A_0})$ (see [Bor91, V.18.7] for a proof). Now $\mathcal{G}$ is generated by T^{A_0} together with all root subgroups (see [Spr09, 8.1.1]) and as all of these are defined over $\mathbb{F}_q \subseteq \overline{\mathbb{F}}_q$, we obtain

$$\begin{aligned} \mathcal{G}(\overline{\mathbb{F}}_q) &= < T^{A_0}(\overline{\mathbb{F}}_q), U_\alpha(\overline{\mathbb{F}}_q) \mid \alpha \in \Phi(\mathcal{G}, T^{A_0}) > \\ &= < T(\overline{\mathbb{F}}_q)^{A_0}, U_\alpha(\overline{\mathbb{F}}_q) \mid \alpha \in \Phi(\mathcal{G}, T^{A_0}) > . \end{aligned}$$

Let now g be contained in $\mathcal{G}(\overline{\mathbb{F}}_q)$. Then there exist an $r \in \mathbb{N}$, roots $\alpha_1, \ldots, \alpha_r \in \Phi(\mathcal{G}, T^{A_0})$ (not necessarily pairwise distinct), $s_1, \ldots, s_r \in \overline{\mathbb{F}}_q$ as well as $x_1, \ldots, x_{r+1} \in T(\overline{\mathbb{F}}_q)$ such that g can be written as

$$g = x_1^{A_0} u_{\alpha_1}(s_1) \cdots x_r^{A_0} u_{\alpha_r}(s_r) x_{r+1}^{A_0}.$$

Any root $\alpha \in \Phi(\mathcal{G}, T^{A_0})$ is a non-trivial character $\alpha \colon T^{A_0} \to \mathbb{G}_m$, hence it is surjective. As $u_\alpha(0) = 1$ holds for all $\alpha \in \Phi(\mathcal{G}, T^{A_0})$, we may assume that all $s_1, \ldots, s_r$ are contained in $\overline{\mathbb{F}}_q^\times$, so there exist elements $y_1^{A_0}, \ldots, y_r^{A_0} \in T^{A_0}(\overline{\mathbb{F}}_q)$ (that is, $y_1, \ldots, y_r$ are contained in $T(\overline{\mathbb{F}}_q)$) such that

$$s_i = \alpha_i(y_i^{A_0})$$

for $1 \leq i \leq r$. The root subgroup isomorphisms u_α are subject to the relation

$$u_\alpha(\alpha(y)s) = u_\alpha(s)^y$$

for all elements y in the maximal torus and field elements s. Therefore, we have $u_{\alpha_i}(s_i) = u_{\alpha_i}(\alpha_i(y_i^{A_0}) \cdot 1) = u_{\alpha_i}(1)^{y_i^{A_0}}$ for all $1 \leq i \leq r$ and thus

$$g = x_1^{A_0}(y_1^{A_0})^{-1} u_{\alpha_1}(1) y_1^{A_0} \cdots x_r^{A_0}(y_r^{A_0})^{-1} u_{\alpha_r}(1) y_r^{A_0} x_{r+1}^{A_0}.$$

As all isomorphisms u_{α_i} are defined over $\mathbb{F}_q$, we have $u_{\alpha_i}(1) \in \mathcal{G}(\mathbb{F}_q)$ for all $i \leq r$. By assumptions, there exist elements $h_1, \ldots, h_r \in \mathcal{H}(\overline{\mathbb{F}}_q[[t]])$ such that the constant part of h_i equals $u_{\alpha_i}(1)$ for $1 \leq i \leq r$. Now consider

$$h := x_1^A (y_1^A)^{-1} h_1 y_1^A \cdots x_r^A (y_r^A)^{-1} h_r y_r^A x_{r+1}^A \in \mathcal{H}(\overline{\mathbb{F}}_q[[t]]).$$

It is immediate from the second part of Lemma 4.2.1 that the constant part of h equals g (recall that x_1 and y_1 are contained in $\mathcal{G}(\overline{\mathbb{F}}_q)$). Hence $\mathcal{H} = \mathcal{G}$ holds.

As a special case, let $\mathcal{H} \subseteq \mathcal{G}$ be the Zariski closure of $< T^A, \mathcal{G}(\mathbb{F}_q) >$. As A is contained in $\mathcal{G}(\overline{\mathbb{F}}_q((t)))$, we deduce that $T^A \cup \mathcal{G}(\mathbb{F}_q)$ is a closed subset of $\mathcal{G}$ defined over $\overline{\mathbb{F}}_q((t))$. Therefore, $\mathcal{H}$ is defined over $\overline{\mathbb{F}}_q((t))$ as well (see [Bor91, I.2.1(b)]). Hence $\mathcal{H}$ conforms to the assumptions made in this Theorem, and $\mathcal{H} = \mathcal{G}$ follows. □

4.4 Conjugacy over Power Series

In the previous sections, we found maximal tori such that any $\mathcal{G}(\mathbb{F}_q+t\cdot\overline{\mathbb{F}}_q[[t]])$-conjugates generate the given classical group $\mathcal{G}$. The lower bound criterion Corollary 3.3.11 provides us with $\mathcal{G}(\overline{\mathbb{F}}_q[[t]])$-conjugates of certain elements that are contained in the Galois group. Therefore, we have to descend from $\mathcal{G}(\overline{\mathbb{F}}_q[[t]])$-conjugacy to $\mathcal{G}(\mathbb{F}_q + t\cdot\overline{\mathbb{F}}_q[[t]])$-conjugacy.

Lemma 4.4.1. *Let $\mathcal{G}$ be a linear algebraic group defined over $\mathbb{F}_q$. Let g, h be two semisimple elements in $\mathcal{G}(\mathbb{F}_q)$ and assume that the centralizer of g is connected. If g and h are conjugate over $\mathcal{G}(\overline{\mathbb{F}}_q)$ then they are already conjugate over $\mathcal{G}(\mathbb{F}_q)$.*

Proof. Let $x \in \mathcal{G}(\overline{\mathbb{F}}_q)$ be such that $g^x = h$. As g and h are both $\mathbb{F}_q$-rational, we have

$$g^x = h = \phi_q(h) = \phi_q(g)^{\phi_q(x)} = g^{\phi_q(x)}.$$

Hence $\phi_q(x)x^{-1}$ is contained in the centralizer $\mathcal{C}$ of g. By assumptions, $\mathcal{C}$ is connected and it is defined over $\mathbb{F}_q$. Hence we can apply the Lang isogeny to $\mathcal{C}$ to get an element $y \in \mathcal{C}(\overline{\mathbb{F}}_q)$ with $\phi_q(y)y^{-1} = \phi_q(x)x^{-1}$. It follows that $y^{-1}x$ is contained in $\mathcal{G}(\mathbb{F}_q)$ and as y and g commute, we have $h = g^x = g^{y^{-1}x}$. □

Remark 4.4.2. *In case $\mathcal{G}$ is a reductive, connected linear algebraic group such that the commutator subgroup $\mathcal{G}'$ is simply-connected, all centralizers of semisimple elements are connected (see [Car85, 3.5.6]).*

Proposition 4.4.3. *Let $\mathcal{G} \leq \mathrm{GL}_n$ be a linear algebraic group defined over $\mathbb{F}_q$. Let g, h be contained in $\mathcal{G}(\mathbb{F}_q + t\cdot\overline{\mathbb{F}}_q[[t]])$. Assume that g is contained in a maximal torus T of $\mathcal{G}$ that is defined over $\mathbb{F}_q$ and that the centralizer of the constant part $g_0 \in T(\mathbb{F}_q)$ of g equals T. If g and h are conjugate over $\mathcal{G}(\overline{\mathbb{F}}_q[[t]])$ then they are already conjugate over $\mathcal{G}(\mathbb{F}_q + t\cdot\overline{\mathbb{F}}_q[[t]])$.*

Proof. Let $A \in \mathcal{G}(\overline{\mathbb{F}}_q[[t]]))$ be such that $g^A = h$. As $\mathcal{G}$ is defined over $\mathbb{F}_q$, the constant part A_0 of A is contained in $\mathcal{G}(\overline{\mathbb{F}}_q)$ (by Lemma 4.2.1, a)). Similarly, g and h are contained in $\mathcal{G}(\mathbb{F}_q+t\cdot\overline{\mathbb{F}}_q[[t]])$, so their constant parts g_0 and h_0 are contained in $\mathcal{G}(\mathbb{F}_q)$. Then $g^A = h$ implies $g_0^{A_0} = h_0$ (see Lemma 4.2.1, b)). Now Lemma 4.4.1 (and its proof) implies that there exists an element y in the centralizer $\mathcal{C}$ of g_0 inside $\mathcal{G}(\overline{\mathbb{F}}_q)$ such that $y^{-1}A_0$ is contained in $\mathcal{G}(\mathbb{F}_q)$. By assumptions, $\mathcal{C} = T$, so $y \in T(\overline{\mathbb{F}}_q)$. We conclude that y also commutes with g. Hence $h = g^A = g^{y^{-1}A}$ holds. The constant part of $y^{-1}A$ equals $y^{-1}A_0$ which is $\mathbb{F}_q$-rational. Hence h and g are conjugate over $\mathcal{G}(\mathbb{F}_q + t\cdot\overline{\mathbb{F}}_q[[t]])$. □

Chapter 5

Applications

5.1 Our Fields of Definition

We keep up the notation set up in Chapter 2, but make further specifications that will be effective throughout Chapter 5.

(k, ϕ_q)	$k = \mathbb{F}_q(s)$ with the ordinary Frobenius homomorphism $\phi_q \colon \mathbb{F}_q(s) \to \mathbb{F}_q(s), x \mapsto x^q$.
$\lvert\cdot\rvert$	on k, $\lvert\cdot\rvert$ is the s-adic absolute value $\mathbb{F}_q(s) \to \mathbb{R}$, $0 \neq f \mapsto (\frac{1}{2})^{\nu_s(f)}$, where $\nu_s(f) \in \mathbb{Z}$ denotes the s-adic valuation of f.
(K, ϕ_q)	K denotes the completion of the algebraic closure of the completion of $(k, \lvert\cdot\rvert)$; an algebraically closed field that is complete with respect to the unique extension of $\lvert\cdot\rvert$ to K. Again, ϕ_q is the ordinary Frobenius homomorphism on K.
$(K\{t\}, \phi_q)$, (L, ϕ_q)	are as defined in Chapter 2, with respect to $\lvert\cdot\rvert$ and K as above. In particular, $L \subseteq K((t))$ is a difference field with field of constants $C_L = \mathbb{F}_q(t)$.
(F, ϕ_q)	the base field of our difference modules: $F = \mathbb{F}_q(s,t)$ with $\phi_q(s) = s^q$ and $\phi_q(t) = t$. The field of constants C_F equals $\mathbb{F}_q(t)$.

5.2 Auxiliary Material

We would like our Galois group schemes to be (geometrically) reduced, so we will have to ensure that the Picard-Vessiot extensions are separable (see Theorem 1.3.10). The Picard-Vessiot extensions constructed will eventually be contained in $\overline{\mathbb{F}_q(s)}^{\mathrm{sep}}((t))$ which is separable over $\mathbb{F}_q(s)(t)$ by the following Proposition, where we prove the statement for the slightly more general case $\mathbb{F}_q(\underline{s})$ with $\underline{s} = (s_1, \ldots, s_l)$ finitely many algebraically independent elements.

Proposition 5.2.1. *$\overline{\mathbb{F}_q(\underline{s})}^{\text{sep}}((t))$ is a separable field extension of $\mathbb{F}_q(\underline{s})(t)$.*

Proof. By [Mat89, 26.4], it suffices to show that $\overline{\mathbb{F}_q(\underline{s})}^{\text{sep}}((t))$ and $(\mathbb{F}_q(\underline{s})(t))^{1/p}$ are linearly disjoint over $\mathbb{F}_q(\underline{s})(t)$. Now $(\mathbb{F}_q(\underline{s})(t))^{1/p}$ is a finite extension of $\mathbb{F}_q(\underline{s})(t)$ with basis

$$\{(s_1^{e_1}\cdots s_l^{e_l})^{1/p}t^{f/p} \mid \underline{e}=(e_1,\ldots,e_l)\in\{0,1,\ldots,p-1\}^l, f\in\{0,1,\ldots,p-1\}\}.$$

We have to show that these elements are linearly independent over $\overline{\mathbb{F}_q(\underline{s})}^{\text{sep}}((t))$. Assume they are linearly dependent, so there exist elements $a_{(\underline{e},f)}(t)\in\overline{\mathbb{F}_q(\underline{s})}^{\text{sep}}((t))$ such that

$$\sum_{(\underline{e},f)\in\{0,\ldots,p-1\}^{l+1}} a_{(\underline{e},f)}(t)(s_1^{e_1}\ldots s_l^{e_l})^{1/p}t^{f/p}=0 \tag{5.1}$$

is a non-trivial combination of zero. After multiplying by a suitable power of t, we may assume that all $a_{(\underline{e},f)}(t)$ are contained in $\overline{\mathbb{F}_q(\underline{s})}^{\text{sep}}[[t]]$ and at least one of them is contained in $\overline{\mathbb{F}_q(\underline{s})}^{\text{sep}}[[t]]^\times$. We now take both sides of Equation (5.1) to their p-th powers and get

$$\begin{aligned}&\sum_{\underline{e}\in\{0,\ldots,p-1\}^l} s_1^{e_1}\ldots s_l^{e_l}(a_{(\underline{e},0)}(t))^p+\sum_{\underline{e}\in\{0,\ldots,p-1\}^l} s_1^{e_1}\ldots s_l^{e_l}(a_{(\underline{e},1)}(t))^pt\\&+\cdots+\sum_{\underline{e}\in\{0,\ldots,p-1\}^l} s_1^{e_1}\ldots s_l^{e_l}(a_{(\underline{e},p-1)}(t))^pt^{p-1}=0.\end{aligned} \tag{5.2}$$

Now the first sum is a power series in t^p over $\overline{\mathbb{F}_q(\underline{s})}^{sep}$, the second sum is a power series over $\overline{\mathbb{F}_q(\underline{s})}^{sep}$ where only t^{ip+1}-terms occur ($i\in\mathbb{N}$) and so on. We conclude that every single sum in Equation (5.2) equals zero. Now let $0\le i\le p-1$ be such that $a_{(\underline{e},i)}(t)$ is contained in $\overline{\mathbb{F}_q(\underline{s})}^{\text{sep}}[[t]]^\times$ for some $\underline{e}$. Then

$$\sum_{\underline{e}\in\{0,\ldots,p-1\}^l} s_1^{e_1}\ldots s_l^{e_l}(a_{(\underline{e},i)}(t))^pt^i=0$$

holds, as we just saw and we can divide by t^i. The resulting power series on the left hand side has constant term

$$\sum_{\underline{e}\in\{0,\ldots,p-1\}^l}(s_1^{e_1}\ldots s_l^{e_l})a_{(\underline{e},i),0}^p=0$$

where one of the $a_{(\underline{e},i),0}$ is non-zero ($a_{(\underline{e},i),0}$ denotes the constant term of $a_{(\underline{e},i)}(t)$). Taking the p-th root on both side, we thus get a non-trivial linear combination of $\{(s_1^{e_1}\cdots s_l^{e_l})^{1/p}\mid\underline{e}=(e_1,\ldots,e_l)\in\{0,1,\ldots,p-1\}^l\}$ equalling zero, which means that these elements are linearly dependent over $\overline{\mathbb{F}_q(\underline{s})}^{sep}$. But $\{(s_1^{e_1}\cdots s_l^{e_l})^{1/p}\mid\underline{e}=(e_1,\ldots,e_l)\in\{0,1,\ldots,p-1\}^l\}$ is a basis of $\mathbb{F}_q(\underline{s})^{1/p}$ over $\mathbb{F}_q(\underline{s})$, so $\overline{\mathbb{F}_q(\underline{s})}^{sep}$ and $\mathbb{F}_q(\underline{s})^{1/p}$ are not linearly disjoint over $\mathbb{F}_q(\underline{s})$, a contradiction to the separability of $\overline{\mathbb{F}_q(\underline{s})}^{sep}$ over $\mathbb{F}_q(\underline{s})$. □

Proposition 5.2.2. *Let $\mathbb{F}$ be a field. Let $A, B \in \mathrm{GL}_n(\mathbb{F}[[t]])$ have the same characteristic polynomial and assume that their eigenvalues $\lambda_1, \dots \lambda_n$ are contained in $\mathbb{F}[[t]]$ with pairwise distinct constant terms $\lambda_{1,0}, \dots, \lambda_{n,0} \in \mathbb{F}^\times$. Then A and B are conjugate over $\mathrm{GL}_n(\mathbb{F}[[t]])$.*

Proof. Note that A and B are diagonalizable over $\mathbb{F}((t))$ since their eigenvalues are pairwise distinct. Hence there exist $C, \tilde{C} \in \mathrm{GL}_n(\mathbb{F}((t)))$ with $C^{-1}AC = \mathrm{diag}(\lambda_1, \dots, \lambda_n) = \tilde{C}^{-1}B\tilde{C}$. By multiplying C from the right with $\mathrm{diag}(t^{e_1}, \dots, t^{e_n})$ for suitable $e_1, \dots, e_n \in \mathbb{Z}$ we may assume that all entries of C are contained in $\mathbb{F}[[t]]$ and that at least one entry in every column is contained in $\mathbb{F}[[t]]^\times$. We claim that C is contained in $\mathrm{GL}_n(\mathbb{F}[[t]])$. Write $C = \sum_{i=0}^{\infty} C_i t^i$ for some $C_i \in \mathrm{M}_n(\mathbb{F})$. Then C_0 has a non-zero entry in every column. We have to show that C_0 is contained in $\mathrm{GL}_n(\mathbb{F})$. Note that $AC = C\,\mathrm{diag}(\lambda_1, \dots, \lambda_n)$ implies $A_0C_0 = C_0\,\mathrm{diag}(\lambda_{1,0}, \dots, \lambda_{n,0})$, where $A_0 \in \mathrm{GL}_n(\mathbb{F})$ denotes the constant coefficient matrix of A. Hence the i-th column of C_0 is an eigenvector of A_0 with respect to $\lambda_{i,0}$. As all these eigenvalues are pairwise distinct, the columns of C_0 are linearly independent. Similarly, $\tilde{C}$ can be transformed to a matrix inside $\mathrm{GL}_n(\mathbb{F}[[t]])$, hence A and B are conjugate via $C\tilde{C}^{-1} \in \mathrm{GL}_n(\mathbb{F}[[t]])$. □

5.3 The Method

5.3.1 How to Choose the Representing Matrix

Given a difference module M over F with representing matrix D (such that there exists a separable Picard-Vessiot extension), we know that the Galois group contains conjugates of all permissible specializations of D, by Theorem 3.3.10. On the other hand, Theorem 4.2.5 provides elements that generate a given classical group $\mathcal{G}$ even after certain conjugations. So the question is: How to choose a representing matrix D that allows sufficient specializations?
(Of course, D has also to be chosen in such a way that there exists a separable Picard-Vessiot extension for M and such that we can apply the upper bound Theorem 3.2.4. All these issues will be dealt with in the next paragraph.)

We start with a Theorem due to Steinberg, a proof can be found in [Ste65, Theorem 1.4]. We note that the Steinberg cross section $X_{\mathcal{G}}$ (as introduced in the following theorem) has already proved useful to construct polynomials over $\mathbb{F}_q(s)$ with finite classical Galois groups (see [AM10]).

Theorem 5.3.1 (Steinberg)**.** *Let $\mathcal{G}$ be a semisimple linear algebraic group of rank r over an algebraically closed field. Let T be a maximal torus of $\mathcal{G}$ and fix simple roots $\{\alpha_i \mid 1 \le i \le r\}$ with respect to T. For each i, let X_i denote the root subgroup with respect to α_i and fix elements $w_1, \dots, w_r \in \mathcal{N}_{\mathcal{G}}(T)$*

corresponding to the reflections relative to $\alpha_1, \dots, \alpha_r$. Set $X_{\mathcal{G}} := \prod_{i=1}^{r} X_i w_i$. If $\mathcal{G}$ is simply-connected, then $X_{\mathcal{G}}$ is a cross section of the collection of regular classes in $\mathcal{G}$. In particular, $X_{\mathcal{G}}$ contains an element in every semisimple regular conjugacy class.

Remark 5.3.2. *In case $\mathcal{G}$ splits over $\mathbb{F}_q$, it follows from [Ste65, Theorem 9.2] that $X_{\mathcal{G}}$ is defined over $\mathbb{F}_q$ (for a suitable choice of X_i and w_i).*

Example 5.3.3. *For $\mathcal{G} = \mathrm{SL}_3$ we let T be the diagonal torus with standard characters χ_1, χ_2 and χ_3. We choose the simple roots $\alpha_1 = \chi_1\chi_2^{-1}$ and $\alpha_2 = \chi_2\chi_3^{-1}$. Then the Steinberg cross section is easily computed to be*

$$X_{\mathrm{SL}_3} = \{ \begin{pmatrix} f_1 & f_2 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \mid f_1, f_2 \}.$$

If we want to construct a difference module with Galois group SL_3, it would be a good choice to start with a matrix $D_{(f_1,f_2)} := \begin{pmatrix} f_1 & f_2 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ where f_1 and f_2 have to be chosen inside F in a suitable way.

In general, let $x_i \colon \mathbb{G}_a \to U_{\alpha_i}$ be isomorphisms of the additive group onto the root subgroups. As all classical groups split over $\mathbb{F}_q$, we can choose a split maximal torus T (the diagonal torus) and isomorphisms x_i defined over $\mathbb{F}_q$. Then we let

$$D_{(f_1,\dots,f_r)} := x_1(f_1)w_1 \dots x_r(f_r)w_r \in \mathcal{G}(\mathbb{F}_q(f_1, \dots, f_r))$$

be a "generic element" of the cross section. The elements $f_1, \dots f_r$ will be chosen inside F in a suitable way. Consider specializations $s \mapsto \alpha \in \mathbb{F}_q$. Assume that $f_1, \dots f_r \in F = \mathbb{F}_q(s,t)$ have been fixed and that they specialize to elements $\overline{f}_1, \dots, \overline{f}_r \in \mathbb{F}_q(t)$ (i.e., no coefficient of $f_i \in \mathbb{F}_q(s)(t)$ has denominator divisible by $(s-\alpha)$, for $1 \le i \le r$). As the entries of D are polynomials in $f_1, \dots, f_r$ over $\mathbb{F}_q$, we have that $D_{(f_1,\dots,f_r)}$ specializes to $D_{(\overline{f}_1,\dots,\overline{f}_r)}$, an element in the cross section over $\mathbb{F}_q(t)$. Now Theorem 5.3.1 asserts that

$$\{D_{(\overline{f}_1,\dots,\overline{f}_r)} \mid \overline{f}_1, \dots, \overline{f}_r \in \overline{\mathbb{F}_q(t)}\}$$

contains elements in every regular conjugacy class of $\mathcal{G}(\overline{\mathbb{F}_q(t)})$. Hence the elements $\{f_1, \dots, f_r\}$ have to be chosen in such a way that they specialize to the finitely many sets of $\{\overline{f}_1, \dots, \overline{f}_r\}$ corresponding to conjugates of the desired generators. Of course, here we have to check that these $\{\overline{f}_1, \dots, \overline{f}_r\}$ provided by Theorem 5.3.1 are actually contained in $\mathbb{F}_q(t)$ and not just in $\overline{\mathbb{F}_q(t)}$. Another issue is that not all of the groups treated later on are simply-connected (SO_n is not), so Theorem 5.3.1 doesn't apply. However, this doesn't affect us much as we won't actually apply the theorem but only use it as starting point how to choose the matrix D.

5.3.2 An Outline of the Procedure

So far, we have worked out different tools as to construct separable Picard-Vessiot extension with predetermined Galois group. We now give a quick overview of how these tools will be combined in our applications to classical groups.
Given a classical group $\mathcal{G}$ of rank r, proceed as follows:

(1) Determine the Steinberg cross section $X_{\mathcal{G}}$ and start with a generic matrix $D_{(f_1,\dots,f_r)} \in X_{\mathcal{G}}(\mathbb{F}_q(f_1,\dots,f_r))$.

(2) Choose $f_1,\dots,f_r \in F = \mathbb{F}_q(s)(t)$ such that $D_{(f_1,\dots,f_r)}$ can be specialized (via specializations $s \mapsto \alpha \in \mathbb{F}_q$) to $\mathcal{G}(\overline{\mathbb{F}}_q[[t]])$-conjugates of regular elements $t_1 \in T_1(\mathbb{F}_q[[t]])$ and $t_2 \in T_2(\mathbb{F}_q[[t]])$ (where the maximal tori T_1 and T_2 are defined in 4.1.7) that are dense in T_1 and T_2, resp. Dense elements in maximal tori can be easily determined using Lemma 4.2.6. The procedure now is to check that the characteristic polynomial of D specializes to the (separable) characteristic polynomials of t_1 and t_2. It follows that the corresponding specializations of $D_{(f_1,\dots,f_r)}$ are conjugate to t_1 and t_2 over $\mathrm{GL}_n(\mathbb{F}_q((t)))$. However, it has to be checked by hand that they are also conjugate over $\mathcal{G}(\overline{\mathbb{F}}_q[[t]])$.

(3) Use Theorem 3.1.3 to get a fundamental solution matrix $Y \in \mathrm{GL}_n(L)$ for the difference module M over F that is given by $D_{(f_1,\dots,f_r)}$. In order to meet the assumptions of this theorem, the elements $f_1,\dots,f_r$ might have to be altered a little bit. This can be done for example by multiplying certain coefficients of $f_1,\dots,f_r$ by terms of small enough absolute value which do not change anything on the things we arranged in the previous point. For example, s^{q-1} might be a good candidate as it specializes to 1 whenever s is specialized to a non-zero element of $\mathbb{F}_q$ and it has valuation $(\frac{1}{2})^{q-1} < 1$.

(4) It follows from Theorem 1.2.11 that $E := F(Y)$ is a Picard-Vessiot extension for M. Our fundamental matrix Y provided by Theorem 3.1.3 is contained in $\mathrm{GL}_n(E \cap K[[t]])$ and should thus be contained in $\mathrm{GL}_n(\overline{\mathbb{F}_q(s)}^{\mathrm{sep}}[[t]])$, by Proposition 3.3.3. In particular, $E \subseteq \overline{\mathbb{F}_q(s)}^{\mathrm{sep}}((t))$ is separable over F by Proposition 5.2.1. Hence the Galois group scheme $\mathcal{H} := \mathcal{G}_{M,E}$ of M is a linear algebraic group (defined over $\mathbb{F}_q(t)$), by Theorem 1.3.10. Now use Theorem 3.2.4 to obtain that Y can be chosen inside $\mathcal{G}(E \cap K[[t]])$. In particular, $\mathcal{H}$ is a closed subgroup of $\mathcal{G}$ by Proposition 1.3.11.

(5) As Y is contained in $\mathcal{G}(K[[t]])$, the lower bound criterion 3.3.11 (applied to $\tilde{k} := K$) asserts that $\mathcal{H}$ contains a $\mathcal{G}(\overline{\mathbb{F}}_q[[t]])$-conjugates of T_1 and T_2 (as D specializes to $\mathcal{G}(\overline{\mathbb{F}}_q[[t]])$-conjugate of t_1 and t_2 which are

dense in T_1 and T_2, resp., and $\mathcal{H}$ is a closed subgroup of $\mathcal{G}$). By Proposition 4.4.3, $\mathcal{H}$ even contains $\mathcal{G}(\mathbb{F}_q + t\overline{\mathbb{F}}_q[[t]])$-conjugates of T_1 and T_2 if t_1 and t_2 were chosen such that the centralizers of their constant parts consists only of T_1 and T_2, resp. These conjugates generate $\mathcal{G}$, by Theorem 4.2.5, so we have $\mathcal{H} = \mathcal{G}$.

5.4 Special Linear Groups

For any elements $f_1, \dots, f_{n-1} \in F = \mathbb{F}_q(s,t)$, we set

$$D_{(f_1,\dots,f_{n-1})} = \begin{pmatrix} f_1 & \cdots & f_{n-1} & (-1)^{n-1} \\ 1 & & & \\ & \ddots & & \\ & & 1 & 0 \end{pmatrix} \in \mathrm{SL}_n(F).$$

This is by the way a generic element of the Steinberg cross section of SL_n with respect to the diagonal torus and the standard set of simple roots and root subgroups.
It is well known (and easy to check) that the characteristic polynomial of a matrix of this shape equals

$$X^n - f_1 X^{n-1} - \cdots - f_{n-1} X + (-1)^n. \tag{5.3}$$

Remark 5.4.1. *It is straightforward to compute that the equation*

$$D_{(f_1,\dots,f_{n-1})} \phi_q(Y) = Y$$

corresponds to the scalar difference equation

$$(-1)^{n-1} \phi_q^n(y) + \sum_{i=1}^{n-1} f_i \phi_q^i(y) - y = 0.$$

We proceed with a preliminary Lemma that will enable us to specialize $D_{(f_1,\dots,f_{n-1})}$ to a $\mathrm{SL}_n(\overline{\mathbb{F}}_q[[t]])$-conjugate of a regular diagonal matrix.

Lemma 5.4.2. *Let $p_1, \dots, p_n$ be elements in $\overline{\mathbb{F}}_q[[t]]$ such that their product equals 1 and their constant terms $\lambda_1, \dots, \lambda_n$ are pairwise distinct. Let further $h_1, \dots, h_{n-1} \in \overline{\mathbb{F}}_q[[t]]$ be defined via*

$$\prod_{i=1}^{n} (X - p_i) = X^n - h_1 X^{n-1} - \cdots - h_{n-1} X + (-1)^n.$$

Then $D_{(h_1,\dots,h_{n-1})}$ and $\mathrm{diag}(p_1, \dots, p_n)$ are conjugate over $\mathrm{SL}_n(\overline{\mathbb{F}}_q[[t]])$.

Proof. By construction, $D_{(h_1,\dots,h_{n-1})}$ and $\mathrm{diag}(p_1, \dots, p_n)$ have the same characteristic polynomial (see (5.3)). Note that all p_i are invertible inside $\overline{\mathbb{F}}_q[[t]]$, since their product equals 1. By Proposition 5.2.2, there exists a $C \in \mathrm{GL}_n(\overline{\mathbb{F}}_q[[t]])$ with $D^C_{(h_1,\dots,h_n)} = \mathrm{diag}(p_1, \dots, p_n)$. Then $B := C \cdot \mathrm{diag}(\det(C)^{-1}, 1 \dots, 1)$ is contained in $\mathrm{SL}_n(\overline{\mathbb{F}}_q[[t]])$ and $D_{(h_1,\dots,h_n)}$ and $\mathrm{diag}(p_1, \dots, p_n)$ are conjugate via B.

□

5.4.1 Dense Elements in T_1 and T_2

Recall that we fixed maximal tori T_1 and T_2 inside SL_n that are defined over $\mathbb{F}_q$. These were defined in 4.1.7 as $T_i = T_0^{g_i}$, where T_0 denotes the diagonal torus inside SL_n and g_i are contained in $\mathrm{SL}_n(\overline{\mathbb{F}}_q)$ such that $g_i\phi_q(g_i)^{-1} = w_i$ holds, where w_1 and w_2 were defined in Chapter 4 to be monomial matrices inside $\mathrm{SL}_n(\mathbb{F}_q)$ corresponding to the permutations

$$\begin{aligned}\sigma_1 &:= (1,2,\ldots,n)\\ \sigma_2 &:= (1,2,\ldots,n-1).\end{aligned}$$

Proposition 5.4.3. *Let $n \geq 2$ and assume $(n,q) \neq (2,2)$ and $(n,q) \neq (2,3)$. Set*

$\zeta_1 \in \mathbb{F}_{q^n}$ $\zeta_2 \in \mathbb{F}_{q^{n-1}}$	*primitive (q^n-1)-th root of unity* *primitive $(q^{n-1}-1)$-th root of unity*
$p_i \in \overline{\mathbb{F}}_q[t]_{(t)}$, $1 \leq i \leq n$ $\tilde{p}_i \in \overline{\mathbb{F}}_q[t]_{(t)}$, $1 \leq i \leq n$	$p_i := \frac{t+\zeta_1^{q^{i-1}}}{t+\zeta_1^{q^i}}$ $\tilde{p}_1 := t+\zeta_2,\ \tilde{p}_2 := t+\zeta_2^q, \ldots,\ \tilde{p}_{n-1} := t+\zeta_2^{q^{n-2}},$ $\tilde{p}_n := (\tilde{p}_1\cdots\tilde{p}_{n-1})^{-1}$
t_1 t_2	$t_1 := \mathrm{diag}(p_1,\ldots,p_n)^{g_1}$ $t_2 := \mathrm{diag}(\tilde{p}_1,\ldots,\tilde{p}_n)^{g_2}$

Then for $i = 1,2$, t_i is contained in $T_i(\mathbb{F}_q[[t]])$ and the centralizer of its constant part equals T_i. Moreover, t_i generates a dense subgroup of T_i ($i = 1,2$).

Proof. First of all, note that $\mathrm{diag}(p_1,\ldots,p_n)$ and $\mathrm{diag}(\tilde{p}_1,\ldots,\tilde{p}_n)$ are both of determinant one, so they are contained in T_0. The constant parts of the numerators and denominators of all p_j and $\tilde{p}_j$ are non-zero hence $p_1,\ldots,p_n$ as well as $\tilde{p}_1,\ldots,\tilde{p}_n$ are contained in $\overline{\mathbb{F}}_q[[t]]^\times$. Therefore, $\mathrm{diag}(p_1,\ldots,p_n)$ and $\mathrm{diag}(\tilde{p}_1,\ldots,\tilde{p}_n)$ are both contained in $T_0(\overline{\mathbb{F}}_q[[t]])$ which implies that t_1 and t_2 are contained in $T_1(\overline{\mathbb{F}}_q[[t]])$ and $T_2(\overline{\mathbb{F}}_q[[t]])$ (as $g_1, g_2 \in \mathrm{SL}_n(\overline{\mathbb{F}}_q)$).
Note that $\phi_q(p_1) = p_2,\ldots,\phi_q(p_{n-1}) = p_n, \phi_q(p_n) = p_1$ holds, as $\zeta_1^{q^n} = \zeta_1$. Hence

$$\begin{aligned}\phi_q(t_1) &= \mathrm{diag}(p_2,\ldots,p_n,p_1)^{\phi_q(g_1)} = \mathrm{diag}(p_2,\ldots,p_n,p_1)^{w_1^{-1}g_1}\\ &= \mathrm{diag}(p_1,\ldots,p_n)^{g_1} = t_1.\end{aligned}$$

Similarly, $\phi_q(t_2) = t_2$ holds, as $\phi_q(\tilde{p}_1) = \tilde{p}_2,\ldots,\phi_q(\tilde{p}_{n-1}) = \tilde{p}_1$ and $\phi_q(\tilde{p}_n) = \tilde{p}_n$. Hence t_i is contained in $T_i(\mathbb{F}_q[[t]])$ for $i = 1,2$.

Now the constant part of t_1 equals

$$t_{1,0} = \mathrm{diag}(\frac{\zeta_1}{\zeta_1^q},\ldots,\frac{\zeta_1^{q^{n-1}}}{\zeta_1})^{g_1} = \mathrm{diag}(\zeta_1^{1-q},\zeta_1^{q-q^2},\ldots,\zeta_1^{q^{n-2}-q^{n-1}},\zeta_1^{q^{n-1}-1})^{g_1}.$$

As ζ_1 is a primitive (q^n-1)-th root of unity, all entries of $t_{1,0}^{g_1^{-1}}$ are pairwise distinct which implies that only diagonal matrices can commute with it and

so the centralizer of $t_{1,0}$ equals $T_0^{g_1} = T_1$.
The constant part of t_2 equals

$$\begin{aligned} t_{2,0} &= \operatorname{diag}(\zeta_2, \zeta_2^q, \ldots, \zeta_2^{q^{n-2}}, \zeta_2^{-1-q-\cdots-q^{n-2}})^{g_2} \\ &= \operatorname{diag}(\zeta_2, \zeta_2^q, \ldots, \zeta_2^{q^{n-2}}, \zeta_2^{-\frac{q^{n-1}-1}{q-1}})^{g_2}. \end{aligned}$$

As ζ_2 is a primitive $(q^{n-1}-1)$-th root of unity, all elements $\zeta_2, \zeta_2^2, \ldots, \zeta_2^{q^{n-1}-1}$ are pairwise distinct. In particular, $\zeta_2, \zeta_2^q, \ldots, \zeta_2^{q^{n-2}}$ are pairwise distinct and every single one of them is a primitive $(q^{n-1}-1)$-th primitive root of unity, while $\zeta_2^{-\frac{q^{n-1}-1}{q-1}}$ is contained in $\mathbb{F}_q$. Thus all entries of $t_{2,0}^{g_2^{-1}}$ are pairwise distinct in case $n \geq 3$. If $n = 2$, we have $t_{2,0} = \operatorname{diag}(\zeta_2, \zeta_2^{-1})^{g_2}$ and $\zeta_2 \neq \zeta_2^{-1}$ since we assumed $(n, q) \neq (2, 3), (2, 2)$. We conclude that the centralizer of $t_{2,0}$ equals T_2.

It remains to show that t_i generates a dense subgroup of T_i for $i = 1, 2$. For $i = 1, 2$, t_i generates a dense subgroup of T_i if and only if $t_i^{g_i^{-1}}$ generates a dense subgroup of $T_i^{g_i^{-1}} = T_0$ which is the case if and only if no non-trivial character of T_0 maps $t_i^{g_i^{-1}}$ to 1, by Lemma 4.2.6. Any character of T_0 is of the form $\chi_1^{e_1} \ldots \chi_{n-1}^{e_{n-1}}$ for an $(e_1, \ldots, e_{n-1}) \in \mathbb{Z}^{n-1}$, where χ_i denotes the projection on the i-th diagonal entry. Assume that $\chi(t_1^{g_1^{-1}}) = 1$, i.e. $1 = \chi(\operatorname{diag}(p_1, \ldots, p_n)) = p_1^{e_1} \ldots p_{n-1}^{e_{n-1}}$. By definition of $p_1, \ldots, p_n$, this implies

$$(t + \zeta_1)^{e_1}(t + \zeta_1^q)^{e_2 - e_1} \cdots (t + \zeta_1^{q^{n-2}})^{e_{n-1} - e_{n-2}}(t + \zeta_1^{q^{n-1}})^{-e_{n-1}} = 1. \quad (5.4)$$

Now $\overline{\mathbb{F}}_q[t]$ is a factorial ring and the factors $(t + \zeta_1^{q^i})$ are pairwise coprime for $0 \leq i \leq n-1$, as ζ_1 is a $(q^n - 1)$-th primitive root of unity. We conclude that Equation (5.4) can only hold for $e_1 = \cdots = e_{n-1} = 0$, hence t_1 generates a dense subgroup of T_1. Similarly, t_2 spans a dense subgroup of T_2, as $\tilde{p}_1, \ldots, \tilde{p}_{n-1}$ are pairwise coprime polynomials in $\overline{\mathbb{F}}_q[t]$. □

5.4.2 A Difference Module for SL_n

The aim is now to define suitable $f_1, \ldots, f_{n-1}$ such that $D_{(f_1, \ldots, f_{n-1})}$ gives rise to a difference module with Galois group scheme SL_n.

n q α	$n \geq 2$ prime power such that $q \neq 2$ and $(n,q) \neq (2,3)$ a fixed element in $\mathbb{F}_q^\times \backslash \{1\}$ (e.g. $\alpha = -1$ if q is odd)
$\zeta_1 \in \mathbb{F}_{q^n}$ $\zeta_2 \in \mathbb{F}_{q^{n-1}}$	primitive (q^n-1)-th root of unity primitive $(q^{n-1}-1)$-th root of unity
$p_i \in \overline{\mathbb{F}}_q[t]_{(t)}$ $\tilde{p}_i \in \overline{\mathbb{F}}_q[t]_{(t)}$	$p_1 := \frac{t+\zeta_1}{t+\zeta_1^q},\ p_2 := \frac{t+\zeta_1^q}{t+\zeta_1^{q^2}}, \ldots,\ p_n := \frac{t+\zeta_1^{q^{n-1}}}{t+\zeta_1}$ $\tilde{p}_1 := t+\zeta_2,\ \tilde{p}_2 := t+\zeta_2^q, \ldots,\ \tilde{p}_{n-1} := t+\zeta_2^{q^{n-2}},$ $\tilde{p}_n := (\tilde{p}_1 \cdots \tilde{p}_{n-1})^{-1}$
$h_i \in \mathbb{F}_q[t]_{(t)}$ $\tilde{h}_i \in \mathbb{F}_q[t]_{(t)}$	defined via $\prod_{i=1}^{n}(X-p_i) = X^n - \sum_{i=1}^{n-1} h_i X^{n-i} + (-1)^n$ defined via $\prod_{i=1}^{n}(X-\tilde{p}_i) = X^n - \sum_{i=1}^{n-1} \tilde{h}_i X^{n-i} + (-1)^n$
$a_{ij}, b_{ij} \in \mathbb{F}_q$ $\tilde{a}_{ij}, \tilde{b}_{ij} \in \mathbb{F}_q$	coefficients of h_i: $h_i(t) = \frac{\sum_{j=0}^{n} a_{ij}t^j}{\sum_{j=0}^{n} b_{ij}t^j}$; $b_{i0} \neq 0$ for all i coefficients of $\tilde{h}_i$: $\tilde{h}_i(t) = \frac{\sum_{j=0}^{2n-2} \tilde{a}_{ij}t^j}{\sum_{j=0}^{n-1} \tilde{b}_{ij}t^j}$; $\tilde{b}_{i0} \neq 0$ for all i
$H_i \in \mathbb{F}_q(t,s)$ $\tilde{H}_i \in \mathbb{F}_q(t,s)$	$H_i := \frac{s\sum_{j=0}^{n} a_{ij}t^j}{b_{i0}+s\sum_{j=1}^{n} b_{ij}t^j},\ 1 \leq i \leq n-1$ $\tilde{H}_i := \frac{\frac{s}{\alpha}\sum_{j=0}^{2n-2} \tilde{a}_{ij}t^j}{\tilde{b}_{i0}+\frac{s}{\alpha}\sum_{j=1}^{n-1} \tilde{b}_{ij}t^j},\ 1 \leq i \leq n-1$
$f_i \in F$	$f_i := \frac{s-\alpha}{1-\alpha}H_i + \frac{s-1}{\alpha-1}\tilde{H}_i,\ 1 \leq i \leq n-1$

Table 5.1: Definition of $f_1, \ldots, f_{n-1}$.

Note that h_i and $\tilde{h}_i$ are contained in $\mathbb{F}_q[t]_{(t)}$ by the choice of ζ_i. Indeed, h_i are the coefficients of the characteristic polynomial of $t_1 \in T_1(\mathbb{F}_q[[t]])$ as in Proposition 5.4.3 and similarly for $\tilde{h}_i$.

Theorem 5.4.4. *Assume $q > 2$ and $n \geq 2$ such that $(n,q) \neq (2,3)$. Let $M = (F^n, \Phi)$ be the ϕ_q-difference module over $F = \mathbb{F}_q(s,t)$ given by $D_{(f_1,\ldots,f_{n-1})}$, where $f_i \in F$ are as defined in Table 5.1. Then there exists a Picard-Vessiot ring $R \subseteq \overline{\mathbb{F}_q(s)}^{\mathrm{sep}}((t)) \cap L$ for M such that R/F is separable and the Galois group scheme $\mathcal{G}_{M,R}$ of M with respect to R is isomorphic to SL_n (as linear algebraic group over $\mathbb{F}_q(t)$).*

Proof. We abbreviate $D := D_{(f_1,\ldots,f_{n-1})}$. Let $\mathcal{O}_{|\cdot|} \subseteq K$ denote the valu-

ation ring corresponding to $|\cdot|$ with maximal ideal $\mathfrak{m} \subseteq \mathcal{O}_{|\cdot|}$. All non-constant coefficients of the numerators and denominators of H_i and $\tilde{H}_i$ $(1 \leq i \leq n-1)$ are contained in $\mathfrak{m}$ and the constant coefficients of the denominators are contained in $\mathbb{F}_q^\times \subseteq \mathcal{O}_{|\cdot|}^\times$, so it follows from Lemma 3.1.4 that all H_i and $\tilde{H}_i$ are contained in $\mathcal{O}_{|\cdot|}[[t]]$ and their j-th coefficients can be bounded by δ^j for a suitable $\delta < 1$. Hence the same is true for all f_i, $1 \leq i \leq n-1$. We conclude $D = \sum_{l=0}^{\infty} D_l t^l \in \mathrm{SL}_n(\mathcal{O}_{|\cdot|}[[t]])$ satisfies $||D_l|| \leq \delta^l$ for all $l \in \mathbb{N}$. By Theorem 3.1.3, there exists a fundamental solution matrix $Y = \sum_{l=0}^{\infty} Y_l t^l \in \mathrm{GL}_n(L \cap K[[t]])$ satisfying $||Y_l|| \leq \delta^l$, i.e., $Y \in \mathrm{M}_n(\mathcal{O}_{|\cdot|}\{t\})$. Let $E = F(Y)$ be the field generated by the entries of Y. Then $E \subseteq L$, hence $C_E = C_F$ and $R := F[Y, Y^{-1}] \subseteq E$ is a Picard-Vessiot ring for M by Theorem 1.2.11.

Consider $\mathfrak{o} := \mathcal{O}_{|\cdot|} \cap k = \mathbb{F}_q[s]_{(s)}$ and $\mathcal{O} := \mathcal{O}_{|\cdot|} \cap \overline{k}^{\mathrm{sep}}$ (with respect to a fixed embedding of $\overline{k}^{\mathrm{sep}} = \overline{\mathbb{F}_q(s)}^{\mathrm{sep}}$ into K). Let $\mathfrak{p} = (s)$ denote the maximal ideal inside $\mathfrak{o}$. Then $\mathfrak{o}/\mathfrak{p} \cong \mathbb{F}_q$. Therefore, $\mathfrak{o}$ and $\mathcal{O}$ conform to all assumptions made in 3.3.1 hence we can apply Proposition 3.3.3 c) (with $\tilde{k} := K$) to conclude that Y is contained in $\mathrm{GL}_n(\mathcal{O}[[t]])$. In particular, all entries of Y are contained in $\overline{\mathbb{F}_q(s)}^{\mathrm{sep}}((t))$, hence R/F is separable by Proposition 5.2.1. Also, Y is contained in $\mathrm{GL}_n(\mathcal{O}_{|\cdot|}[[t]]) \cap \mathrm{M}_n(\mathcal{O}_{|\cdot|}\{t\})$, so we may assume that Y is contained in $\mathrm{SL}_n(L \cap K[[t]])$, by Theorem 3.2.4. Indeed, $\mathcal{O}_{|\cdot|}/\mathfrak{m} \cong \overline{\mathbb{F}}_q \subseteq K$, $D \in \mathrm{SL}_n(\mathcal{O}_{|\cdot|}[[t]])$ and $\kappa_{|\cdot|}(D) = D_{(0,\ldots,0)} \in \mathrm{SL}_n(\mathbb{F}_q) \subseteq \mathrm{SL}_n(\mathcal{O}_{|\cdot|}/\mathfrak{m})$ (the latter follows from $\kappa_{|\cdot|}(H_i) = \kappa_{|\cdot|}(\tilde{H}_i) = 0$ for all $i \leq n-1$).

We conclude that the Galois group scheme $\mathcal{H} := \mathcal{G}_{M,R}$ of (M, Φ) is a linear algebraic group (see Theorem 1.3.10) defined over $\mathbb{F}_q(t)$ that is a closed subgroup of SL_n (see Proposition 1.3.11). We will now use the lower bound criterion 3.3.11 to show that $\mathcal{H}$ is all of SL_n.

Consider $\mathfrak{p}_1 = (s-1) \subseteq \mathfrak{o}_1 := \mathbb{F}_q[s]_{(s-1)}$ and $\mathfrak{p}_2 = (s-\alpha) \subseteq \mathfrak{o}_2 := \mathbb{F}_q[s]_{(s-\alpha)}$. Then $\mathfrak{o}_1$ and $\mathfrak{o}_2$ are valuation rings inside $k = \mathbb{F}_q(s)$ with $\mathfrak{o}_1/\mathfrak{p}_1 \cong \mathbb{F}_q$ and $\mathfrak{o}_2/\mathfrak{p}_2 \cong \mathbb{F}_q$. Fix extensions $(\mathcal{O}_j, \mathcal{P}_j)$ of $(\mathfrak{o}_j, \mathfrak{p}_j)$ to $\overline{k}^{\mathrm{sep}} = \overline{\mathbb{F}_q(s)}^{\mathrm{sep}}$ $(j = 1, 2)$. These valuation rings conform to all assumptions made in 3.3.1 and we may thus apply the results from Section 3.3. Note that $H_i \in \mathfrak{o}_j[[t]]$ for all $1 \leq i \leq n-1$, $j = 1, 2$ since the numerators are contained in $\mathfrak{o}_j[t]$ and the denominators are contained in $\mathfrak{o}_j[t]$ with constant coefficient $b_{i0} \in \mathbb{F}_q^\times \subseteq \mathfrak{o}_j^\times$. Similarly, all $\tilde{H}_i$ and thus all f_i are contained in $\mathfrak{o}_j[[t]]$. Hence D is contained in $\mathrm{SL}_n(\mathfrak{o}_j[[t]])$ for both $j = 1, 2$. Therefore, we can apply Corollary 3.3.11 (with $\mathcal{G} := \mathrm{SL}_n$ and $\tilde{k} := K$) to conclude that $\mathcal{H}(\mathbb{F}_q[[t]])$ contains $\mathrm{SL}_n(\overline{\mathbb{F}}_q[[t]])$-conjugates of $\kappa_1(D)$ and $\kappa_2(D)$, where $\kappa_j \colon \mathfrak{o}_j[[t]] \to \mathbb{F}_q[[t]]$ denotes the coefficient-wise reduction mod $\mathfrak{p}_j$.

Specializing $s \mapsto 1$ maps f_i to h_i $(1 \leq i \leq n-1)$, thus $\kappa_1(D) = D_{(h_1,\ldots,h_{n-1})}$. Similarly, $\kappa_2(D) = D_{(\tilde{h}_1,\ldots,\tilde{h}_{n-1})}$ as specializing $s \mapsto \alpha$ maps f_i to $\tilde{h}_i$. Set

$$\begin{aligned} d_1 &:= \operatorname{diag}(p_1, \ldots, p_n) \\ d_2 &:= \operatorname{diag}(\tilde{p}_1, \ldots, \tilde{p}_n). \end{aligned}$$

and $t_1 = d_1^{g_1}$, $t_2 = d_2^{g_2}$ with $g_1, g_2 \in \mathrm{SL}_n(\overline{\mathbb{F}}_q)$ as in Proposition 5.4.3. The constant parts of $p_1, \ldots, p_n$ are pairwise distinct by Proposition 5.4.3, hence $\kappa_1(D)$ is conjugate to d_1 over $\mathrm{SL}_n(\overline{\mathbb{F}}_q[[t]])$, by Lemma 5.4.2. Similarly, $\kappa_2(D)$ is conjugate to d_2 over $\mathrm{SL}_n(\overline{\mathbb{F}}_q[[t]])$. It follows that $\mathcal{H}(\mathbb{F}_q[[t]])$ contains $\mathrm{SL}_n(\overline{\mathbb{F}}_q[[t]])$-conjugates of $d_1 = t_1^{g_1^{-1}}$ and $d_2 = t_1^{g_2^{-1}}$. Therefore, $\mathcal{H}(\mathbb{F}_q[[t]])$ also contains $\mathrm{SL}_n(\overline{\mathbb{F}}_q[[t]])$-conjugates x_1 and x_2 of t_1 and t_2 which are both contained in $\mathrm{SL}_n(\mathbb{F}_q[[t]])$ (see Proposition 5.4.3). By Proposition 4.4.3 together with Proposition 5.4.3, there exist A_1 and A_2 contained in $\mathrm{SL}_n(\mathbb{F}_q + t\overline{\mathbb{F}}_q[[t]])$ with $x_j = t_j^{A_j}$ $(j = 1, 2)$. Now $\mathcal{H}$ is a closed subgroup of SL_n and t_1 and t_2 generate dense subgroups of T_1 and T_2 by Proposition 5.4.3, so $\mathcal{H}$ contains $< T_1^{A_1}, T_2^{A_2} >$. For $n \geq 3$, Theorem 4.2.5 implies $< T_1^{A_1}, T_2^{A_2} >= \mathrm{SL}_n$, hence $\mathcal{H} = \mathrm{SL}_n$.

In case $n = 2$, we either have $< T_1^{A_1}, T_2^{A_2} >= \mathrm{SL}_2$ or $< T_1^{A_1}, T_2^{A_2} >$ is solvable (since $< T_1^{A_1}, T_2^{A_2} >$ is connected and every two dimensional Lie algebra is solvable). Assume that $< T_1^{A_1}, T_2^{A_2} >$ is solvable. Then there exists a $C \in \mathrm{GL}_2(\overline{\mathbb{F}_q((t))})$ such that $< T_1^{A_1}, T_2^{A_2} >^C$ is contained in $\mathcal{B}_2$, the group of upper triangular matrices inside SL_2. Note that up to conjugacy over $\mathrm{SL}_2(\mathbb{F}_q)$, T_2 equals the diagonal torus T_0 inside SL_2 since $\sigma_2 \in S_2$ is trivial in case $n = 2$. By multiplying A_2 from the left with a suitable element in $\mathrm{SL}_2(\mathbb{F}_q)$, we may assume $T_2 = T_0$ and conclude that $T_0^{A_2 C}$ is contained in $\mathcal{B}_2$. Hence $T_0^{A_2 C}$ is a maximal torus of $\mathcal{B}_2$, so there exist a $b \in \mathcal{B}_2(\overline{\mathbb{F}_q((t))})$ such that $T_0^{A_2 C} = T_0^b$. Therefore, $A_2 C b^{-1}$ is a monomial matrix inside GL_2 and can thus be written as $A_2 C b^{-1} = w t_0$ for a monomial matrix $w \in \mathrm{SL}_2(\mathbb{F}_q)$ and a diagonal matrix $t_0 \in \mathrm{GL}_2(\overline{\mathbb{F}_q((t))})$. Hence $C = A_2^{-1} w t_0 b$ and it follows that $< T_1^{A_1}, T_2^{A_2} >^{A_2^{-1} w}$ is contained in $\mathcal{B}_2^{b^{-1} t_0^{-1}} = \mathcal{B}_2$. In particular, $t_1^{A_1 A_2^{-1} w}$ is contained in $\mathcal{B}_2$, and as $A_1, A_2 \in \mathrm{SL}_2(\mathbb{F}_q + t\overline{\mathbb{F}}_q[[t]])$, $w \in \mathrm{SL}_2(\mathbb{F}_q)$ and $t_1 \in \mathrm{SL}_2(\mathbb{F}_q[[t]])$, we conclude that $t_1^{A_1 A_2^{-1} w}$ is contained in $\mathcal{B}_2(\mathbb{F}_q + t\overline{\mathbb{F}}_q[[t]])$. It follows that the constant part of $t_1^{A_1 A_2^{-1} w}$ is contained in $\mathcal{B}_2(\mathbb{F}_q)$. Now the constant term of $t_1^{A_1 A_2^{-1} w}$ is conjugate to the constant term of t_1 (see Lemma 4.2.1 b)) and the constant term of t_1 equals $\operatorname{diag}(\zeta_1^{1-q}, \zeta_1^{-1+q})^{g_1}$ (see the proof of Proposition 5.4.3). Hence $\mathcal{B}_2(\mathbb{F}_q)$ contains an element of order $q+1$ since ζ_1 is a primitive (q^2-1)-th root of unity. This contradicts the fact that the order of $\mathcal{B}_2(\mathbb{F}_q)$ equals $q \cdot (q-1)$. □

Remark 5.4.5. *We have to assume $q \neq 2$, since otherwise there are only two possible specializations $s \mapsto 1$ and $s \mapsto 0$ and the latter would only*

give us an element of finite order (as D has to specialize to an element in $\mathrm{GL}_n(\mathbb{F}_q)$ to conform to the assumptions of Theorem 3.1.3).

5.5 Symplectic Groups

In this section we let $n = 2d$ be even and consider the symplectic group $\mathcal{G} = \mathrm{Sp}_{2d}$ with respect to the symplectic form given by

$$J = \left(\begin{array}{ccc|ccc} & & & & & -1 \\ & & & & \iddots & \\ & & & -1 & & \\ \hline & & 1 & & & \\ & \iddots & & & & \\ 1 & & & & & \end{array}\right).$$

For any elements $f_1, \ldots, f_d \in F = \mathbb{F}_q(s,t)$, we set

$$D_{(f_1,\ldots,f_d)} = \left(\begin{array}{cccc|cccc} f_1 & \cdots & f_{d-1} & f_d & 1 & & & \\ 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & 0 & & & & \\ \hline & & & f_{d-1} & 0 & 1 & & \\ & & & \vdots & \vdots & & \ddots & \\ & & & f_1 & 0 & & & 1 \\ & & & -1 & 0 & & & 0 \end{array}\right).$$

It is easily seen that $D_{(f_1,\ldots,f_d)}$ is symplectic (in fact, it is a generic element in the Steinberg cross section of Sp_{2d} with respect to the diagonal torus) and its characteristic polynomial equals

$$g(X) = X^{2d} - \sum_{i=1}^{d-1} f_i X^{2d-i} - f_d X^d - \sum_{i=1}^{d-1} f_i X^i + 1. \tag{5.5}$$

(A proof can be found in [AM10, 4.2.]).

5.5.1 Specializations of $D_{(f_1,\ldots,f_d)}$

Recall that the diagonal matrices contained in Sp_{2d} are exactly those of the form $\mathrm{diag}(\lambda_1, \ldots, \lambda_d, \lambda_d^{-1}, \ldots, \lambda_1^{-1})$ for non-zero elements $\lambda_1, \ldots, \lambda_d$. The coefficients of the characteristic polynomial of such an element are palindromic in the following way:

Lemma 5.5.1. *Let $\mathbb{F}$ be a field and let $\lambda_1, \ldots, \lambda_d$ be non-zero elements in $\mathbb{F}$. Consider the diagonal matrix*

$$A := \mathrm{diag}(\lambda_1, \ldots, \lambda_d, \lambda_d^{-1}, \ldots, \lambda_1^{-1}) \in \mathrm{SL}_{2d}(\mathbb{F}).$$

Then the characteristic polynomial of A is of the form

$$X^{2d} + a_1X^{2d-1} + \cdots + a_{d-1}X^{d+1} + a_dX^d + a_{d-1}X^{d-1} + \cdots + a_1X + 1$$

for some $a_1, \ldots, a_d \in \mathbb{F}$.

Proof. Let $a_i \in \mathbb{F}$ denote the coefficient of X^i in the characteristic polynomial of A, for $1 \leq i \leq 2d-1$. We have to show that

$$a_i = a_{2d-i}$$

holds for all $1 \leq i \leq d-1$. Now $(-1)^i a_i = (-1)^{2d-i} a_i$ is the sum of all products of $2d-i$ elements out of $\lambda_1, \ldots, \lambda_d, \lambda_d^{-1}, \ldots, \lambda_1^{-1}$. By multiplying by $1 = \lambda_1 \cdots \lambda_d \lambda_d^{-1} \cdots \lambda_1^{-1}$, it is easy to see that this is also the sum of all products of i elements out of $\lambda_1, \ldots, \lambda_d, \lambda_d^{-1}, \ldots, \lambda_1^{-1}$, that is, $(-1)^i a_i = (-1)^i a_{2d-i}$, so we have $a_i = a_{2d-i}$. □

Lemma 5.5.2. *Let $p_1, \ldots, p_d$ be elements in $\overline{\mathbb{F}}_q[[t]]^\times$ such that the constant terms of $p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1}$ are pairwise distinct elements in $\overline{\mathbb{F}}_q^\times$. Let $h_1, \ldots, h_d \in \overline{\mathbb{F}}_q[[t]]$ be defined via*

$$\prod_{i=1}^{d}(X - p_i)(X - p_i^{-1}) = X^{2d} - \sum_{i=1}^{d-1} h_i X^{2d-i} - h_d X^d - \sum_{i=1}^{d-1} h_i X^i + 1. \quad (5.6)$$

Then $D_{(h_1,\ldots,h_d)}$ and $\mathrm{diag}(p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1})$ are conjugate over $\mathrm{Sp}_{2d}(\overline{\mathbb{F}}_q[[t]])$.

Proof. We abbreviate $\mathcal{G} = \mathrm{Sp}_{2d}$. The elements $h_1, \ldots, h_d$ exist inside $\overline{\mathbb{F}}_q((t))$ by Lemma 5.5.1, and as they are constructed as sums of products of the elements $p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1}$, they are also contained in $\overline{\mathbb{F}}_q[[t]]$.

By the choice of h_i together with Equation (5.5), the characteristic polynomial of $D_{(h_1,\ldots,h_d)}$ equals $\prod_{i=1}^{d}(X - p_i)(X - p_i^{-1})$ and is thus separable. Hence $D_{(h_1,\ldots,h_d)}$ is a semisimple element of $\mathcal{G}(\overline{\mathbb{F}_q((t))})$. It follows that there exists a maximal torus T containing $D_{(h_1,\ldots,h_d)}$. All maximal tori of $\mathcal{G}(\overline{\mathbb{F}_q((t))})$ are conjugate, hence there exists an element $g \in \mathcal{G}(\overline{\mathbb{F}_q((t))})$ such that T^g equals the diagonal torus T_0 inside $\mathcal{G}$. It follows that $t_0 := D_{(h_1,\ldots,h_d)}^g$ is diagonal. We relabel $p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1}$ as $p_1, \ldots, p_d, p_{d+1}, \ldots, p_{2d}$. Then $p_1, \ldots, p_{2d}$ are the $2d$ pairwise distinct eigenvalues of t_0. It follows that there exists a permutation $\sigma \in S_{2d}$ such that $t_0 = \mathrm{diag}(p_{\sigma(1)}, \ldots, p_{\sigma(2d)})$ holds. Now t_0 is symplectic, so we have $p_{\sigma(i)} = p_{\sigma(2d+1-i)}^{-1}$ for all $1 \leq i \leq d$. On the other hand, $p_1, \ldots, p_{2d}$ are pairwise distinct and $p_i = p_{2d+1-i}^{-1}$ holds for all $1 \leq i \leq d$. It follows that $\sigma(2d+1-i) = 2d+1-\sigma(i)$ holds for all $1 \leq i \leq d$. Therefore, σ gives rise to a symplectic permutation matrix

$A_\sigma \in \mathcal{G}(\mathbb{F}_q)$, by Lemma 4.1.5. By multiplying g with A_σ^{-1} from the right, we may assume that t_0 equals $\mathrm{diag}(p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1})$.

So far, we have seen that there exists a $g \in \mathcal{G}(\overline{\mathbb{F}_q((t))})$ satisfying $D^g_{(h_1,\ldots,h_d)} = \mathrm{diag}(p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1}) =: t_0$. We would like to show that g can be chosen inside $\mathcal{G}(\overline{\mathbb{F}}_q[[t]])$. Proposition 5.2.2 implies that there exists a $C \in \mathrm{GL}_n(\overline{\mathbb{F}}_q[[t]])$ with $D^C_{(h_1,\ldots,h_d)} = \mathrm{diag}(p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1}) = t_0$, since $p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1}$ have pairwise distinct constant terms. Hence $C^{-1}g$ is contained in the centralizer of t_0 inside GL_n which only consists of diagonal matrices (since the diagonal entries of t_0 are pairwise distinct). Let $x_1, \ldots, x_{2d} \in \overline{\mathbb{F}_q((t))}^\times$ be such that $g = C \cdot \mathrm{diag}(x_1, \ldots, x_{2d})$ holds.

By multiplying g from the right with $\mathrm{diag}(x_{2d}, \ldots, x_{d+1}, x_{d+1}^{-1}, \ldots, x_{2d}^{-1}) \in \mathcal{G}(\overline{\mathbb{F}_q((t))})$, we may assume that $C = g \cdot \mathrm{diag}(\alpha_1, \ldots, \alpha_d, 1 \ldots, 1)$ holds for some elements $\alpha_i \in \overline{\mathbb{F}_q((t))}^\times$. We now use that g is symplectic to compute

$$\begin{aligned} C^{\mathrm{tr}} JC &= \mathrm{diag}(\alpha_1, \ldots, \alpha_d, 1 \ldots, 1) g^{\mathrm{tr}} J g \, \mathrm{diag}(\alpha_1, \ldots, \alpha_d, 1 \ldots, 1) \\ &= \mathrm{diag}(\alpha_1, \ldots, \alpha_d, 1 \ldots, 1) J \, \mathrm{diag}(\alpha_1, \ldots, \alpha_d, 1 \ldots, 1) \\ &= \left(\begin{array}{ccc|ccc} & & & & & -\alpha_1 \\ & & & & \iddots & \\ & & & -\alpha_d & & \\ \hline & & \alpha_d & & & \\ & \iddots & & & & \\ \alpha_1 & & & & & \end{array}\right), \end{aligned} \tag{5.7}$$

so all entries of $C^{\mathrm{tr}} JC$ away from the "reversed diagonal" (by which we mean the $(i, 2d+1-i)$-th coordinates, $1 \leq i \leq 2d$) are zero, that is, C is already quite close to being symplectic. Equation (5.7) implies that all α_i are contained in $\overline{\mathbb{F}}_q[[t]]$, as all entries of C and J are. On the other hand, g has determinant 1 (as $\mathrm{Sp}_{2d} \leq \mathrm{SL}_{2d}$), so $C = g \cdot \mathrm{diag}(\alpha_1, \ldots, \alpha_d, 1 \ldots, 1)$ implies $\alpha_1 \cdots \alpha_d = \det(C) \in \overline{\mathbb{F}}_q[[t]]^\times$. Hence $\alpha_1, \ldots, \alpha_d$ are all contained in $\overline{\mathbb{F}}_q[[t]]^\times$. It follows that all entries of $g = C \cdot \mathrm{diag}(\alpha_1^{-1}, \ldots, \alpha_d^{-1}, 1, \ldots, 1)$ are contained in $\overline{\mathbb{F}}_q[[t]]$, thus $g \in \mathcal{G}(\overline{\mathbb{F}}_q[[t]])$. □

5.5.2 Dense Elements in T_1 and T_2

Proposition 5.5.3. *Let $n = 2d \geq 4$ such that $(n, q) \neq (4, 2)$. Let $T_0 \leq \mathrm{Sp}_{2d}$ be the diagonal torus and let $T_1 = T_0^{g_1}$ and $T_2 = T_0^{g_2}$ be the maximal tori of Sp_{2d} defined over $\mathbb{F}_q$ as in Definition 4.1.7. Consider*

$\zeta_1 \in \mathbb{F}_{q^{2d}}$ $\zeta_2 \in \mathbb{F}_{q^d}$	*primitive* $(q^{2d}-1)$*-th root of unity* *primitive* (q^d-1)*-th root of unity*
$p_i \in \overline{\mathbb{F}}_q[t]_{(t)}$, $1 \leq i \leq d$ $\tilde{p}_i \in \overline{\mathbb{F}}_q[t]_{(t)}$, $1 \leq i \leq d$	$p_1 := \frac{t+\zeta_1}{t+\zeta_1^{q^d}},\ p_2 := \frac{t+\zeta_1^q}{t+\zeta_1^{q^{d+1}}}, \ldots,\ p_d := \frac{t+\zeta_1^{q^{d-1}}}{t+\zeta_1^{q^{2d-1}}}$ $\tilde{p}_1 := t+\zeta_2,\ \tilde{p}_2 := t+\zeta_2^q, \ldots,\ \tilde{p}_d := t+\zeta_2^{q^{d-1}}$
t_1 t_2	$t_1 := \mathrm{diag}(p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1})^{g_1}$ $t_2 := \mathrm{diag}(\tilde{p}_1, \ldots, \tilde{p}_d, \tilde{p}_d^{-1}, \ldots, \tilde{p}_1^{-1})^{g_2}$

Then t_i is contained in $T_i(\mathbb{F}_q[[t]])$ and the centralizer of its constant part equals T_i. Moreover, t_i generates a dense subgroup of T_i $(i = 1, 2)$.

Proof. First of all, note that $\mathrm{diag}(p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1})$ and $\mathrm{diag}(\tilde{p}_1, \ldots, \tilde{p}_d, \tilde{p}_d^{-1}, \ldots, \tilde{p}_1^{-1})$ are both contained in $T_0 \leq \mathrm{Sp}_{2d}$. For $i = 1, 2$, g_i is contained in $\mathrm{Sp}_{2d}(\overline{\mathbb{F}}_q)$ and $p_1, \ldots, p_d$ as well as $\tilde{p}_1, \ldots, \tilde{p}_d$ are contained in $\overline{\mathbb{F}}_q[[t]]^\times$ (as the constant parts of numerators and denominators are all non-zero) hence t_i is contained in $T_i(\overline{\mathbb{F}}_q[[t]])$.
Recall that $g_i \phi_q(g_i)^{-1} = w_i$ holds, where w_1 and w_2 were defined in Chapter 4 to be monomial matrices inside $\mathrm{Sp}_{2d}(\mathbb{F}_q)$ corresponding to the permutations

$$\begin{aligned} \sigma_1 &:= (1, \ldots, d, 2d, \ldots, d+1) \\ \sigma_2 &:= (1, \ldots, d)(2d, \ldots, d+1). \end{aligned}$$

Relabel $p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1}$ by $p_1, \ldots, p_{2d}$. Then $\zeta_1^{q^{2d}} = \zeta_1$ implies $\phi_q(p_1) = p_2, \ldots, \phi_q(p_{d-1}) = p_d$, $\phi_q(p_d) = p_{2d}$, $\phi_q(p_{2d}) = p_{2d-1}, \ldots,$ $\phi_q(p_{d+2}) = p_{d+1}$, $\phi_q(p_{d+1}) = p_1$. Hence

$$\begin{aligned} \phi_q(t_1) &= \mathrm{diag}(p_2, \ldots, p_d, p_{2d}, p_1, p_{d+1}, \ldots, p_{2d-1})^{\phi_q(g_1)} \\ &= \mathrm{diag}(p_{\sigma_1(1)}, \ldots, p_{\sigma_1(2d)})^{w_1^{-1} g_1} \\ &= \mathrm{diag}(p_1, \ldots, p_n)^{g_1} \\ &= t_1. \end{aligned}$$

Similarly, $\phi_q(t_2) = t_2$ holds, as ϕ_q permutes the entries of $\mathrm{diag}(\tilde{p}_1, \ldots, \tilde{p}_d, \tilde{p}_d^{-1}, \ldots, \tilde{p}_1^{-1})$ as indicated by σ_2. Hence t_i is contained in $T_i(\mathbb{F}_q[[t]])$ for $i = 1, 2$.

Now the constant part of t_1 equals

$$t_{1,0} = \mathrm{diag}(\zeta_1^{1-q^d}, \zeta_1^{q-q^{d+1}}, \ldots, \zeta_1^{q^{d-1}-q^{2d-1}}, \zeta_1^{q^{2d-1}-q^{d-1}}, \ldots, \zeta^{q^d-1})^{g_1}.$$

Using that ζ_1 is a primitive $(q^{2d}-1)$-th root of unity, it is easy to see that all elements $\zeta_1^{1-q^d}, \ldots, \zeta_1^{q^{d-1}-q^{2d-1}}, \zeta_1^{q^{2d-1}-q^{d-1}}, \ldots, \zeta^{q^d-1}$ are pairwise distinct, hence only diagonal matrices commute with $t_{1,0}^{g_1^{-1}}$ which implies that the centralizer of $t_{1,0}$ equals T_1.
The constant part of t_2 equals

$$t_{2,0} = \mathrm{diag}(\zeta_2, \zeta_2^q, \ldots, \zeta_2^{q^{d-1}}, \zeta_2^{-q^{d-1}}, \ldots, \zeta_2^{-1})^{g_2}.$$

As ζ_2 is a primitive (q^d-1)-th root of unity, all eigenvalues of $t_{2,0}$ are pairwise distinct (here we used $(n,q) \neq (4,2)$), hence the centralizer of $t_{2,0}$ equals T_2.

It remains to show that t_i generates a dense subgroup of T_i for $i = 1, 2$. For $i = 1, 2$, $<t_i>$ is dense in T_i if and only if $<t_i^{g_i^{-1}}>$ is dense in $T_i^{g_i^{-1}} = T_0$ which is the case if and only if no non-trivial character of T_0 maps $t_i^{g_i^{-1}}$ to 1, by Lemma 4.2.6. Any character of T_0 is of the form $\chi_1^{e_1} \dots \chi_d^{e_d}$ for an $(e_1, \dots, e_d) \in \mathbb{Z}^d$, where χ_i denotes the projection on the i-th diagonal entry. Assume that $\chi(t_1^{g_1^{-1}}) = 1$, i.e., $1 = \chi(\mathrm{diag}(p_1, \dots, p_d, p_d^{-1}, \dots, p_1^{-1})) = p_1^{e_1} \dots p_d^{e_d}$. By definition of $p_1, \dots, p_d$, this implies

$$(t+\zeta_1)^{e_1}(t+\zeta_1^q)^{e_2} \cdots (t+\zeta_1^{q^{d-1}})^{e_d}(t+\zeta_1^{q^d})^{-e_1}(t+\zeta_1^{q^{d+1}})^{-e_2} \cdots (t+\zeta_1^{q^{2d-1}})^{-e_d} = 1. \tag{5.8}$$

Now $\overline{\mathbb{F}}_q[t]$ is a factorial ring and $(t+\zeta_1^{q^i})$ are pairwise coprime for $0 \leq i \leq 2d-1$, as ζ_1 is a $(q^{2d}-1)$-th primitive root of unity. We conclude that Equation (5.8) can only hold for $e_1 = \dots = e_d = 0$, hence t_1 generates a dense subgroup of T_1. Similarly, t_2 spans a dense subgroup of T_2, as $\tilde{p}_1, \dots, \tilde{p}_d$ are pairwise coprime polynomials in $\overline{\mathbb{F}}_q[t]$. □

5.5.3 A Difference Module for Sp_{2d}

We can now define the elements $f_1, \dots, f_d \in F$ in a similar way as in the special linear case:

n	$n = 2d \geq 4$
q	prime power such that $q > 2$
α	a fixed element in $\mathbb{F}_q^\times \backslash \{1\}$ (e.g. $\alpha = -1$ if q is odd)
$\zeta_1 \in \mathbb{F}_{q^{2d}}$	primitive $(q^{2d}-1)$-th root of unity
$\zeta_2 \in \mathbb{F}_{q^d}$	primitive (q^d-1)-th root of unity
$p_i \in \overline{\mathbb{F}}_q[t]^\times_{(t)}$	$p_1 := \frac{t+\zeta_1}{t+\zeta_1^{q^d}},\ p_2 := \frac{t+\zeta_1^q}{t+\zeta_1^{q^{d+1}}}, \dots,\ p_d := \frac{t+\zeta_1^{q^{d-1}}}{t+\zeta_1^{q^{2d-1}}}$
$\tilde{p}_i \in \overline{\mathbb{F}}_q[t]^\times_{(t)}$	$\tilde{p}_1 := t+\zeta_2,\ \tilde{p}_2 := t+\zeta_2^q, \dots,\ \tilde{p}_d := t+\zeta_2^{q^{d-1}}$
$h_i \in \mathbb{F}_q[t]_{(t)}$	defined via $\prod_{i=1}^{d}(X-p_i)(X-p_i^{-1})$ $= X^{2d} - \sum_{i=1}^{d-1} h_i X^{2d-i} - h_d X^d - \sum_{i=1}^{d-1} h_i X^i + 1$
$\tilde{h}_i \in \mathbb{F}_q[t]_{(t)}$	defined via $\prod_{i=1}^{d}(X-\tilde{p}_i)(X-\tilde{p}_i^{-1})$ $= X^{2d} - \sum_{i=1}^{d-1} \tilde{h}_i X^{2d-i} - \tilde{h}_d X^d - \sum_{i=1}^{d-1} \tilde{h}_i X^i + 1$

$a_{ij}, b_{ij} \in \mathbb{F}_q$	coefficients of h_i: $h_i(t) = \frac{\sum_{j=0}^{2d} a_{ij}t^j}{\sum_{j=0}^{2d} b_{ij}t^j}$; $b_{i0} \neq 0$ for all i
$\tilde{a}_{ij}, \tilde{b}_{ij} \in \mathbb{F}_q$	coefficients of $\tilde{h}_i$: $\tilde{h}_i(t) = \frac{\sum_{j=0}^{2d} \tilde{a}_{ij}t^j}{\sum_{j=0}^{d} \tilde{b}_{ij}t^j}$; $\tilde{b}_{i0} \neq 0$ for all i
$H_i \in \mathbb{F}_q(t,s)$	$H_i := \frac{s\sum_{j=0}^{2d} a_{ij}t^j}{b_{i0}+s\sum_{j=1}^{2d} b_{ij}t^j}$, $1 \leq i \leq d$
$\tilde{H}_i \in \mathbb{F}_q(t,s)$	$\tilde{H}_i := \frac{\frac{s}{\alpha}\sum_{j=0}^{2d} \tilde{a}_{ij}t^j}{\tilde{b}_{i0}+\frac{s}{\alpha}\sum_{j=1}^{d} \tilde{b}_{ij}t^j}$, $1 \leq i \leq d$
$f_i \in F$	$f_i := \frac{s-\alpha}{1-\alpha}H_i + \frac{s-1}{\alpha-1}\tilde{H}_i$, $1 \leq i \leq d$

Table 5.2: Definition of $f_1, \ldots, f_d$.

Note that the elements h_i and $\tilde{h}_i$ exist inside $\overline{\mathbb{F}}_q[t]_{(t)}$ by Lemma 5.5.1 and they are contained in $\mathbb{F}_q[t]_{(t)}$ as they are the coefficients of the characteristic polynomials of $t_1 \in T_1(\mathbb{F}_q[[t]])$ and $t_2 \in T_2(\mathbb{F}_q[[t]])$ as in Proposition 5.5.3.

Theorem 5.5.4. *Assume $q > 2$ and $n = 2d \geq 4$.*
Let $M = (F^n, \Phi)$ be the ϕ_q-difference module over $F = \mathbb{F}_q(s,t)$ given by $D_{(f_1,\ldots,f_d)}$, where $f_i \in F$ are as defined in Table 5.2. Then there exists a Picard-Vessiot ring $R \subseteq \overline{\mathbb{F}_q(s)}^{\mathrm{sep}}((t)) \cap L$ for M such that R/F is separable and the Galois group scheme $\mathcal{G}_{M,R}$ of M with respect to R is isomorphic to Sp_{2d} (as linear algebraic group over $\mathbb{F}_q(t)$).

Proof. We abbreviate $D := D_{(f_1,\ldots,f_d)}$. We proceed along the same line as in the proof of Theorem 5.4.4. By replacing every occurrence of "SL_n" and "$n-1$" by "Sp_{2d}" and "d" in the first three paragraphs of the proof of Theorem 5.4.4, we conclude that there exists a fundamental matrix $Y \in \mathrm{Sp}_{2d}(L \cap K[[t]])$ for M such that $R := F[Y, Y^{-1}]$ is a Picard-Vessiot ring for M contained in $\overline{\mathbb{F}_q(s)}^{\mathrm{sep}}((t))$ (and thus separable over F) and the Galois group scheme $\mathcal{H} := \mathcal{G}_{M,R} \leq \mathrm{Sp}_{2d}$ is a linear algebraic group (defined over $\mathbb{F}_q(t)$).

As in the proof of Theorem 5.4.4, we now consider the valuation rings $\mathfrak{o}_1 := \mathbb{F}_q[s]_{(s-1)}$ and $\mathfrak{o}_2 := \mathbb{F}_q[s]_{(s-\alpha)}$ inside $k = \mathbb{F}_q(s)$ with maximal ideals $\mathfrak{p}_1 = (s-1)$ and $\mathfrak{p}_2 = (s-\alpha)$, resp., and we fix extensions $(\mathcal{O}_j, \mathcal{P}_j)$ of $(\mathfrak{o}_j, \mathfrak{p}_j)$ to $\overline{k}^{\mathrm{sep}} = \overline{\mathbb{F}_q(s)}^{\mathrm{sep}}$ $(j = 1, 2)$. The same argument as in the proof of

Theorem 5.4.4 then yields that all entries of D are contained in $\mathfrak{o}_j[[t]]$, and as $\mathrm{Sp}_{2d} \leq \mathrm{SL}_{2d}$, we thus have $D \in \mathrm{Sp}_{2d}(\mathfrak{o}_j[[t]])$ for both $j = 1, 2$. Therefore, we can apply Corollary 3.3.11 (with $\mathcal{G} := \mathrm{Sp}_{2d}$ and $\tilde{k} := K$) to conclude that $\mathcal{H}(\mathbb{F}_q[[t]])$ contains $\mathrm{Sp}_{2d}(\overline{\mathbb{F}}_q[[t]])$-conjugates of $\kappa_1(D)$ and $\kappa_2(D)$, where $\kappa_j \colon \mathfrak{o}_j[[t]] \to \mathbb{F}_q[[t]]$ denotes the coefficient-wise reduction mod $\mathfrak{p}_j$.

Specializing $s \mapsto 1$ maps f_i to h_i $(1 \leq i \leq d)$, thus $\kappa_1(D) = D_{(h_1,\ldots,h_d)}$ and similarly $\kappa_2(D) = D_{(\tilde{h}_1,\ldots,\tilde{h}_d)}$. By Proposition 5.5.2, $\mathcal{H}(\mathbb{F}_q[[t]])$ thus contains $\mathrm{Sp}_{2d}(\overline{\mathbb{F}}_q[[t]])$-conjugates of t_1 and t_2 as in Proposition 5.5.3 (we used that g_1 and g_2 are contained in $\mathrm{Sp}_{2d}(\overline{\mathbb{F}}_q)$ and that their constant parts have pairwise distinct eigenvalues by 5.5.3). Applying Proposition 4.4.3 together with Proposition 5.5.3, we conclude that there exist A_1 and A_2 contained in $\mathrm{Sp}_{2d}(\mathbb{F}_q + t\overline{\mathbb{F}}_q[[t]])$ such that $t_1^{A_1}$ and $t_2^{A_2}$ are contained in $\mathcal{H}(\mathbb{F}_q[[t]])$. Now t_1 and t_2 generate dense subgroups of T_1 and T_2 by Proposition 5.5.3, and $< T_1^{A_1}, T_2^{A_2} >= \mathrm{Sp}_{2d}$ holds by Theorem 4.2.5, so we conclude $\mathcal{H} = \mathrm{Sp}_{2d}$. $\square$

5.6 Special Orthogonal Groups in Odd Dimension

In this section we let $n = 2d+1$ be odd and we are only working in characteristic $\neq 2$. Consider the special orthogonal group $\mathcal{G} = \mathrm{SO}_{2d+1}$ with respect to the orthogonal form given by

$$J = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}.$$

For any elements $f_1, \ldots, f_d \in F = \mathbb{F}_q(s,t)$ with $f_d \neq 0$, we set

$$D_{(f_1,\ldots,f_d)} = \left(\begin{array}{cccc|c|cccc} f_1 & \cdots & f_{d-1} & f_d & -2f_d & -2f_d & & & \\ 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & 0 & & & & & \\ \hline & & & 1 & -1 & & & & \\ \hline & & & \frac{f_{d-1}}{2f_d} & & 0 & 1 & & \\ & & & \vdots & & & & \ddots & \\ & & & \frac{f_1}{2f_d} & & & & & 1 \\ & & & -\frac{1}{2f_d} & & & & & 0 \end{array}\right).$$

It is easily seen that $D_{(f_1,\ldots,f_d)}$ is orthogonal and of determinant 1 and its characteristic polynomial equals

$$\chi_{(f_1,\ldots,f_d)}(X) = X^{2d+1} - \sum_{i=1}^{d}(f_i + f_{i-1})X^{2d+1-i} + \sum_{i=1}^{d}(f_i + f_{i-1})X^i - 1, \quad (5.9)$$

where we set $f_0 = -1$. (A proof can be found in [AM10, 4.3.]).

5.6.1 Specializations of $D_{(f_1,\ldots,f_d)}$

Recall that the diagonal matrices contained in SO_{2d+1} are exactly those of the form $\mathrm{diag}(\lambda_1, \ldots, \lambda_d, 1, \lambda_d^{-1}, \ldots, \lambda_1^{-1})$ for non-zero elements $\lambda_1, \ldots, \lambda_d$. They form a maximal torus T_0 which we call the diagonal torus. The coefficients of the characteristic polynomial of such an element are palindromic in the following way:

Lemma 5.6.1. *Let $\mathbb{F}$ be a field and let $\lambda_1, \ldots, \lambda_d$ be non-zero elements in $\mathbb{F}$. Consider the diagonal matrix*

$$A := \mathrm{diag}(\lambda_1, \ldots, \lambda_d, 1, \lambda_d^{-1}, \ldots, \lambda_1^{-1}).$$

Then the characteristic polynomial of A is of the form

$$X^{2d+1} - a_1X^{2d} - \cdots - a_dX^{d+1} + a_dX^d + a_{d-1}X^{d-1} + \cdots + a_1X - 1$$

for some $a_1, \ldots, a_d \in \mathbb{F}$.

Proof. This can easily be deduced from Lemma 5.5.1 by multiplying the characteristic polynomial of $\mathrm{diag}(\lambda_1, \ldots, \lambda_d, \lambda_d^{-1}, \ldots, \lambda_1^{-1})$ by $(X-1)$. □

Lemma 5.6.2. *Let $p_1, \ldots, p_d$ be elements in $\overline{\mathbb{F}}_q[t]^\times_{(t)}$ such that the constant terms of $p_1, \ldots, p_d, 1, p_d^{-1}, \ldots, p_1^{-1}$ regarded as power series in t are pairwise distinct elements in $\overline{\mathbb{F}}_q^\times \setminus \{-1\}$. Then there exist unique elements $h_1, \ldots, h_d \in \overline{\mathbb{F}}_q[t]_{(t)}$ with $h_d \in \overline{\mathbb{F}}_q[t]^\times_{(t)}$ such that*

$$(X-1)\prod_{i=1}^{d}(X-p_i)(X-p_i^{-1}) = \chi_{(h_1,\ldots,h_d)}(X). \tag{5.10}$$

Moreover, $D_{(h_1,\ldots,h_d)}$ and $\mathrm{diag}(p_1, \ldots, p_d, 1, p_d^{-1}, \ldots, p_1^{-1})$ are conjugate over $\mathrm{SO}_{2d+1}(\overline{\mathbb{F}}_q[[t]])$.

Proof. We abbreviate $\mathcal{G} = \mathrm{SO}_{2d+1}$. There exist elements $a_1, \ldots, a_d$ inside $\overline{\mathbb{F}}_q(t)$ for which

$$(X-1)\prod_{i=1}^{d}(X-p_i)(X-p_i^{-1}) = X^{2d+1} - \sum_{i=1}^{d} a_i X^{2d+1-i} + \sum_{i=1}^{d} a_i X^i - 1$$

by Lemma 5.6.1, and as they are constructed as sums of products of the elements $p_1, \ldots, p_d, 1, p_d^{-1}, \ldots, p_1^{-1}$, they are contained in $\overline{\mathbb{F}}_q[t]_{(t)}$. Equation (5.9) implies that we are looking for solutions $h_1, \ldots, h_d$ of the following system of equations

$$\begin{aligned} h_1 - 1 &= a_1 \\ h_2 + h_1 &= a_2 \\ &\vdots \\ h_d + h_{d-1} &= a_d \end{aligned}$$

which is equivalent to

$$\begin{aligned} h_1 &= a_1 + 1 \\ h_2 &= (a_2 - a_1 - 1) \\ h_3 &= (a_3 - a_2 + a_1 + 1) \\ &\vdots \\ h_d &= (a_d - a_{d-1} \pm \cdots + (-1)^d a_1 + (-1)^d). \end{aligned} \tag{5.11}$$

Hence there exists a unique solution $(h_1, \ldots, h_d) \in (\overline{\mathbb{F}}_q[t]_{(t)})^d$. It remains to show that h_d is contained in $\overline{\mathbb{F}}_q[t]^\times_{(t)}$. Abbreviate

$$f(X) = (X-1)\prod_{i=1}^{d}(X-p_i)(X-p_i^{-1}) = X^{2d+1} - \sum_{i=1}^{d} a_i X^{2d+1-i} + \sum_{i=1}^{d} a_i X^i - 1.$$

Equation (5.11) implies $f(-1) = 2h_d$. Since we assumed that none of the p_i's has constant term -1, it follows that $f(-1) \in \overline{\mathbb{F}}_q[t]^\times_{(t)}$ and thus $h_d \in \overline{\mathbb{F}}_q[t]^\times_{(t)}$.

We have found elements $h_1, \ldots, h_d$ such that the characteristic polynomial of $D_{(h_1,\ldots,h_d)}$ equals $(X-1)\prod_{i=1}^{d}(X-p_i)(X-p_i^{-1})$ and is thus separable. Hence $D_{(h_1,\ldots,h_d)}$ is a semisimple element of $\mathcal{G}(\overline{\mathbb{F}_q(t)})$. It follows that there exists a maximal torus T containing $D_{(h_1,\ldots,h_d)}$. All maximal tori of $\mathcal{G}(\overline{\mathbb{F}_q(t)})$ are conjugate, hence there exists an element $g \in \mathcal{G}(\overline{\mathbb{F}_q(t)})$ such that T^g equals the diagonal torus T_0 inside $\mathcal{G}$. It follows that $t_0 := D^g_{(h_1,\ldots,h_d)}$ is diagonal. We relabel $p_1, \ldots, p_d, 1, p_d^{-1}, \ldots, p_1^{-1}$ as $p_1, \ldots, p_d, p_{d+1}, \ldots, p_{2d+1}$. Then $p_1, \ldots, p_{2d+1}$ are the $2d+1$ pairwise distinct eigenvalues of t_0. It follows that there exists a permutation $\sigma \in S_{2d+1}$ such that $t_0 = \operatorname{diag}(p_{\sigma(1)}, \ldots, p_{\sigma(2d+1)})$ holds. Now t_0 is orthogonal, so we have $p_{\sigma(d+1)} = 1$ and $p_{\sigma(i)} = p^{-1}_{\sigma(2d+2-i)}$ for all $1 \leq i \leq d$. On the other hand, $p_1, \ldots, p_{2d+1}$ are pairwise distinct and $p_i = p^{-1}_{2d+2-i}$ holds for all $1 \leq i \leq d$. It follows that $\sigma(2d+2-i) = 2d+2-\sigma(i)$ holds for all $1 \leq i \leq d$. Therefore, σ gives rise to an orthogonal permutation matrix $A_\sigma \in \mathcal{G}(\mathbb{F}_q)$, by Lemma 4.1.5. By multiplying g with A_σ^{-1} from the right, we may assume that t_0 equals $\operatorname{diag}(p_1, \ldots, p_d, 1, p_d^{-1}, \ldots, p_1^{-1})$.

So far, we have seen that there exists a $g \in \mathcal{G}(\overline{\mathbb{F}_q(t)})$ satisfying $D^g_{(h_1,\ldots,h_d)} = \operatorname{diag}(p_1, \ldots, p_d, 1, p_d^{-1}, \ldots, p_1^{-1}) =: t_0$. We would like to show that g can be chosen inside $\mathcal{G}(\overline{\mathbb{F}}_q[[t]])$. Proposition 5.2.2 implies that there exists a $C \in \mathrm{GL}_n(\overline{\mathbb{F}}_q[[t]])$ with $D^C_{(h_1,\ldots,h_d)} = \operatorname{diag}(p_1, \ldots, p_d, 1, p_d^{-1}, \ldots, p_1^{-1}) = t_0$, since
$p_1, \ldots, p_d, 1, p_d^{-1}, \ldots, p_1^{-1}$ have pairwise distinct constant terms. Hence $C^{-1}g$ is contained in the centralizer of t_0 inside GL_n which only consists of diagonal matrices (since the diagonal entries of t_0 are pairwise distinct). Let $x_1, \ldots, x_{2d+1} \in \overline{\mathbb{F}_q((t))}^\times$ be such that $g = C \cdot \operatorname{diag}(x_1, \ldots, x_{2d+1})$ holds.

By multiplying g from the right with

$$\operatorname{diag}(x_{2d+1}, \ldots, x_{d+1}, 1, x_{d+1}^{-1}, \ldots, x_{2d+1}^{-1}) \in \mathcal{G}(\overline{\mathbb{F}_q((t))}),$$

we may assume that $C = g \cdot \operatorname{diag}(\alpha_1, \ldots, \alpha_{d+1}, 1 \ldots, 1)$ holds for some ele-

ments $\alpha_i \in \overline{\mathbb{F}_q((t))}^\times$. We now use that g is orthogonal to compute

$$\begin{aligned} C^{\mathrm{tr}} JC &= \mathrm{diag}(\alpha_1, \ldots, \alpha_{d+1}, 1 \ldots, 1) g^{\mathrm{tr}} Jg \,\mathrm{diag}(\alpha_1, \ldots, \alpha_{d+1}, 1 \ldots, 1) \\ &= \mathrm{diag}(\alpha_1, \ldots, \alpha_{d+1}, 1 \ldots, 1) J \,\mathrm{diag}(\alpha_1, \ldots, \alpha_{d+1}, 1 \ldots, 1) \\ &= \left(\begin{array}{ccc} & & \alpha_1 \\ & & \iddots \\ & & \alpha_d \\ \hline & \alpha_{d+1}^2 & \\ \hline & & \\ \alpha_d & & \\ \iddots & & \\ \alpha_1 & & \end{array}\right). \end{aligned} \tag{5.12}$$

Equation (5.12) implies that $\alpha_1, \ldots, \alpha_d$ and α_{d+1}^2 are contained in $\overline{\mathbb{F}}_q[[t]]$, as all entries of C and J are. On the other hand, g has determinant 1, so $C = g \cdot \mathrm{diag}(\alpha_1, \ldots, \alpha_{d+1}, 1 \ldots, 1)$ implies $\alpha_1 \cdots \alpha_d \alpha_{d+1}^2 = \det(C) \in \overline{\mathbb{F}}_q[[t]]^\times$. Hence $\alpha_1, \ldots, \alpha_d$ as well as α_{d+1}^2 are contained in $\overline{\mathbb{F}}_q[[t]]^\times$. Now $\overline{\mathbb{F}}_q[[t]]^\times$ is closed under taking square roots (recall that we are working in characteristic $\neq 2$), so α_{d+1} is contained in $\overline{\mathbb{F}}_q[[t]]$, too. It follows that all entries of $g = C \cdot \mathrm{diag}(\alpha_1^{-1}, \ldots, \alpha_{d+1}^{-1}, 1, \ldots, 1)$ are contained in $\overline{\mathbb{F}}_q[[t]]$, thus $g \in \mathcal{G}(\overline{\mathbb{F}}_q[[t]])$. □

Proposition 5.6.3. *Let $n = 2d + 1 \geq 3$. Let $T_0 \leq \mathrm{SO}_{2d+1}$ be the diagonal torus and let $T_1 = T_0^{g_1}$ and $T_2 = T_0^{g_2}$ be the maximal tori of SO_{2d+1} defined over $\mathbb{F}_q$ as in Definition 4.1.7. Consider*

$\zeta_1 \in \mathbb{F}_{q^{2d}}$	*primitive $(q^{2d}-1)$-th root of unity*
$\zeta_2 \in \mathbb{F}_{q^d}$	*primitive (q^d-1)-th root of unity*
$p_i \in \overline{\mathbb{F}}_q[t]_{(t)}$, $1 \leq i \leq d$	$p_1 := \frac{t+\zeta_1}{t+\zeta_1^{q^d}}$, $p_2 := \frac{t+\zeta_1^q}{t+\zeta_1^{q^{d+1}}}, \ldots,$ $p_d := \frac{t+\zeta_1^{q^{d-1}}}{t+\zeta_1^{q^{2d-1}}}$
$\tilde{p}_i \in \overline{\mathbb{F}}_q[t]_{(t)}$, $1 \leq i \leq d$	$\tilde{p}_1 := t + \zeta_2$, $\tilde{p}_2 := t + \zeta_2^q, \ldots,$ $\tilde{p}_d := t + \zeta_2^{q^{d-1}}$
t_1	$t_1 := \mathrm{diag}(p_1, \ldots, p_d, 1, p_d^{-1}, \ldots, p_1^{-1})^{g_1}$
t_2	$t_2 := \mathrm{diag}(\tilde{p}_1, \ldots, \tilde{p}_d, 1, \tilde{p}_d^{-1}, \ldots, \tilde{p}_1^{-1})^{g_2}$

Then t_i is contained in $T_i(\mathbb{F}_q[[t]])$ and the centralizer of its constant part equals T_i. Moreover, t_i generates a dense subgroup of T_i $(i = 1, 2)$.

Proof. Note that the elements $p_1, \ldots, p_d$ and $\tilde{p}_1, \ldots, \tilde{p}_d$ are the same as in the symplectic case. The proof is then almost identical to the proof of Proposition 5.5.3. □

5.6.2 A Difference Module for SO_{2d+1}

We can now define the elements $f_1, \ldots, f_d \in F$ in a similar way as in the symplectic case:

n q	$n = 2d+1 \geq 7$ an odd prime power
$\zeta_1 \in \mathbb{F}_{q^{2d}}$ $\zeta_2 \in \mathbb{F}_{q^d}$	primitive $(q^{2d}-1)$-th root of unity primitive (q^d-1)-th root of unity
$p_i \in \overline{\mathbb{F}}_q[t]^\times_{(t)}$ $\tilde{p}_i \in \overline{\mathbb{F}}_q[t]^\times_{(t)}$	$p_1 := \frac{t+\zeta_1}{t+\zeta_1^{q^d}},\ p_2 := \frac{t+\zeta_1^q}{t+\zeta_1^{q^{d+1}}}, \ldots,\ p_d := \frac{t+\zeta_1^{q^{d-1}}}{t+\zeta_1^{q^{2d-1}}}$ $\tilde{p}_1 := t+\zeta_2,\ \tilde{p}_2 := t+\zeta_2^q, \ldots,\ \tilde{p}_d := t+\zeta_2^{q^{d-1}}$
$h_i \in \mathbb{F}_q[t]_{(t)}$ $\tilde{h}_i \in \mathbb{F}_q[t]_{(t)}$	defined via $(X-1)\prod_{i=1}^{d}(X-p_i)(X-p_i^{-1})$ $= \chi_{(h_1,\ldots,h_d)}(X)$ defined via $(X-1)\prod_{i=1}^{d}(X-\tilde{p}_i)(X-\tilde{p}_i^{-1})$ $= \chi_{(\tilde{h}_1,\ldots,\tilde{h}_d)}(X)$
$a_{ij}, b_{ij} \in \mathbb{F}_q$ $\tilde{a}_{ij}, \tilde{b}_{ij} \in \mathbb{F}_q$	coefficients of h_i: $h_i(t) = \frac{\sum_{j=0}^{2d} a_{ij}t^j}{\sum_{j=0}^{2d} b_{ij}t^j}$; $b_{i0} \neq 0$ for all i coefficients of $\tilde{h}_i$: $\tilde{h}_i(t) = \frac{\sum_{j=0}^{2d} \tilde{a}_{ij}t^j}{\sum_{j=0}^{d} \tilde{b}_{ij}t^j}$; $\tilde{b}_{i0} \neq 0$ for all i
$H_i \in \mathbb{F}_q(t,s)$ $\tilde{H}_i \in \mathbb{F}_q(t,s)$	$H_i := \frac{s\sum_{j=0}^{2d} a_{ij}t^j}{b_{i0}+s\sum_{j=1}^{2d} b_{ij}t^j},\ 1 \leq i \leq d$ $\tilde{H}_i := \frac{-s\sum_{j=0}^{2d} \tilde{a}_{ij}t^j}{\tilde{b}_{i0}-s\sum_{j=1}^{d} \tilde{b}_{ij}t^j},\ 1 \leq i \leq d$
$f_i \in F$	$f_i := \frac{s+1}{2}H_i + \frac{1-s}{2}\tilde{H}_i,\ 1 \leq i \leq d-1$ $f_d := \frac{s+1}{2}H_d + \frac{1-s}{2}\tilde{H}_d + (s+1)(1-s)$

Table 5.3: Definition of $f_1, \ldots, f_d$.

Note that the elements h_i and $\tilde{h}_i$ exist inside $\overline{\mathbb{F}}_q[t]_{(t)}$ by Lemma 5.6.1 and they are contained in $\mathbb{F}_q[t]_{(t)}$ as the coefficients of $(X-1)\prod_{i=1}^{d}(X-p_i)(X-p_i^{-1})$ and $(X-1)\prod_{i=1}^{d}(X-\tilde{p}_i)(X-\tilde{p}_i^{-1})$ are contained in $\mathbb{F}_q[t]_{(t)}$ by Proposition 5.6.3.

Theorem 5.6.4. *Assume q odd and $n = 2d + 1 \geq 7$.*
Let $M = (F^n, \Phi)$ be the ϕ_q-difference module over $F = \mathbb{F}_q(s,t)$ given by $D_{(f_1,\dots,f_d)}$, where $f_i \in F$ are as defined in Table 5.3. Then there exists a Picard-Vessiot ring $R \subseteq \overline{\mathbb{F}_q(s)}^{\text{sep}}((t)) \cap L$ for M such that R/F is separable and the Galois group scheme $\mathcal{G}_{M,R}$ of M with respect to R is isomorphic to SO_{2d+1} (as linear algebraic group over $\mathbb{F}_q(t)$).

Proof. We abbreviate $D := D_{(f_1,\dots,f_d)}$. Let $\mathcal{O}_{|\cdot|} \subseteq K$ denote the valuation ring corresponding to $|\cdot|$ with maximal ideal $\mathfrak{m} \subseteq \mathcal{O}_{|\cdot|}$. All non-constant coefficients of the numerators and denominators of H_i and $\tilde{H}_i$ $(1 \leq i \leq n-1)$ are contained in $\mathfrak{m}$ and the constant coefficients of the denominators are contained in $\mathbb{F}_q^\times \subseteq \mathcal{O}_{|\cdot|}^\times$, so it follows from Lemma 3.1.4 that all H_i and $\tilde{H}_i$ are contained in $\mathcal{O}_{|\cdot|}[[t]]$ and their j-th coefficients can be bounded by δ^j for a suitable $\delta < 1$. Hence the same is true for all f_i, $1 \leq i \leq d$. Note that $\frac{s+1}{2}H_d + \frac{1-s}{2}\tilde{H}_d$ is contained in $\mathfrak{m}[[t]]$, so $f_d = \frac{s+1}{2}H_d + \frac{1-s}{2}\tilde{H}_d + (s+1)(1-s)$ is contained in $\mathcal{O}_{|\cdot|}[[t]]^\times$, since we added the extra term $(s+1)(1-s) \in \mathcal{O}_{|\cdot|}^\times$. We conclude that $D = \sum_{l=0}^{\infty} D_l t^l \in \mathrm{SO}_n(\mathcal{O}_{|\cdot|}[[t]])$ satisfies $||D_l|| \leq \delta^l$ for all $l \in \mathbb{N}$. By Theorem 3.1.3, there exists a fundamental solution matrix $Y = \sum_{l=0}^{\infty} Y_l t^l \in \mathrm{GL}_n(L \cap K[[t]])$ satisfying $||Y_l|| \leq \delta^l$, i.e., $Y \in \mathrm{M}_n(\mathcal{O}_{|\cdot|}\{t\})$. Let $E = F(Y)$ be the field generated by the entries of Y. Then $E \subseteq L$, hence $C_E = C_F$ and $R := F[Y, Y^{-1}] \subseteq E$ is a Picard-Vessiot ring for M by Theorem 1.2.11.

Consider $\mathfrak{o} := \mathcal{O}_{|\cdot|} \cap k = \mathbb{F}_q[s]_{(s)}$ and $\mathcal{O} := \mathcal{O}_{|\cdot|} \cap \overline{k}^{\text{sep}}$ (with respect to a fixed embedding of $\overline{k}^{\text{sep}} = \overline{\mathbb{F}_q(s)}^{\text{sep}}$ into K). Let $\mathfrak{p} = (s)$ denote the maximal ideal inside $\mathfrak{o}$. Then $\mathfrak{o}/\mathfrak{p} \cong \mathbb{F}_q$. Therefore, $\mathfrak{o}$ and $\mathcal{O}$ conform to all assumptions made in 3.3.1 hence we can apply Proposition 3.3.3 c) (with $\tilde{k} := K$) to conclude that Y is contained in $\mathrm{GL}_n(\mathcal{O}[[t]])$. In particular, all entries of Y are contained in $\overline{\mathbb{F}_q(s)}^{\text{sep}}((t))$, hence R/F is separable by Proposition 5.2.1. Also, Y is contained in $\mathrm{GL}_n(\mathcal{O}_{|\cdot|}[[t]]) \cap \mathrm{M}_n(\mathcal{O}_{|\cdot|}\{t\})$, so we may assume that Y is contained in $\mathrm{SO}_n(L \cap K[[t]])$, by Theorem 3.2.4. Indeed, $\mathcal{O}_{|\cdot|}/\mathfrak{m} \cong \overline{\mathbb{F}}_q \subseteq K$, $D \in \mathrm{SO}_n(\mathcal{O}_{|\cdot|}[[t]])$ and $\kappa_{|\cdot|}(D) = D_{(0,\dots,0,1)} \in \mathrm{SO}_n(\mathbb{F}_q) \subseteq \mathrm{SO}_n(\mathcal{O}_{|\cdot|}/\mathfrak{m})$ (the latter follows from $\kappa_{|\cdot|}(H_i) = \kappa_{|\cdot|}(\tilde{H}_i) = 0$ for all $i \leq n-1$).

We conclude that the Galois group scheme $\mathcal{H} := \mathcal{G}_{M,R}$ of (M, Φ) is a linear algebraic group (see Theorem 1.3.10) defined over $\mathbb{F}_q(t)$ that is a closed subgroup of SO_n (see Proposition 1.3.11). We will now use the lower bound criterion 3.3.11 to show that $\mathcal{H}$ is all of SO_n.

Consider $\mathfrak{p}_1 = (s-1) \subseteq \mathfrak{o}_1 := \mathbb{F}_q[s]_{(s-1)}$ and $\mathfrak{p}_2 = (s+1) \subseteq \mathfrak{o}_2 := \mathbb{F}_q[s]_{(s+1)}$. Then $\mathfrak{o}_1$ and $\mathfrak{o}_2$ are valuation rings inside $k = \mathbb{F}_q(s)$ with $\mathfrak{o}_1/\mathfrak{p}_1 \cong \mathbb{F}_q$ and $\mathfrak{o}_2/\mathfrak{p}_2 \cong \mathbb{F}_q$. Fix extensions $(\mathcal{O}_j, \mathcal{P}_j)$ of $(\mathfrak{o}_j, \mathfrak{p}_j)$ to $\overline{k}^{\text{sep}} = \overline{\mathbb{F}_q(s)}^{\text{sep}}$ $(j = 1, 2)$.

These valuation rings conform to all assumptions made in 3.3.1 and we may thus apply the results from Section 3.3. Note that $H_i \in \mathfrak{o}_j[[t]]$ for all $1 \leq i \leq n-1$, $j = 1, 2$ since the numerators are contained in $\mathfrak{o}_j[t]$ and the denominators are contained in $\mathfrak{o}_j[t]$ with constant coefficient $b_{i0} \in \mathbb{F}_q^{\times} \subseteq \mathfrak{o}_j^{\times}$. Similarly, all $\tilde{H}_i$ and thus all f_i are contained in $\mathfrak{o}_j[[t]]$. Therefore, all $f_1, \ldots, f_d$ are contained in $\mathfrak{o}_j[[t]]$ $(j = 1, 2)$. We claim that f_d is moreover contained in $\mathfrak{o}_j[[t]]^{\times}$. The reduction of f_d modulo $\mathfrak{p}_1$ equals h_d and the reduction modulo $\mathfrak{p}_2$ equals $\tilde{h}_d$. As h_d and $\tilde{h}_d$ are both contained in $\mathbb{F}_q[t]^{\times}_{(t)}$ by Lemma 5.6.2, the claim follows and we conclude that D is contained in $\mathrm{SO}_n(\mathfrak{o}_j[[t]])$ for both $j = 1, 2$. Therefore, we can apply Corollary 3.3.11 (with $\mathcal{G} := \mathrm{SO}_n$ and $\tilde{k} := K$) to conclude that $\mathcal{H}(\mathbb{F}_q[[t]])$ contains $\mathrm{SO}_n(\overline{\mathbb{F}}_q[[t]])$-conjugates of $\kappa_1(D)$ and $\kappa_2(D)$, where $\kappa_j \colon \mathfrak{o}_j[[t]] \to \mathbb{F}_q[[t]]$ denotes the coefficient-wise reduction mod $\mathfrak{p}_j$.

Specializing $s \mapsto 1$ maps f_i to h_i $(1 \leq i \leq d)$, thus $\kappa_1(D) = D_{(h_1,\ldots,h_d)}$. Similarly, $\kappa_2(D) = D_{(\tilde{h}_1,\ldots,\tilde{h}_d)}$ as specializing $s \mapsto -1$ maps f_i to $\tilde{h}_i$. The constant parts of $p_1, \ldots, p_d, 1, p_d^{-1}, \ldots, p_1^{-1}$ are pairwise distinct and not equal to -1, hence $\kappa_1(D)$ is conjugate to t_1 over $\mathrm{SO}_n(\overline{\mathbb{F}}_q[[t]])$, by Lemma 5.6.2. Similarly, $\kappa_2(D)$ is conjugate to t_2 over $\mathrm{SO}_n(\overline{\mathbb{F}}_q[[t]])$. Therefore, $\mathcal{H}(\mathbb{F}_q[[t]])$ contains $\mathrm{SO}_n(\overline{\mathbb{F}}_q[[t]])$-conjugates x_1 and x_2 of t_1 and t_2 which are both contained in $\mathrm{SO}_n(\mathbb{F}_q[[t]])$ (see Proposition 5.6.3). By Proposition 4.4.3 together with Proposition 5.6.3, there exist A_1 and A_2 contained in $\mathrm{SO}_n(\mathbb{F}_q + t\overline{\mathbb{F}}_q[[t]])$ with $x_j = t_j^{A_j}$ $(j = 1, 2)$. Now $\mathcal{H}$ is a closed subgroup of SO_n and t_1 and t_2 generate dense subgroups of T_1 and T_2 by Proposition 5.6.3, so $\mathcal{H}$ contains $< T_1^{A_1}, T_2^{A_2} >$. Finally, Theorem 4.2.5 implies $< T_1^{A_1}, T_2^{A_2} >= \mathrm{SO}_n$, hence $\mathcal{H} = \mathrm{SO}_n$. $\square$

5.7 Special Orthogonal Groups in Even Dimension

In this section we let $n = 2d$ be even and we are only working in characteristic $\neq 2$. Again, we consider the special orthogonal group $\mathcal{G} = \mathrm{SO}_{2d}$ with respect to the orthogonal form given by

$$J = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}.$$

For any elements $f_1, \ldots, f_d \in F = \mathbb{F}_q(s,t)$ with $f_d \neq 0$, we set

$$D_{(f_1,\ldots,f_d)} = \left(\begin{array}{cccc|cccccc} f_1 & \cdots & f_{d-1} & f_d & f_{d-1} & -f_d & & & & \\ 1 & & & & & & & & & \\ & \ddots & & & & & & & & \\ & & 1 & 0 & 1 & & & & & \\ \hline & & \frac{f_{d-1}}{f_d} & 1 & 0 & & & & & \\ & & \frac{f_{d-2}}{f_d} & & 0 & 0 & 1 & & & \\ & & \vdots & & & & & \ddots & & \\ & & \frac{f_1}{f_d} & & & & & & 1 & \\ & & -\frac{1}{f_d} & & & & & & 0 & \end{array}\right).$$

It is easily seen that $D_{(f_1,\ldots,f_d)}$ is orthogonal and of determinant 1 and its characteristic polynomial equals

$$\begin{aligned} \chi_{(f_1,\ldots,f_d)}(X) &= X^{2d} + \sum_{i=1}^{d-1}(-f_i + f_{i-2})X^{2d-i} + (-f_d + 2f_{d-2} - \frac{f_{d-1}^2}{f_d})X^d \\ &\quad + \sum_{i=1}^{d-1}(-f_i + f_{i-2})X^i + 1, \end{aligned} \tag{5.13}$$

where we set $f_0 = -1$ and $f_{-1} = 0$. (A proof can be found in [AM10, 4.4.]).

5.7.1 Specializations of $D_{(f_1,\ldots,f_d)}$

Recall that the diagonal matrices contained in SO_{2d} are exactly those of the form $\mathrm{diag}(\lambda_1, \ldots, \lambda_d, \lambda_d^{-1}, \ldots, \lambda_1^{-1})$ for non-zero elements $\lambda_1, \ldots, \lambda_d$.

Lemma 5.7.1. *Let $p_1, \ldots, p_d$ be elements in $\overline{\mathbb{F}}_q[t]^\times_{(t)}$ such that the constant terms of $p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1}$ regarded as power series in t are pairwise distinct elements in $\overline{\mathbb{F}}_q^\times \setminus \{\pm 1\}$. Then*

a) there exist elements $h_1, \ldots, h_d \in \overline{\mathbb{F}}_q[t]_{(t)}$ with $h_d \in \overline{\mathbb{F}}_q[t]^\times_{(t)}$ such that

$$\prod_{i=1}^{d}(X - p_i)(X - p_i^{-1}) = \chi_{(h_1,\ldots,h_d)}(X). \tag{5.14}$$

b) For any such elements $h_1, \ldots, h_d$, $D_{(h_1,\ldots,h_d)}$ is conjugate to one of the following diagonal matrices over $\mathrm{SO}_{2d}(\overline{\mathbb{F}}_q[[t]])$:

$$\mathrm{diag}(p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1})$$

or

$$\mathrm{diag}(p_1, \ldots, p_{d-1}, p_d^{-1}, p_d, p_{d-1}^{-1}, \ldots, p_1^{-1}).$$

c) If moreover $\prod_{i=1}^{d}(X - p_i)(X - p_i^{-1})$ is contained in $\mathbb{F}_q[t]_{(t)}[X]$ and $\prod_{i=1}^{d}(1 - p_i)(1 + p_i^{-1})$ is contained in $\mathbb{F}_q[t]_{(t)}$, all $h_1, \ldots, h_d$ are contained in $\mathbb{F}_q[t]_{(t)}$.

Proof. a) We abbreviate $\mathcal{G} = \mathrm{SO}_{2d}$. There exist elements $a_1, \ldots, a_d$ inside $\overline{\mathbb{F}}_q(t)$ with

$$\prod_{i=1}^{d}(X - p_i)(X - p_i^{-1}) = X^{2d} + \sum_{i=1}^{d-1} a_i X^{2d-i} + a_d X^d + \sum_{i=1}^{d-1} a_i X^i + 1$$

by Lemma 5.5.1, and as they are constructed as sums of products of the elements $p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1}$, they are contained in $\overline{\mathbb{F}}_q[t]_{(t)}$. Equation (5.13) implies that we are looking for solutions $h_1, \ldots, h_d$ of the following system of equations

$$\begin{aligned}
-h_1 &= a_1 \\
-h_2 - 1 &= a_2 \\
-h_3 + h_1 &= a_3 \\
&\vdots \\
-h_{d-1} + h_{d-3} &= a_{d-1} \\
-h_d + 2h_{d-2} - \frac{h_{d-1}^2}{h_d} &= a_d
\end{aligned}$$

which is equivalent to

$$\begin{aligned}
h_1 &= -a_1 \\
h_2 &= -a_2 - 1 \\
h_3 &= -a_3 - a_1 \\
h_4 &= -a_4 - a_2 - 1 \\
&\vdots \\
h_{d-1} &= -\sum_{j=0}^{\lfloor \frac{d-1}{2} \rfloor} a_{d-1-2j} \\
h_d^2 + (-2h_{d-2} + a_d)h_d + h_{d-1}^2 &= 0, \qquad (5.15)
\end{aligned}$$

where we set $a_0 = 1$. Hence $(h_1, \ldots, h_{d-1})$ are uniquely determined inside $\overline{\mathbb{F}}_q[t]_{(t)}$. It remains to show that Equation (5.15) can be solved inside $\overline{\mathbb{F}}_q[t]^{\times}_{(t)}$. Equation (5.15) is quadratic with discriminant

$$(-2h_{d-2}+a_d)^2-4h_{d-1}^2 = (-2h_{d-2}+a_d+2h_{d-1})(-2h_{d-2}+a_d-2h_{d-1}).$$

Abbreviate

$$f(X) = \prod_{i=1}^{d}(X-p_i)(X-p_i^{-1}) = \sum_{i=0}^{d-1} a_i X^{2d-i} + a_d X^d + \sum_{i=0}^{d-1} a_i X^i.$$

Then

$$\begin{aligned}
-2h_{d-2} + a_d - 2h_{d-1} &= a_d + 2\sum_{i=0}^{d-1} a_i = f(1) \\
-2h_{d-2} + a_d + 2h_{d-1} &= a_d - 2a_{d-1} + 2a_{d-2} \mp \ldots \\
&= (-1)^d((-1)^d a_d + 2\sum_{i=0}^{d-1}(-1)^i a_i) \\
&= (-1)^d f(-1).
\end{aligned}$$

Hence the discriminant equals

$$\begin{aligned}
(-1)^d f(1)f(-1) &= (-1)^d \prod_{i=1}^{d}(1-p_i)(1-p_i^{-1}) \prod_{i=1}^{d}(1+p_i)(1+p_i^{-1}) \\
&= (-1)^d \prod_{i=1}^{d} \frac{(1-p_i)(p_i-1)}{p_i} \prod_{i=1}^{d} \frac{(1+p_i)^2}{p_i} \\
&= \left(\prod_{i=1}^{d} \frac{(1-p_i)(1+p_i)}{p_i}\right)^2
\end{aligned}$$

We set

$$\Delta = \prod_{i=1}^{d} \frac{(1-p_i)(1+p_i)}{p_i}.$$

Note that Δ is contained in $\overline{\mathbb{F}}_q[t]^{\times}_{(t)}$, as we assumed that the constant parts of p_i are distinct from ± 1. Then at least one of the two solutions

$$\frac{2h_{d-2} - a_d \pm \Delta}{2} \tag{5.16}$$

of Equation (5.15) is contained in $\overline{\mathbb{F}}_q[t]^{\times}_{(t)}$.

b) We have found elements $h_1, \ldots, h_d$ such that the characteristic polynomial of $D_{(h_1,\ldots,h_d)}$ equals $\prod_{i=1}^{d}(X-p_i)(X-p_i^{-1})$ and is thus separable. Hence $D_{(h_1,\ldots,h_d)}$ is a semisimple element of $\mathcal{G}(\overline{\mathbb{F}_q(t)})$. It follows that there exists a maximal torus T containing $D_{(h_1,\ldots,h_d)}$. All maximal tori of $\mathcal{G}(\overline{\mathbb{F}_q(t)})$ are conjugate, hence there exists an element $g \in \mathcal{G}(\overline{\mathbb{F}_q(t)})$ such that T^g equals the diagonal torus T_0 inside $\mathcal{G}$. It follows that $t_0 := D^g_{(h_1,\ldots,h_d)}$ is diagonal. We relabel $p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1}$ as $p_1, \ldots, p_d, p_{d+1}, \ldots, p_{2d}$. Then $p_1, \ldots, p_{2d}$ are the $2d$ pairwise distinct eigenvalues of t_0. It follows that there exists a permutation $\sigma \in S_{2d}$ such that $t_0 = \operatorname{diag}(p_{\sigma(1)}, \ldots, p_{\sigma(2d)})$ holds. Now t_0 is orthogonal, so we have $p_{\sigma(i)} = p^{-1}_{\sigma(2d+1-i)}$ for all $1 \leq i \leq d$. On the other hand, $p_1, \ldots, p_{2d}$ are pairwise distinct and $p_i = p^{-1}_{2d+1-i}$ holds for all $1 \leq i \leq d$. It follows that $\sigma(2d+1-i) = 2d+1-\sigma(i)$ holds for all $1 \leq i \leq d$. If σ has sign 1, it gives rise to an orthogonal permutation matrix $A_\sigma \in \mathcal{G}(\mathbb{F}_q)$, by Lemma 4.1.5. By multiplying g with A_σ^{-1} from the right, we may assume that t_0 equals $\operatorname{diag}(p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1})$. If σ has sign -1, $\sigma' := \sigma \cdot (k, k+1)$ gives rise to an orthogonal permutation matrix $A_{\sigma'} \in \mathcal{G}(\mathbb{F}_q)$, by Lemma 4.1.5 and we may assume that t_0 equals $\operatorname{diag}(p_1, \ldots, p_{d-1}, p_d^{-1}, p_d, p_{d-1}^{-1}, \ldots, p_1^{-1})$.

So far, we have seen that there exists a $g \in \mathcal{G}(\overline{\mathbb{F}_q(t)})$ satisfying $D^g_{(h_1,\ldots,h_d)} = t_0$, where either

$$t_0 = \operatorname{diag}(p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1})$$

or

$$t_0 = \operatorname{diag}(p_1, \ldots, p_{d-1}, p_d^{-1}, p_d, p_{d-1}^{-1}, \ldots, p_1^{-1}).$$

We would like to show that g can be chosen inside $\mathcal{G}(\overline{\mathbb{F}}_q[[t]])$. Proposition 5.2.2 implies that there exists a $C \in \mathrm{GL}_n(\overline{\mathbb{F}}_q[[t]])$ with $D^C_{(h_1,\ldots,h_d)} = t_0$, since $p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1}$ have pairwise distinct constant terms. Hence $C^{-1}g$ is contained in the centralizer of t_0 inside GL_n which only consists of diagonal matrices (since the diagonal entries of t_0 are pairwise distinct). Let $x_1, \ldots, x_{2d} \in \overline{\mathbb{F}_q((t))}^\times$ be such that $g = C \cdot \operatorname{diag}(x_1, \ldots, x_{2d})$ holds.

By multiplying g from the right with $\operatorname{diag}(x_{2d}, \ldots, x_{d+1}, x_{d+1}^{-1}, \ldots, x_{2d}^{-1}) \in \mathcal{G}(\overline{\mathbb{F}_q((t))})$, we may assume that $C = g \cdot \operatorname{diag}(\alpha_1, \ldots, \alpha_d, 1 \ldots, 1)$ holds for some elements $\alpha_i \in \overline{\mathbb{F}_q((t))}^\times$. We now use that g is orthogonal to compute

$$\begin{aligned} C^{\mathrm{tr}} J C &= \operatorname{diag}(\alpha_1, \ldots, \alpha_d, 1 \ldots, 1) g^{\mathrm{tr}} J g \operatorname{diag}(\alpha_1, \ldots, \alpha_d, 1 \ldots, 1) \\ &= \operatorname{diag}(\alpha_1, \ldots, \alpha_d, 1 \ldots, 1) J \operatorname{diag}(\alpha_1, \ldots, \alpha_d, 1 \ldots, 1) \end{aligned}$$

$$= \left(\begin{array}{cc|cc} & & & \alpha_1 \\ & & & \iddots \\ & & \alpha_d & \\ \hline & \alpha_d & & \\ & \iddots & & \\ \alpha_1 & & & \end{array}\right). \tag{5.17}$$

Equation (5.17) implies that $\alpha_1, \ldots, \alpha_d$ are contained in $\overline{\mathbb{F}}_q[[t]]$, as all entries of C and J are. On the other hand, g has determinant 1, so $C = g \cdot \mathrm{diag}(\alpha_1, \ldots, \alpha_d, 1 \ldots, 1)$ implies $\alpha_1 \cdots \alpha_d = \det(C) \in \overline{\mathbb{F}}_q[[t]]^\times$. Hence $\alpha_1, \ldots, \alpha_d$ are contained in $\overline{\mathbb{F}}_q[[t]]^\times$. It follows that all entries of $g = C \cdot \mathrm{diag}(\alpha_1^{-1}, \ldots, \alpha_{d+1}^{-1}, 1, \ldots, 1)$ are contained in $\overline{\mathbb{F}}_q[[t]]$, thus $g \in \mathcal{G}(\overline{\mathbb{F}}_q[[t]])$.

c) If moreover $\prod_{i=1}^{d}(X - p_i)(X - p_i^{-1})$ is contained in $\mathbb{F}_q[t]_{(t)}[X]$, all $a_1, \ldots, a_d$ are contained in $\mathbb{F}_q[t]_{(t)}$ and it follows that $h_1, \ldots, h_{d-1}$ are contained in $\mathbb{F}_q[t]_{(t)}$ (see the block of equations above Equation (5.15)). If moreover $\prod_{i=1}^{d}(1 - p_i)(1 + p_i^{-1}) = F$ is contained in $\mathbb{F}_q[t]_{(t)}$, h_d is contained in $\mathbb{F}_q[t]_{(t)}^\times$ by Equation (5.16).

□

5.7.2 Another Maximal Torus

In Chapter 4 we constructed maximal tori T_1 and T_2 defined over $\mathbb{F}_q$ (corresponding to permutations σ_1 and σ_2) such that any conjugates generate SO_{2d}. In this section, we introduce a third maximal torus T_2' in SO_{2d} defined over $\mathbb{F}_q$ that corresponds to a permutation σ_2' conjugate to σ_2. Hence T_2' has very similar properties as T_2 but they are not conjugate over $\mathrm{SO}_{2d}(\mathbb{F}_q)$. Eventually we will only know that $D_{(f_1,\ldots,f_d)}$ specializes to a conjugate of an element that generates a dense subgroup of either T_2 or T_2'. Therefore we need to show that also any conjugates of T_1 and T_2' generate SO_{2d}. This peculiar situation reflects the fact that SO_n is not simply-connected and hence not every regular element has to be conjugate to an element inside the Steinberg section.

Definition 5.7.2. *We set $\sigma_2' := (k, k+1)\sigma_2(k, k+1)$ where σ_2 is defined as in Table 4.2 on page 54. By Lemma 4.1.5 there exists a monomial matrix $w_2' \in \mathrm{SO}_{2d}(\mathbb{F}_q)$ that corresponds to the permutation σ_2'. We fix an element $g_2' \in \mathrm{SO}_{2d}(\overline{\mathbb{F}}_q)$ with $g_2'\phi_q(g_2')^{-1} = w_2'$. Then $T_2' := T_0^{g_2'}$ is a maximal torus defined over $\mathbb{F}_q$ (where T_0 denotes the diagonal torus inside $\mathrm{SO}_{2d}(\mathbb{F}_q)$).*

Proposition 5.7.3. *The order of $T_2'(\mathbb{F}_q)$ equals $n_2(q)$, where $n_2(q)$ is as defined in Table 4.1.*

Proof. The $\mathbb{F}_q$-rational points of T_2' can be computed using Proposition 4.1.1. If d is odd,

$$\sigma_2' = (1, \dots, d-1, d+1)(2d, \dots, d+2, d)$$

and we get

$$T_2'(\mathbb{F}_q) = \{\mathrm{diag}(\zeta, \zeta^q, \dots, \zeta^{q^{d-2}}, \zeta^{-q^{d-1}}, \zeta^{q^{d-1}}, \zeta^{-q^{d-2}}, \dots, \zeta^{-1}) \mid \zeta^{q^d-1} = 1\}^{g_2'}.$$

Hence $|T_2'(\mathbb{F}_q)| = q^d - 1 = n_2(q)$.

If $d = 2m$ is even and m is odd, $n_2(q) = (q^m - 1)^2$ and

$$\sigma_2' = (1, \dots, m)(m+1, \dots, 2m-1, 2m+1)(3m, \dots, 2m+2, 2m)(4m, \dots, 3m+1).$$

We conclude that $T_2'(\mathbb{F}_q)$ consists of all elements of the form

$$\mathrm{diag}(\zeta, \dots, \zeta^{q^{m-1}}, \mu, \dots, \mu^{q^{m-2}}, \mu^{-q^{m-1}}, \mu^{q^{m-1}}, \mu^{-q^{m-2}}, \dots, \mu^{-1}, \zeta^{-q^{m-1}}, \dots, \zeta^{-1})^{g_2'}$$

for $(q^m - 1)$-th roots of unities ζ and μ, so $|T_2'(\mathbb{F}_q)| = (q^m - 1)^2 = n_2(q)$.

Finally, if $d = 2m$ for an even m, $n_2(q) = (q^m + 1)^2$ and

$$\sigma_2' = (1, \dots, m, 4m, \dots, 3m{+}1)(m{+}1, \dots, 2m{-}1, 2m{+}1, 3m, \dots, 2m{+}2, 2m).$$

Therefore, $T_2'(\mathbb{F}_q)$ consists of all elements of the form

$$\mathrm{diag}(\zeta, \dots, \zeta^{q^{m-1}}, \mu, \dots, \mu^{q^{m-2}}, \mu^{-q^{m-1}}, \mu^{q^{m-1}}, \mu^{-q^{m-2}}, \dots, \mu^{-1}, \zeta^{-q^{m-1}}, \dots, \zeta^{-1})^{g_2'}$$

for $(q^m + 1)$-th roots of unities ζ and μ, hence $|T_2'(\mathbb{F}_q)| = (q^m + 1)^2 = n_2(q)$. □

Theorem 5.7.4. *Let q be an odd power of a prime and assume $n = 2d \geq 8$. Then for any $A, B \in \mathrm{SO}_{2d}(\mathbb{F}_q + \overline{\mathbb{F}}_q[[t]])$ we have*

$$< T_1^A, T_2'^B >= \mathrm{SO}_{2d}\,.$$

Proof. Now that we know that $T_2'(\mathbb{F}_q) = n_2(q) = T_2(\mathbb{F}_q)$ we can prove this in the same way as we proved $< T_1^A, T_2^B >= \mathrm{SO}_{2d}$ in Chapter 4. Let l_0 denote the least common multiple of the order of σ_1 and σ_2'. As σ_2 and σ_2' are conjugate by $(k, k+1)$, this is the same as the least common multiple of the order of σ_1 and σ_2. Set

$$\mathbb{F} = \bigcup_{l \in \mathbb{N}:\ l \equiv 1 \bmod l_0} \mathbb{F}_{q^l} \subseteq \overline{\mathbb{F}}_q.$$

Then $\mathbb{F}$ is a field of infinite order by Lemma 4.2.3. Using Proposition 5.7.3, the same proof as that for Proposition 4.2.4 implies that

$$< T_1(\mathbb{F})^{A_0}, T_2'^{B_0} >= \mathrm{SO}_{2d}(\mathbb{F})$$

holds for any $A_0, B_0 \in \mathrm{SO}_{2d}(\mathbb{F}_q)$. The claim then follows similarly as in the proof of Theorem 4.2.5. □

5.7.3 Dense Elements in T_1,T_2 and T_2'

Lemma 5.7.5. *Let $m \geq 2 \in \mathbb{N}$ and assume q odd such that $(m, q) \neq (2, 3)$.*

a) There exist primitive $(q^m - 1)$-th roots of unity α and β such that

$$\alpha^{\pm 1}, \alpha^{\pm q}, \ldots, \alpha^{\pm q^{m-1}}, \beta^{\pm 1}, \beta^{\pm q}, \ldots, \beta^{\pm q^{m-1}}$$

are pairwise distinct.

b) There exist primitive $(q^{2m} - 1)$-th roots of unity α and β such that

$$\begin{gathered}\alpha^{\pm(1-q^m)}, \alpha^{\pm(q-q^{m+1})}, \ldots, \alpha^{\pm(q^{m-1}-q^{2m-1})}, \\ \beta^{\pm(1-q^m)}, \beta^{\pm(q-q^{m+1})}, \ldots, \beta^{\pm(q^{m-1}-q^{2m-1})}\end{gathered}$$

are pairwise distinct.

Proof. If ζ runs through all $(q^{2m}-1)$-th roots of unities, ζ^{1-q^m} runs through all $(q^m + 1)$-th roots of unities. Hence in both cases the claim is that there exists a $(q^m \pm 1)$-th primitive root of unity α and a $(q^m \pm 1)$-th primitive root of unity β such that

$$\alpha^{\pm 1}, \alpha^{\pm q}, \ldots, \alpha^{\pm q^{m-1}}, \beta^{\pm 1}, \beta^{\pm q}, \ldots, \beta^{\pm q^{m-1}}$$

are pairwise distinct. This has been proven in [AM10, p.10]. For the convenience of the reader, we sketch the proof: Fix a primitive $(q^m \pm 1)$-th root of unity α. Then $\alpha^{\pm 1}, \alpha^{\pm q}, \ldots, \alpha^{\pm q^{m-1}}$ are pairwise distinct. We have to show that there exists a primitive $(q^m \pm 1)$-th root of unity β such that $\alpha^{\pm q^i} \neq \beta^{q^j}$ for all $0 \leq i, j \leq m - 1$ which is equivalent to $\beta \neq \alpha^{\pm q^i}$ for all $0 \leq i \leq m - 1$. It is therefore sufficient to show that the number $\varphi(q^m \pm 1)$ of primitive $(q^m \pm 1)$-th roots of unity is greater than $2m$. As $m \geq 2$ and $q \geq 3$ it follows that $q^m \pm 1 \geq 6$ hence $\varphi(q^m \pm 1) \geq \sqrt{q^m \pm 1}$. We first treat the case $(m, q) = (3, 3)$. Then $\varphi(q^m \pm 1) \in \{26, 28\}$ and is clearly greater than $2m$. If $(m, q) \neq (3, 3)$, $\sqrt{q^m \pm 1} > 2m$ always holds. □

Proposition 5.7.6. *Let $n = 2d \geq 8$ and q odd such that $(n, q) \neq (8, 3)$. Let $T_0 \leq \mathrm{SO}_{2d}$ be the diagonal torus and let $T_1 = T_0^{g_1}$ and $T_2 = T_0^{g_2}$ be the maximal tori of SO_{2d} defined over $\mathbb{F}_q$ as in Definition 4.1.7 and $T_2' = T_0^{g_2'}$ as before. We define elements $t_1 \in T_1$, $t_1' \in T_1$, $t_2 \in T_2$ and $t_2' \in T_2'$ as follows.*

if $d \equiv 1 \mod 2$	
$\zeta \in \mathbb{F}_{q^2}$	*primitive* (q^2-1)*-th root of unity*
$\zeta_1 \in \mathbb{F}_{q^{2d-2}}$	*primitive* $(q^{2(d-1)}-1)$*-th root of unity*
$\zeta_2 \in \mathbb{F}_{q^d}$	*primitive* (q^d-1)*-th root of unity*
$p_i \in \overline{\mathbb{F}}_q[t]_{(t)}$	$p_i := \frac{t+\zeta_1^{q^{i-1}}}{t+\zeta_1^{q^{d+i-2}}}, \ \ 1 \le i \le d-1$
$p_d \in \overline{\mathbb{F}}_q[t]_{(t)}$	$p_d := \frac{t+\zeta}{t+\zeta^q}$
$\tilde{p}_i \in \overline{\mathbb{F}}_q[t]_{(t)}$	$\tilde{p}_i := t + \zeta_2^{q^{i-1}}, \ \ 1 \le i \le d$

if $d = 2m \equiv 2 \mod 4$	
$\zeta \in \mathbb{F}_{q^2}$	*primitive* (q^2-1)*-th root of unity*
$\zeta_1 \in \mathbb{F}_{q^{2d-2}}$	*primitive* $(q^{2(d-1)}-1)$*-th root of unity*
$\alpha, \beta \in \mathbb{F}_{q^m}$	*primitive* (q^m-1)*-th roots of unity*
	as in Lemma 5.7.5a)
$p_i \in \overline{\mathbb{F}}_q[t]_{(t)}$	$p_i := \frac{t+\zeta_1^{q^{i-1}}}{t+\zeta_1^{q^{d+i-2}}}, \ \ 1 \le i \le d-1$
$p_d \in \overline{\mathbb{F}}_q[t]_{(t)}$	$p_d := \frac{t+\zeta}{t+\zeta^q}$
$\tilde{p}_i \in \overline{\mathbb{F}}_q[t]_{(t)}$	$\tilde{p}_i := t + \alpha^{q^{i-1}}, \ 1 \le i \le m$
	$\tilde{p}_{m+i} := t + \beta^{q^{i-1}}, \ 1 \le i \le m$

if $d = 2m \equiv 0 \mod 4$	
$\zeta \in \mathbb{F}_{q^2}$	*primitive* (q^2-1)*-th root of unity*
$\zeta_1 \in \mathbb{F}_{q^{2d-2}}$	*primitive* $(q^{2(d-1)}-1)$*-th root of unity*
$\alpha, \beta \in \mathbb{F}_{q^{2m}}$	*primitive* $(q^{2m}-1)$*-th roots of unity*
	as in Lemma 5.7.5b)
$p_i \in \overline{\mathbb{F}}_q[t]_{(t)}$	$p_i := \frac{t+\zeta_1^{q^{i-1}}}{t+\zeta_1^{q^{d+i-2}}}, \ \ 1 \le i \le d-1$
$p_d \in \overline{\mathbb{F}}_q[t]_{(t)}$	$p_d := \frac{t+\zeta}{t+\zeta^q}$
$\tilde{p}_i \in \overline{\mathbb{F}}_q[t]_{(t)}$	$\tilde{p}_i := \frac{t+\alpha^{q^{i-1}}}{t+\alpha^{q^{m+i-1}}}, \ \ 1 \le i \le m$
	$\tilde{p}_{m+i} := \frac{t+\beta^{q^{i-1}}}{t+\beta^{q^{m+i-1}}}, \ \ 1 \le i \le m$

t_1	$t_1 := \mathrm{diag}(p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1})^{g_1}$
t_1'	$t_1' := \mathrm{diag}(p_1, \ldots, p_{d-1}, p_d^{-1}, p_d, p_{d-1}^{-1}, \ldots, p_1^{-1})^{g_1}$
t_2	$t_2 := \mathrm{diag}(\tilde{p}_1, \ldots, \tilde{p}_d, \tilde{p}_d^{-1}, \ldots, \tilde{p}_1^{-1})^{g_2}$
t_2'	$t_2' := \mathrm{diag}(\tilde{p}_1, \ldots, \tilde{p}_{d-1}, \tilde{p}_d^{-1}, \tilde{p}_d, \tilde{p}_{d-1}^{-1}, \ldots, \tilde{p}_1^{-1})^{g_2'}$

Then

a) t_1 and t_1' are contained in $T_1(\mathbb{F}_q[t]_{(t)})$, t_2 is contained in $T_2(\mathbb{F}_q[t]_{(t)})$ and t_2' is contained in $T_2'(\mathbb{F}_q[t]_{(t)})$.

b) The centralizers of the constant parts of t_1 and t_1' both equal T_1, and t_1 and t_1' both generate dense subgroups of T_1. The centralizers of the constant parts of t_2 and t_2' equal T_2 and T_2', resp., and t_2 and t_2' generate dense subgroups of T_2 and T_2'.

c) There exist $h_1, \ldots, h_d \in \mathbb{F}_q[t]_{(t)}$ *with* $h_d \in \mathbb{F}_q[t]^\times_{(t)}$ *such that* $D_{(h_1,\ldots,h_d)}$ *is conjugate to either* t_1 *or* t_1' *over* $\mathrm{SO}_n(\overline{\mathbb{F}}_q[[t]])$. *Similarly, there exist* $\tilde{h}_1, \ldots, \tilde{h}_d \in \mathbb{F}_q[t]_{(t)}$ *with* $\tilde{h}_d \in \mathbb{F}_q[t]^\times_{(t)}$ *such that* $D_{(\tilde{h}_1,\ldots,\tilde{h}_d)}$ *is conjugate to either* t_2 *or* t_2' *over* $\mathrm{SO}_n(\overline{\mathbb{F}}_q[[t]])$.

Proof. a) First of all, note that the diagonal matrices corresponding to t_1, t_1', t_2 and t_2' are all contained $T_0 \leq \mathrm{SO}_{2d}$. Now g_1, g_2 and g_2' are contained in $\mathrm{SO}_{2d}(\overline{\mathbb{F}}_q)$ and $p_1, \ldots, p_d$ as well as $\tilde{p}_1, \ldots, \tilde{p}_d$ are contained in $\overline{\mathbb{F}}_q[t]^\times_{(t)}$ hence $t_1 \in T_1(\overline{\mathbb{F}}_q[t]_{(t)})$, $t_1' \in T_1(\overline{\mathbb{F}}_q[t]_{(t)})$, $t_2 \in T_2(\overline{\mathbb{F}}_q[t]_{(t)})$ and $t_2' \in T_2'(\overline{\mathbb{F}}_q[t]_{(t)})$. It remains to show that all of them are $\mathbb{F}_q[t]_{(t)}$-rational. Recall that $g_i\phi_q(g_i)^{-1} = w_i$ holds for $i = 1, 2$, where w_1 and w_2 were defined in Chapter 4 to be monomial matrices inside $\mathrm{SO}_{2d}(\mathbb{F}_q)$ corresponding to the permutations

d odd	$\sigma_1 = (d, d+1)(1, \ldots, d-1, 2d, \ldots, d+2)$ $\sigma_2 = (1, \ldots, d)(2d, \ldots, d+1)$
$d = 2m$, m odd	$\sigma_1 = (d, d+1)(1, \ldots, d-1, 2d, \ldots, d+2)$ $\sigma_2 = (1, \ldots, m)(m+1, \ldots, 2m)(3m, \ldots, 2m+1)(4m, \ldots, 3m+1)$
$d = 2m$, m even	$\sigma_1 = (d, d+1)(1, \ldots, d-1, 2d, \ldots, d+2)$ $\sigma_2 = (1, \ldots, m, 4m, \ldots, 3m+1)(m+1, \ldots, 2m, 3m, \ldots, 2m+1)$

Besides, we have $g_2'\phi_q(g_2')^{-1} = w_2'$ where w_2' corresponds to the permutation $\sigma_2' = (k, k+1)\sigma_2(k, k+1)$. We use the following labels:

$$p_1, \ldots, p_{2d} \leftrightarrow p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1}$$

and also

$$p_1', \ldots, p_{2d}' \leftrightarrow p_1, \ldots, p_{d-1}, p_{d+1}, p_d, p_{d+2}, \ldots, p_{2d}$$

and similarly $\tilde{p}_1, \ldots, \tilde{p}_{2d}$ and $\tilde{p}_1', \ldots, \tilde{p}_{2d}'$. It is now straight-forward to check that

$$\phi_q(p_1, \ldots, p_{2d}) = (p_{\sigma_1(1)}, \ldots, p_{\sigma_1(2d)})$$

as well as

$$\phi_q(p_1', \ldots, p_{2d}') = (p_{\sigma_1(1)}', \ldots, p_{\sigma_1(2d)}')$$

holds and similarly

$$\phi_q(\tilde{p}_1, \ldots, \tilde{p}_{2d}) = (\tilde{p}_{\sigma_2(1)}, \ldots, \tilde{p}_{\sigma_2(2d)})$$

$$\phi_q(\tilde{p}_1', \ldots, \tilde{p}_{2d}') = (\tilde{p}_{\sigma_2'(1)}', \ldots, \tilde{p}_{\sigma_2'(2d)}')$$

(this has to be checked for all three cases of d). Hence $\phi_q(t_1) = \phi_q(\mathrm{diag}(p_1, \ldots, p_{2d}))^{\phi_q(g_1)} = \mathrm{diag}(p_{\sigma_1(1)}, \ldots, p_{\sigma_1(2d)})^{w_1^{-1}g_1} = t_1$ and similarly for t_1', t_2 and t_2'.

b) The centralizers of the constant parts of t_1 and t_1' equal T_1 if and only if $p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1}$ have pairwise distinct constant terms, which can be proven similarly as in the symplectic case (see Proposition 5.5.3). The same proof shows that $\tilde{p}_1, \ldots, \tilde{p}_d, \tilde{p}_d^{-1}, \ldots, \tilde{p}_1^{-1}$ have pairwise distinct constant terms in case d is odd. If d is even, this follows from Lemma 5.7.5. Hence the centralizer of the constant part of t_2 equals T_2 in both cases and the centralizer of the constant part of t_2' equals T_2'.
It remains to show that t_1, t_1', t_2 and t_2' generate dense subgroups of the corresponding maximal tori T_1, T_2 and T_2' which is the case if and only if no non-trivial character of T_0 maps the corresponding diagonal matrices to 1, by Lemma 4.2.6. Again, this can be shown very similar as in the proof of Proposition 5.5.3.

c) By Lemma 5.7.1, there exist elements $h_1, \ldots, h_d \in \overline{\mathbb{F}}_q[t]_{(t)}$ with $h_d \in \overline{\mathbb{F}}_q[t]_{(t)}^\times$ such that $D_{(h_1,\ldots,h_d)}$ is conjugate to either $\mathrm{diag}(p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1})$ or $\mathrm{diag}(p_1, \ldots, p_{d-1}, p_d^{-1}, p_d, p_{d-1}^{-1} \ldots, p_1^{-1})$ over $\mathrm{SO}_n(\overline{\mathbb{F}}_q[[t]])$. We first show that all h_i are contained in $\mathbb{F}_q[t]_{(t)}$. According to Lemma 5.7.1c), it is sufficient to show that $\prod_{i=1}^{d}(X - p_i)(X - p_i^{-1})$ is contained in $\mathbb{F}_q[t]_{(t)}[X]$ and $\Delta := \prod_{i=1}^{d}(1-p_i)(1+p_i^{-1})$ is contained in $\mathbb{F}_q[t]_{(t)}$. Clearly, $\prod_{i=1}^{d}(X - p_i)(X - p_i^{-1})$ is contained in $\mathbb{F}_q[t]_{(t)}[X]$ as this is the characteristic polynomial of $t_1 \in T_1(\mathbb{F}_q[t]_{(t)})$. Then

$$\begin{aligned}
\phi_q(\Delta) &= \phi_q((1-p_1)(1+p_1^{-1}) \cdots (1-p_d)(1+p_d^{-1})) \\
&= (1-p_2)(1+p_2^{-1}) \cdots (1-p_{d-1})(1+p_{d-1}^{-1}) \cdot \\
&\quad (1-p_1^{-1})(1+p_1)(1-p_d^{-1})(1+p_d) \\
&= \Delta \frac{(1-p_1^{-1})(1+p_1)(1-p_d^{-1})(1+p_d)}{(1-p_1)(1+p_1^{-1})(1-p_d)(1+p_d^{-1})} \\
&= \Delta \frac{(p_1-1)(1+p_1)(p_d-1)(1+p_d)}{(1-p_1)(p_1+1)(1-p_d)(p_d+1)} \\
&= \Delta,
\end{aligned}$$

hence Δ is contained in $\mathbb{F}_q[t]_{(t)}$. We conclude that there exist elements $h_1, \ldots, h_d \in \mathbb{F}_q[t]_{(t)}$ (with h_d invertible) such that $D_{(h_1,\ldots,h_d)}$ is conjugate to either $\mathrm{diag}(p_1, \ldots, p_{2d})$ or $\mathrm{diag}(p_1', \ldots, p_{2d}')$ via an element $g \in \mathrm{SO}_n(\overline{\mathbb{F}}_q[[t]])$. As g_1 is contained in $\mathrm{SO}_n(\overline{\mathbb{F}}_q)$, we conclude that $D_{(h_1,\ldots,h_d)}$ is conjugate to either t_1 or t_1' via $gg_1 \in \mathrm{SO}_n(\overline{\mathbb{F}}_q[[t]])$.

Similarly, it can be shown that there exist $\tilde{h}_1, \ldots, \tilde{h}_d \in \mathbb{F}_q[t]_{(t)}$ with $\tilde{h}_d \in \mathbb{F}_q[t]_{(t)}^\times$ such that $D_{(\tilde{h}_1,\ldots,\tilde{h}_d)}$ is conjugate to either $\mathrm{diag}(\tilde{p}_1, \ldots, \tilde{p}_{2d})$

or $\mathrm{diag}(\tilde{p}'_1, \ldots, \tilde{p}'_{2d})$ via an element $\tilde{g} \in \mathrm{SO}_n(\overline{\mathbb{F}}_q[[t]])$ (where the computation $\phi_q(\Delta) = \Delta$ has to be done separately for all three cases of d). Hence $D_{(\tilde{h}_1,\ldots,\tilde{h}_d)}$ is conjugate to either t_2 or t'_2 via $\tilde{g}g_2 \in \mathrm{SO}_n(\overline{\mathbb{F}}_q[[t]])$. □

5.7.4 A Difference Module for SO_{2d}

According to Proposition 5.7.6, we can now fix $\mathfrak{t}_1 \in \{t_1, t'_1\}$ and $\mathfrak{t}_2 \in \{t_2, t'_2\}$ such that there exist $(h_1, \ldots, h_d) \in \mathbb{F}_q[t]_{(t)}$ and $(\tilde{h}_1, \ldots, \tilde{h}_d) \in \mathbb{F}_q[t]_{(t)}$ with $h_d, \tilde{h}_d \in \mathbb{F}_q[t]^\times_{(t)}$ such that $D_{(h_1,\ldots,h_d)}$ is conjugate to $\mathfrak{t}_1$ over $\mathrm{SO}_n(\overline{\mathbb{F}}_q[[t]])$ and $D_{(\tilde{h}_1,\ldots,\tilde{h}_d)}$ is conjugate to $\mathfrak{t}_2$ over $\mathrm{SO}_n(\overline{\mathbb{F}}_q[[t]])$. We can now define the elements $f_1, \ldots, f_d \in F$ using these elements $(h_1, \ldots, h_d)$ and $(\tilde{h}_1, \ldots, \tilde{h}_d)$:

$a_{ij}, b_{ij} \in \mathbb{F}_q$	coefficients of h_i: $h_i(t) = \frac{\sum_{j=0}^{2d} a_{ij}t^j}{\sum_{j=0}^{2d} b_{ij}t^j}$; $b_{i0} \neq 0$ for all i
$\tilde{a}_{ij}, \tilde{b}_{ij} \in \mathbb{F}_q$	coefficients of $\tilde{h}_i$: $\tilde{h}_i(t) = \frac{\sum_{j=0}^{2d} \tilde{a}_{ij}t^j}{\sum_{j=0}^{2d} \tilde{b}_{ij}t^j}$; $\tilde{b}_{i0} \neq 0$ for all i
$H_i \in \mathbb{F}_q(t,s)$	$H_i := \frac{s\sum_{j=0}^{2d} a_{ij}t^j}{b_{i0}+s\sum_{j=1}^{2d} b_{ij}t^j}$, $1 \leq i \leq d$
$\tilde{H}_i \in \mathbb{F}_q(t,s)$	$\tilde{H}_i := \frac{-s\sum_{j=0}^{2d} \tilde{a}_{ij}t^j}{\tilde{b}_{i0}-s\sum_{j=1}^{2d} \tilde{b}_{ij}t^j}$, $1 \leq i \leq d$
$f_i \in F$	$f_i := \frac{s+1}{2}H_i + \frac{1-s}{2}\tilde{H}_i$, $1 \leq i \leq d-1$
	$f_d := \frac{s+1}{2}H_d + \frac{1-s}{2}\tilde{H}_d + (s+1)(1-s)$

Table 5.4: Definition of $f_1, \ldots, f_d$.

Theorem 5.7.7. *Assume q odd and $n = 2d \geq 8$ such that $(n,q) \neq (8,3)$. Let $M = (F^n, \Phi)$ be the ϕ_q-difference module over $F = \mathbb{F}_q(s,t)$ given by $D_{(f_1,\ldots,f_d)}$, where $f_i \in F$ are as defined in Table 5.4. Then there exists a Picard-Vessiot ring $R \subseteq \overline{\mathbb{F}_q(s)}^{\mathrm{sep}}((t)) \cap L$ for M such that R/F is separable and the Galois group scheme $\mathcal{G}_{M,R}$ of M with respect to R is isomorphic to SO_{2d} (as linear algebraic group over $\mathbb{F}_q(t)$).*

Proof. Having at hand Proposition 5.7.6, this can be proven in exactly the same way as Theorem 5.6.4. Indeed, the first three paragraphs of that proof provide a Picard-Vessiot ring $R \subseteq \overline{\mathbb{F}_q(s)}^{\mathrm{sep}}((t))$ with Galois group $\mathcal{H} =$

$\mathcal{G}_{M,R}$ a closed subgroup of SO_{2d} such that $\mathcal{H}(\mathbb{F}_q[[t]])$ contains $\mathrm{SO}_{2d}(\overline{\mathbb{F}}_q[[t]])$-conjugates of the specializations $D_{(h_1,\ldots,h_d)}$ and $D_{(\tilde{h}_1,\ldots,\tilde{h}_d)}$. By Proposition 5.7.6 together with Proposition 4.4.3, $\mathcal{H}(\mathbb{F}_q[[t]])$ then contains $\mathrm{SO}_{2d}(\mathbb{F}_q + t\overline{\mathbb{F}}_q[[t]])$-conjugates $\mathfrak{t}_1^A$ and $\mathfrak{t}_2^B$ of $\mathfrak{t}_1$ and $\mathfrak{t}_2$. Now $\mathfrak{t}_1$ generates a dense subgroup of T_1 and $\mathfrak{t}_2$ generates a dense subgroup of T_2 or T_2' (depending on whether $\mathfrak{t}_2 = t_2$ or $\mathfrak{t}_2 = t_2'$), by Proposition 5.7.6. Hence $\mathcal{H} \supseteq < T_1^A, T_2^B >$ or $\mathcal{H} \supseteq < T_1^A, T_2'^B >$. We have $< T_1^A, T_2^B >= \mathrm{SO}_{2d}$ by Theorem 4.2.5 and also $< T_1^A, T_2'^B >= \mathrm{SO}_{2d}$ by Theorem 5.7.4. We conclude $\mathcal{H} = \mathrm{SO}_{2d}$ in both cases. $\square$

5.8 The Dickson Group G_2

Let $\mathbb{O}$ be the octonion algebra over $\mathbb{F}_q$. Then the automorphism group of $\mathbb{O} \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ is a connected, simple linear algebraic group of type G_2, defined over $\mathbb{F}_q$ (with $\mathbb{F}_q$-rational points $\mathrm{Aut}(\mathbb{O})$). Details can be found in [SV00, 2.3]. We denote this linear algebraic group simply by G_2. After choosing a suitable basis of $\mathbb{O}$ (see [Wil09, 4.3.4]), G_2 is contained in SO_8, where SO_8 denotes the special orthogonal group with respect to the quadratic form

$$\overline{\mathbb{F}}_q^{\,8} \to \overline{\mathbb{F}}_q,\ (x_1, \ldots, x_8)^{\mathrm{tr}} \mapsto x_1x_8 + x_2x_7 + x_3x_6 + x_4x_5$$

(note that this also works for even q). Then G_2 acts on the hyperplane defined by $x_4 = x_5$ which gives rise to a faithful representation $G_2 \hookrightarrow \mathrm{SO}_7$ which is irreducible in case $\mathrm{char}(\mathbb{F}_q) \neq 2$. In the characteristic 2 case, $(0,0,0,1,0,0,0)^{\mathrm{tr}}$ spans a G_2-stable subspace of this latter representation and the action on the quotient yields an irreducible faithful representation $G_2 \hookrightarrow \mathrm{SO}_6$. In both cases, the diagonal matrices contained in G_2 define a maximal torus T_0. In the odd characteristic case, we have

$$T_0 = \{\mathrm{diag}(\lambda, \mu, \lambda\mu^{-1}, 1, \lambda^{-1}\mu, \mu^{-1}, \lambda^{-1}) \mid \lambda, \mu \in \overline{\mathbb{F}}_q^{\times}\}.$$

Similarly,

$$T_0 = \{\mathrm{diag}(\lambda, \mu, \lambda\mu^{-1}, \lambda^{-1}\mu, \mu^{-1}, \lambda^{-1}) \mid \lambda, \mu \in \overline{\mathbb{F}}_q^{\times}\}$$

if q is even. The root subgroups corresponding to the two simple roots α and β of G_2 with respect to T_0 are described explicitly in [Mal03] and it is easy to compute the corresponding reflections:

$$x_\alpha^{(\mathrm{odd})}(f) = \begin{pmatrix} 1 & f & & & & & \\ 0 & 1 & & & & & \\ & & 1 & f & -f^2 & & \\ & & 0 & 1 & -2f & & \\ & & 0 & 0 & 1 & & \\ & & & & & 1 & -f \\ & & & & & 0 & 1 \end{pmatrix}$$

$$w_\alpha^{(\mathrm{odd})} = \begin{pmatrix} 0 & 1 & & & & & \\ -1 & 0 & & & & & \\ & & 0 & 0 & -1 & & \\ & & 0 & -1 & 0 & & \\ & & -1 & 0 & 0 & & \\ & & & & & 0 & -1 \\ & & & & & 1 & 0 \end{pmatrix}$$

$$x_\beta^{(\mathrm{odd})}(f) = \begin{pmatrix} 1 & & & & & & \\ & 1 & f & & & & \\ & 0 & 1 & & & & \\ & & & 1 & & & \\ & & & & 1 & -f & \\ & & & & 0 & 1 & \\ & & & & & & 1 \end{pmatrix},$$

$$w_\beta^{(\mathrm{odd})} = \begin{pmatrix} 1 & & & & & & \\ & 0 & 1 & & & & \\ & -1 & 0 & & & & \\ & & & 1 & & & \\ & & & & 0 & -1 & \\ & & & & 1 & 0 & \\ & & & & & & 1 \end{pmatrix}.$$

We now choose a generic element $D_{(f_1,f_2)}^{(\mathrm{odd})} = x_\alpha^{(\mathrm{odd})}(f_1) w_\alpha^{(\mathrm{odd})} x_\beta^{(\mathrm{odd})}(f_2) w_\beta^{(\mathrm{even})}$ in the Steinberg cross section and compute

$$D_{(f_1,f_2)}^{(\mathrm{odd})} = \begin{pmatrix} -f_1 & -f_2 & 1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -f_1^2 & 0 & -f_1 & f_2 & 1 & 0 \\ 0 & -2f_1 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -f_1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

The characteristic polynomial of $D_{(f_1,f_2)}^{(\mathrm{odd})}$ is:

$$\begin{aligned} \chi_{(f_1,f_2)}^{(\mathrm{odd})}(X) &= (X-1)(X^6 + (f_1+2)X^5 + (2+2f_1-f_2)X^4 \\ &\quad +(2+2f_1-2f_2-f_1^2)X^3 \\ &\quad +(2+2f_1-f_2)X^2 + (f_1+2)X + 1). \end{aligned} \tag{5.18}$$

Similarly, for even q, we have

$$x_\alpha^{(\mathrm{even})}(f) = \begin{pmatrix} 1 & f & & & & \\ 0 & 1 & & & & \\ & & 1 & f^2 & & \\ & & 0 & 1 & & \\ & & & & 1 & f \\ & & & & 0 & 1 \end{pmatrix}, \quad w_\alpha^{(\mathrm{even})} = \begin{pmatrix} 0 & 1 & & & & \\ 1 & 0 & & & & \\ & & 0 & 1 & & \\ & & 1 & 0 & & \\ & & & & 0 & 1 \\ & & & & 1 & 0 \end{pmatrix}$$

$$x_\beta^{(\text{even})}(f) = \begin{pmatrix} 1 & & & & & \\ & 1 & f & & & \\ & 0 & 1 & & & \\ & & & 1 & f & \\ & & & 0 & 1 & \\ & & & & & 1 \end{pmatrix}, \quad w_\beta^{(\text{even})} = \begin{pmatrix} 1 & & & & & \\ & 0 & 1 & & & \\ & 1 & 0 & & & \\ & & & 0 & 1 & \\ & & & 1 & 0 & \\ & & & & & 1 \end{pmatrix}.$$

Again, we define $D_{(f_1,f_2)}^{(\text{even})} = x_\alpha^{(\text{even})}(f_1) w_\alpha^{(\text{even})} x_\beta^{(\text{even})}(f_2) w_\beta^{(\text{even})}$ and compute

$$D_{(f_1,f_2)}^{(\text{even})} = \begin{pmatrix} f_1 & f_2 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & f_1^2 & 0 & f_2 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & f_1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

The characteristic polynomial of $D_{(f_1,f_2)}^{(\text{even})}$ equals

$$\chi_{(f_1,f_2)}^{(\text{even})}(X) = X^6 + f_1 X^5 + f_2 X^4 + f_1^2 X^3 + f_2 X^2 + f_1 X + 1. \tag{5.19}$$

Proposition 5.8.1. *Let $\mathcal{H} \leq G_2$ be a linear algebraic group defined over $\mathbb{F}_q((t))$ such that for each $l \in 1 + 6\mathbb{N}$ there exist elements $h_l, \tilde{h}_l \in \mathcal{H}(\mathbb{F}_{q^l}[[t]])$ such that their constant parts $h_{l,0}, \tilde{h}_{l,0} \in G_2(\mathbb{F}_{q^l})$ are of order $q^{2l} + q^l + 1$ and $q^{2l} - q^l + 1$. Then $\mathcal{H} = G_2$.*

Proof. Set

$$\mathbb{F} := \bigcup_{l \in \mathbb{N}:\ l \equiv 1 \mod 6} \mathbb{F}_{q^l} \subseteq \overline{\mathbb{F}}_q.$$

By Lemma 4.2.3, $\mathbb{F}$ is a field of infinite order. We apply Proposition 4.2.2 to $K_1 = \mathbb{F}$ and $K_2 = \overline{\mathbb{F}}_q$ to conclude that it suffices to show that each $g \in G_2(\mathbb{F})$ appears as the constant part of an element inside $\mathcal{H}(\overline{\mathbb{F}}_q[[t]])$.

Let g be contained in $G_2(\mathbb{F})$. Then each coordinate of g is contained in some $\mathbb{F}_{q^l}$ for an integer $l \equiv 1 \mod 6$, so by taking the product of these l, we find that g is contained in $G_2(\mathbb{F}_{q^l})$ for some $l \in \mathbb{N}$, $l \equiv 1 \mod 6$. We may further assume that $q^l \geq 8$ holds by replacing l with $7l$ if this is not the case. By assumption there exist h_l and $\tilde{h}_l \in \mathcal{H}(\mathbb{F}_{q^l}[[t]]) \leq G_2(\mathbb{F}_{q^l}[[t]])$ with constant parts $h_{l,0}, \tilde{h}_{l,0} \in G_2(\mathbb{F}_{q^l})$ of order $q^{2l} + q^l + 1$ and $q^{2l} - q^l + 1$. (Note that $h_{l,0}$ and $\tilde{h}_{l,0}$ are contained in $G_2(\mathbb{F}_{q^l})$ since G_2 is defined over $\mathbb{F}_q \subseteq \mathbb{F}_{q^l}$.)

Let q' be an odd prime power with $q' > 3$. Then it follows from the list of maximal subgroups of $G_2(\mathbb{F}_{q'})$ in [Kle88, Thm.A] that any pair of elements of order $q'^2 + q' + 1$ and $q'^2 - q' + 1$ generates $G_2(\mathbb{F}_{q'})$. Similarly, if $q' \geq 8$ is a power of 2, it can easily be seen from the list of maximal

subgroups in [Coo81, 2.3-2.5.] that no proper subgroup of $G_2(\mathbb{F}_{q'})$ contains elements of order $q'^2+q'+1$ and $q'^2-q'+1$. Therefore, $h_{l,0}$ and $\tilde{h}_{l,0}$ generate $G_2(\mathbb{F}_{q^l})$, so there exist $r, \epsilon_i, \mu_i \in \mathbb{N}$ such that g can be written as

$$g = \prod_{i=1}^{r} h_{l,0}^{\epsilon_i} \tilde{h}_{l,0}^{\mu_i}.$$

Then

$$h := \prod_{i=1}^{r} h_l^{\epsilon_i} \tilde{h}_l^{\mu_i} \in \mathcal{H}(\mathbb{F}_{q^l}[[t]])$$

has constant part g which concludes the proof. □

5.8.1 Specializations of $D_{(f_1,f_2)}$

We will work with maximal tori splitting over $\mathbb{F}_{q^6}$, so we take a look at $\mathbb{F}_{q^6}[[t]]$-conjugacy.

Lemma 5.8.2. *Let q be odd.*
Let $p_1, p_2 \in \mathbb{F}_{q^6}[[t]]^\times$ be such that the constant terms of

$$p_1, p_2, p_1p_2^{-1}, 1, p_1^{-1}p_2, p_2^{-1}, p_1^{-1}$$

are pairwise distinct. Then there exist unique $h_1, h_2 \in \mathbb{F}_{q^6}[[t]]$ such that

$$(X-p_1)(X-p_2)(X-p_1p_2^{-1})(X-1)(X-p_1^{-1}p_2)(X-p_2^{-1})(X-p_1^{-1}) = \chi^{(\mathrm{odd})}_{(h_1,h_2)}(X)$$

holds and $D^{(\mathrm{odd})}_{(h_1,h_2)}$ and $\mathrm{diag}(p_1, p_2, p_1p_2^{-1}, 1, p_1^{-1}p_2, p_2^{-1}, p_1^{-1})$ are conjugate over $\mathrm{GL}_7(\mathbb{F}_{q^6}[[t]])$.

Proof. By Lemma 5.5.1, there exist $\tilde{h}_1, \tilde{h}_2, \tilde{h}_3 \in \mathbb{F}_{q^6}[[t]]$ such that

$$\begin{aligned} & (X-p_1)(X-p_2)(X-p_1p_2^{-1})(X-1)(X-p_1^{-1}p_2)(X-p_2^{-1})(X-p_1^{-1}) \\ = \; & (X-1)(X^6+\tilde{h}_1X^5+\tilde{h}_2X^4+\tilde{h}_3X^3+\tilde{h}_2X^2+\tilde{h}_1X+1) \end{aligned}$$

holds. We define

$$\begin{aligned} h_1 &:= \tilde{h}_1 - 2 \\ h_2 &:= -\tilde{h}_2 + 2 + 2(\tilde{h}_1 - 2). \end{aligned}$$

Using a computer algebra system such as magma ([BCP97]), it is now easy to compute that

$$\tilde{h}_3 = 2 + 2h_1 - 2h_2 - h_1^2$$

holds, and Equation (5.18) implies

$$(X-p_1)(X-p_2)(X-p_1p_2^{-1})(X-1)(X-p_1^{-1}p_2)(X-p_2^{-1})(X-p_1^{-1}) = \chi^{(\mathrm{odd})}_{(h_1,h_2)}(X)$$

and h_1, h_2 are uniquely determined by this equality. Now $D^{(\mathrm{odd})}_{(h_1,h_2)}$ and $\mathrm{diag}(p_1, p_2, p_1p_2^{-1}, 1, p_1^{-1}p_2, p_2^{-1}, p_1^{-1})$ have the same characteristic polynomial and their eigenvalues $p_1, p_2, p_1p_2^{-1}, 1, p_1^{-1}p_2, p_2^{-1}, p_1^{-1}$ are contained in $\mathbb{F}_{q^6}[[t]]$ with pairwise distinct constant terms, hence $D^{(\mathrm{odd})}_{(h_1,h_2)}$ and $\mathrm{diag}(p_1, p_2, p_1p_2^{-1}, 1, p_1^{-1}p_2, p_2^{-1}, p_1^{-1})$ are conjugate over $\mathrm{GL}_7(\mathbb{F}_{q^6}[[t]])$, by Proposition 5.2.2.

□

Lemma 5.8.3. *Let q be a power of 2.*
Let $p_1, p_2 \in \mathbb{F}_{q^6}[[t]]^\times$ be such that the constant terms of

$$p_1, p_2, p_1p_2^{-1}, p_1^{-1}p_2, p_2^{-1}, p_1^{-1}$$

are pairwise distinct. Then there exist unique $h_1, h_2 \in \mathbb{F}_{q^6}[[t]]$ such that

$$(X-p_1)(X-p_2)(X-p_1p_2^{-1})(X-p_1^{-1}p_2)(X-p_2^{-1})(X-p_1^{-1}) = \chi^{(\mathrm{even})}_{(h_1,h_2)}(X)$$

holds and $D^{(\mathrm{even})}_{(h_1,h_2)}$ and $\mathrm{diag}(p_1, p_2, p_1p_2^{-1}, p_1^{-1}p_2, p_2^{-1}, p_1^{-1})$ are conjugate over $\mathrm{GL}_6(\mathbb{F}_{q^6}[[t]])$.

Proof. By Lemma 5.5.1, there exist $h_1, h_2, h_3 \in \mathbb{F}_{q^6}[[t]]$ such that

$$\begin{aligned} & (X-p_1)(X-p_2)(X-p_1p_2^{-1})(X-p_1^{-1}p_2)(X-p_2^{-1})(X-p_1^{-1}) \\ = \;& X^6 + h_1X^5 + h_2X^4 + h_3X^3 + h_2X^2 + h_1X + 1 \end{aligned}$$

holds. Clearly, h_1 and h_2 are uniquely determined by this equation. It can now readily checked by hand that $h_3 = h_1^2$ holds, hence we have

$$(X-p_1)(X-p_2)(X-p_1p_2^{-1})(X-p_1^{-1}p_2)(X-p_2^{-1})(X-p_1^{-1}) = \chi^{(\mathrm{even})}_{(h_1,h_2)}(X),$$

by Equation (5.19). Again, it follows from Proposition 5.2.2 that $D^{(\mathrm{even})}_{(h_1,h_2)}$ and $\mathrm{diag}(p_1, p_2, p_1p_2^{-1}, p_1^{-1}p_2, p_2^{-1}, p_1^{-1})$ are conjugate over $\mathrm{GL}_6(\mathbb{F}_{q^6}[[t]])$. □

5.8.2 A Difference Module for G_2

q α	prime power ≥ 3 fixed element in $\mathbb{F}_q^\times \setminus \{1\}$
$\zeta_1 \in \mathbb{F}_{q^6}$ $\zeta_2 \in \mathbb{F}_{q^6}$	primitive (q^6-1)-th root of unity primitive (q^3-1)-th root of unity
$p_1, p_2 \in \mathbb{F}_{q^6}[t]_{(t)}$ $\tilde{p}_1, \tilde{p}_2 \in \mathbb{F}_{q^6}[t]_{(t)}$	$p_1 := \frac{(t+\zeta_1^{q^4})(t+\zeta_1^{q^3})}{(t+\zeta_1^q)(t+\zeta_1)},\ p_2 := \frac{(t+\zeta_1^{q^3})(t+\zeta_1^{q^2})}{(t+\zeta_1)(t+\zeta_1^{q^5})}$ $\tilde{p}_1 := \frac{t+\zeta_2^q}{t+\zeta_2},\ \tilde{p}_2 := \frac{t+\zeta_2^{q^2}}{t+\zeta_2}$
$h_1, h_2 \in \mathbb{F}_q[t]_{(t)}$ (*)	defined via $\chi^{(\text{odd})}_{(h_1,h_2)}(X) = (X-p_1)(X-p_2)(X-p_1p_2^{-1})\cdot$ $(X-1)(X-p_1^{-1}p_2)(X-p_2^{-1})(X-p_1^{-1})$ if q is odd and $\chi^{(\text{even})}_{(h_1,h_2)}(X) = (X-p_1)(X-p_2)(X-p_1p_2^{-1})\cdot$ $(X-p_1^{-1}p_2)(X-p_2^{-1})(X-p_1^{-1})$ if q is even
$\tilde{h}_1, \tilde{h}_2 \in \mathbb{F}_q[t]_{(t)}$ (*)	defined via $\chi^{(\text{odd})}_{(\tilde{h}_1,\tilde{h}_2)}(X) = (X-\tilde{p}_1)(X-\tilde{p}_2)(X-\tilde{p}_1\tilde{p}_2^{-1})\cdot$ $(X-1)(X-\tilde{p}_1^{-1}\tilde{p}_2)(X-\tilde{p}_2^{-1})(X-\tilde{p}_1^{-1})$ if q is odd and $\chi^{(\text{even})}_{(\tilde{h}_1,\tilde{h}_2)}(X) = (X-\tilde{p}_1)(X-\tilde{p}_2)(X-\tilde{p}_1\tilde{p}_2^{-1})\cdot$ $(X-\tilde{p}_1^{-1}\tilde{p}_2)(X-\tilde{p}_2^{-1})(X-\tilde{p}_1^{-1})$ if q is even.
$a_{ij}, b_{ij} \in \mathbb{F}_q$ $\tilde{a}_{ij}, \tilde{b}_{ij} \in \mathbb{F}_q$	coefficients of h_i: $h_i(t) = \frac{\sum_{j=0}^{12} a_{ij}t^j}{\sum_{j=0}^{12} b_{ij}t^j}$; $b_{i0} \neq 0$ coefficients of $\tilde{h}_i$: $\tilde{h}_i(t) = \frac{\sum_{j=0}^{12} \tilde{a}_{ij}t^j}{\sum_{j=0}^{12} \tilde{b}_{ij}t^j}$; $\tilde{b}_{i0} \neq 0$
$H_1, H_2 \in \mathbb{F}_q(t,s)$ $\tilde{H}_1, \tilde{H}_2 \in \mathbb{F}_q(t,s)$	$H_i := \frac{s\sum_{j=0}^{12} a_{ij}t^j}{b_{i0}+s\sum_{j=1}^{12} b_{ij}t^j}$ $\tilde{H}_i := \frac{\frac{s}{\alpha}\sum_{j=0}^{12} \tilde{a}_{ij}t^j}{\tilde{b}_{i0}+\frac{s}{\alpha}\sum_{j=1}^{12} \tilde{b}_{ij}t^j}$
$f_1, f_2 \in \mathbb{F}_q(t,s)$	$f_i := \frac{s-\alpha}{1-\alpha}H_i + \frac{s-1}{\alpha-1}\tilde{H}_i$

Table 5.5: Definition of f_1, f_2.

(*) h_1, h_2 exist inside $\mathbb{F}_{q^6}[[t]]$ by Lemma 5.8.2 and 5.8.3. As ϕ_q permutes $p_1, p_2, p_1p_2^{-1}, p_1^{-1}p_2, p_2^{-1}, p_1^{-1} \in \mathbb{F}_{q^6}[t]_{(t)}$, they are contained in $\mathbb{F}_q[t]_{(t)}$. Similarly, $\tilde{h}_1$ and $\tilde{h}_2$ are contained in $\mathbb{F}_q[t]_{(t)}$.

Theorem 5.8.4. *Assume $q \geq 3$ and set $n := 7$ in case q is odd and $n := 6$ in case q is even. Let $M = (F^n, \Phi)$ be the ϕ_q-difference module over $F = \mathbb{F}_q(s,t)$ with representing matrix D, where $D := D^{(\mathrm{odd})}_{(f_1,f_2)}$ if q is odd and $D := D^{(\mathrm{even})}_{(f_1,f_2)}$ if q is even and $f_1, f_2 \in F$ are as defined in Table 5.5. Then there exists a Picard-Vessiot ring $R \subseteq \overline{\mathbb{F}_q(s)}^{\mathrm{sep}}((t)) \cap L$ for M such that R/F is separable and the Galois group scheme $\mathcal{G}_{M,R}$ is isomorphic to G_2 (as linear algebraic group over $\mathbb{F}_q(t)$).*

Proof. Again, with the very same reasoning as in the first three paragraphs of the proof of 5.4.4 we first get a fundamental matrix inside $\mathrm{GL}_n(K[[t]])$ with entries in $\mathcal{O}_{|\cdot|}\{t\}$ and then a fundamental matrix Y inside $G_2(K[[t]] \cap L)$, where L is as defined in Section 5.1. Then $R := F[Y, Y^{-1}] \subseteq \overline{\mathbb{F}_q(s)}^{\mathrm{sep}}((t))$ is a separable Picard-Vessiot extension for M with $\mathcal{H} := \mathcal{G}_{M,R}$ a linear algebraic group contained in G_2.

Similar to the fourth paragraph of the proof of 5.4.4, we find that $\mathcal{H}(\mathbb{F}_q[[t]])$ contains $G_2(\overline{\mathbb{F}}_q[[t]])$-conjugates of $D_1 := D_{(h_1,h_2)}$ (via the specialization $s \mapsto 1$) and of $D_2 := D_{(\tilde{h}_1,\tilde{h}_2)}$ (via $s \mapsto \alpha$), where $D_{(h_1,h_2)}$ is understood to equal either $D := D^{(\mathrm{odd})}_{(h_1,h_2)}$ or $D := D^{(\mathrm{even})}_{(h_1,h_2)}$ depending on the parity of q. Let T_0 be the diagonal torus inside G_2 and let d_1 and d_2 denote the following elements of $T_0(\mathbb{F}_{q^6}[[t]])$:

$$\begin{aligned}
d_1 &:= \mathrm{diag}(p_1, p_2, p_1p_2^{-1}, 1, p_1^{-1}p_2, p_2^{-1}, p_1^{-1}) \text{ for odd } q\\
d_2 &:= \mathrm{diag}(\tilde{p}_1, \tilde{p}_2, \tilde{p}_1\tilde{p}_2^{-1}, 1, \tilde{p}_1^{-1}\tilde{p}_2, \tilde{p}_2^{-1}, \tilde{p}_1^{-1}) \text{ for odd } q\\
d_1 &:= \mathrm{diag}(p_1, p_2, p_1p_2^{-1}, p_1^{-1}p_2, p_2^{-1}, p_1^{-1}) \text{ for even } q\\
d_2 &:= \mathrm{diag}(\tilde{p}_1, \tilde{p}_2, \tilde{p}_1\tilde{p}_2^{-1}, \tilde{p}_1^{-1}\tilde{p}_2, \tilde{p}_2^{-1}, \tilde{p}_1^{-1}) \text{ for even } q.
\end{aligned}$$

The constant parts of d_1 and d_2 have pairwise distinct eigenvalues. Indeed, the constant part of d_1 has diagonal entries $\zeta_1^{q^4+q^3-q-1}$, $\zeta_1^{-q^5+q^3+q^2-1}$, $\zeta_1^{q^5+q^4-q^2-q}$, 1, $\zeta_1^{-q^5-q^4+q^2+q}$, $\zeta_1^{q^5-q^3-q^2+1}$, $\zeta_1^{-q^4-q^3+q+1}$ (where the 1 in the middle only occurs if q is odd). Since ζ_1 is a primitive $(q^6-1) = (q^2-q+1)(q^4+q^3-q-1)$-th root of unity, $\mu_1 := \zeta_1^{q^4+q^3-q-1}$ is a primitive q^2-q+1 root of unity and the diagonal entries of the constant part of d_1 are $\mu_1, \mu_1^{-q+1}, \mu_1^q, 1,\ \mu_1^{-q}, \mu_1^{q-1}, \mu_1^{-1}$ so they are all pairwise distinct (since $q \geq 3$). Similarly, $\mu_2 := \zeta_2^{q-1}$ is a primitive (q^2+q+1)-th root of unity and the constant part of d_2 has pairwise distinct diagonal entries μ_2, $\mu_2^{-q^2}$, μ_2^{-q}, 1, μ_2^q, $\mu_2^{q^2}$, μ_2^{-1}.

Hence we can apply Lemma 5.8.2 and 5.8.3 and obtain matrices $A_1, A_2 \in \mathrm{GL}_n(\mathbb{F}_{q^6}[[t]])$ satisfying

$$\begin{aligned} D_1 = D_{(h_1,h_2)} &= d_1^{A_1} \\ D_2 = D_{(\tilde{h}_1,\tilde{h}_2)} &= d_2^{A_2}. \end{aligned}$$

Hence $\mathcal{H}(\mathbb{F}_q[[t]])$ (which contains $G_2(\overline{\mathbb{F}}_q[[t]])$-conjugates of D_1 and D_2) contains also $\mathrm{GL}_n(\overline{\mathbb{F}}_q[[t]])$-conjugates of d_1 and d_2. On the other hand, the centralizers of the constant parts of d_1 and d_2 inside GL_2 equal the diagonal torus (as their eigenvalues are pairwise distinct), hence $\mathcal{H}(\mathbb{F}_q[[t]])$ even contains $\mathrm{GL}_n(\mathbb{F}_{q^6} + \overline{\mathbb{F}}_q[[t]])$-conjugates of d_1 and d_2, by Proposition 4.4.3 applied to $\mathcal{G} = \mathrm{GL}_n$. Let $B_1, B_2 \in \mathrm{GL}_n(\mathbb{F}_{q^6} + \overline{\mathbb{F}}_q[[t]])$ be such that $d_i^{B_i}$ is contained in $\mathcal{H}(\mathbb{F}_q[[t]])$.

The character group of T_0 is generated by χ_1 and χ_2, so no non-trivial character can map d_1 or d_2 to 1 since $(t+\zeta_1^{q^i})$ are pairwise coprime (inside $\mathbb{F}_{q^6}[t]$) for $0 \le i \le 5$ and similarly $(t+\zeta_2^{q^i})$ for $0 \le i \le 2$. We conclude that both d_1 and d_2 generate dense subgroups of T_0, by Lemma 4.2.6. Therefore, $d_i^{B_i}$ generates a dense subgroup of $T_0^{B_i} \subseteq \mathrm{GL}_n$ with respect to the Zariski topology inside GL_n. As $d_i^{B_i}$ is contained in $\mathcal{H}$, we conclude that $\mathcal{H} \le G_2$ contains $< T_0^{B_1}, T_0^{B_2} >$. In particular $T_1 := T_0^{B_1}$ and $T_2 := T_0^{B_2}$ are both contained in G_2, so they are maximal tori of G_2 (even though B_1 and B_2 may not be contained in G_2). The subgroup generated by $d_i^{B_i}$ consists of $\mathbb{F}_q((t))$-rational points and is dense in $T_0^{B_i}$, hence $T_0^{B_i}$ is defined over $\mathbb{F}_q((t))$ (see [Bor91, AG.14.4]). We use $B_i \in \mathrm{GL}_n(\overline{\mathbb{F}}_q(((t)))$ to get $T_i(\overline{\mathbb{F}}_q((t))) = T_0(\overline{\mathbb{F}}_q((t)))^{B_i}$ and deduce

$$T_0(\overline{\mathbb{F}}_q((t)))^{B_i} = \phi_q(T_0^{B_i}(\overline{\mathbb{F}}_q((t)))) = T_0(\overline{\mathbb{F}}_q((t)))^{\phi_q(B_i)} \tag{5.20}$$

where we also used that T_0 is defined over $\mathbb{F}_q \subseteq \mathbb{F}_q((t))$. Now $T_0(\overline{\mathbb{F}}_q((t)))$ is dense in T_0 (see [Bor91, Cor.18.3]), hence $w_i := B_i\phi_q(B_i)^{-1}$ is contained in the normalizer of T_0 inside GL_n. As T_0 contains diagonal matrices with pairwise distinct entries such as d_1 and d_2, this normalizer consists of certain monomial matrices inside GL_n. Let $\sigma_1, \sigma_2 \in S_n$ be the permutations corresponding to w_1 and w_2. We can now describe the $\mathbb{F}_q((t))$-rational points of T_i $(i = 1, 2)$ explicitly:

$$\begin{aligned} T_i(\mathbb{F}_q((t))) &= \{g \in T_i(\overline{\mathbb{F}}_q((t))) \mid \phi_q(g) = g\} \\ &= \{g = g_0^{B_i} \in T_0(\overline{\mathbb{F}}_q((t)))^{B_i} \mid \phi_q(g_0^{B_i}) = g_0^{B_i}\} \\ &= \{g_0 \in T_0(\overline{\mathbb{F}}_q((t))) \mid \phi_q(g_0) = g_0^{\sigma_i}\}^{B_i}. \end{aligned}$$

Now $d_i^{B_i}$ is contained in $T_i(\mathbb{F}_q((t)))$, hence $\phi_q(d_i) = d_i^{\sigma_i}$ and we can determine σ_i: We relabel the entries of d_1 and d_2 as

$$\begin{aligned} d_1 &= \mathrm{diag}(p_1, p_2, p_3, (1,)\ p_{-3}, p_{-2}, p_{-1}) \\ d_1 &= \mathrm{diag}(\tilde{p}_1, \tilde{p}_2, \tilde{p}_3, (1,)\ \tilde{p}_{-3}, \tilde{p}_{-2}, \tilde{p}_{-1}), \end{aligned}$$

i.e., $p_3 := p_1 p_2^{-1}$, $p_{-i} := p_i^{-1}$ and similarly for $\tilde{p}_i$. We compute $\phi_q(p_1) = p_3$, $\phi_q(p_3) = p_{-2}$, $\phi_q(p_{-2}) = p_{-1}$, $\phi_q(p_{-1}) = p_{-3}$, $\phi_q(p_{-3}) = p_2$, $\phi_q(p_2) = p_1$, hence

$$\sigma_1 = (1, 3, -2, -1, -3, 2).$$

Similarly, $\phi_q(\tilde{p}_{\pm 1}) = \tilde{p}_{\mp 3}$, $\phi_q(\tilde{p}_{\mp 3}) = \tilde{p}_{\mp 2}$, $\phi_q(\tilde{p}_{\mp 2}) = \tilde{p}_{\pm 1}$, i.e.,

$$\sigma_2 = (1, -3, -2)(-1, 3, 2).$$

For $l \equiv 1 \mod 6$, we have $\sigma_i^l = \sigma_i$ and $B_i \phi_{q^l}(B_i)^{-1} = B_i \phi_{q^{l-1}}(B_i^{-1} w_i) = \cdots = \phi_{q^{l-1}}(w_i) \ldots \phi_q(w_i) w_i$. As each $\phi_{q^j}(w_i)$ is monomial with respect to σ_i, the product $\phi_{q^{l-1}}(w_i) \ldots \phi_q(w_i) w_i$ is monomial with respect to $\sigma_i^l = \sigma_i$. Hence $B_i \phi_{q^l}(B_i)^{-1}$ is monomial with respect to σ_i for both $i = 1, 2$ and we get

$$\begin{aligned} T_i(\mathbb{F}_{q^l}[[t]]) &= \{g \in T_i(\overline{\mathbb{F}}_q[[t]]) \mid \phi_{q^l}(g) = g\} \\ &= \{g = g_0^{B_i} \in T_0(\overline{\mathbb{F}}_q[[t]])^{B_i} \mid \phi_{q^l}(g_0^{B_i}) = g_0^{B_i}\} \\ &= \{g_0 \in T_0(\overline{\mathbb{F}}_q[[t]]) \mid \phi_{q^l}(g_0) = g_0^{\sigma_i}\}^{B_i} \end{aligned} \tag{5.21}$$

for all $l \equiv 1 \mod 6$. Fix primitive $(q^{2l} - q^l + 1)$-th roots of unity γ_l and $(q^{2l} + q + 1)$-th roots of unity ξ_l inside $\overline{\mathbb{F}}_q$ for all $l \equiv 1 \mod 6$ and set

$$\begin{aligned} x_l &:= \operatorname{diag}(\gamma_l, \gamma_l^{-(q^l)^2}, \gamma_l^{q^l}, (1,)\, \gamma_l^{-(q^l)}, \gamma_l^{(q^l)^2}, \gamma_l^{(q^l)^3}) \\ y_l &:= \operatorname{diag}(\xi_l, \xi_l^{-(q^l)^2}, \xi_l^{-q^l}, (1,)\, \xi_l^{q^l}, \xi_l^{(q^l)^2}, \xi^{-1}). \end{aligned}$$

Then $\gamma_l^{(q^l)^3} = \gamma_l^{-1}$ and $\xi_l^{(q^l)^3} = \xi_l$, hence

$$\begin{aligned} \phi_{q^l}(x_l) &= x_l^{\sigma_1} \\ \phi_{q^l}(y_l) &= y_l^{\sigma_2} \end{aligned}$$

and x_l and y_l are both contained in $T_0 \subseteq G_2$. Hence Equation (5.21) implies that $x_l^{B_1} \in T_1(\mathbb{F}_{q^l}[[t]])$ and $y_l^{B_2} \in T_2(\mathbb{F}_{q^l}[[t]])$ for all $l \equiv 1 \mod 6$. Note that x_l and y_l have order $q^{2l} - q^l + 1$ and $q^{2l} + q^l + 1$, resp. As T_1 and T_2 are contained in $\mathcal{H}$, we conclude that $\mathcal{H}(\mathbb{F}_{q^l}[[t]])$ contains the elements $x_l^{B_1}$ and $y_l^{B_2}$ whose constant terms are of order $q^{2l} \pm q^l + 1$ (as they are conjugate to x_l and y_l). Therefore, $\mathcal{H} = G_2$ by Proposition 5.8.1. □

Chapter 6

A General Result

In this chapter, we prove that every semisimple, simply-connected group defined over $\mathbb{F}_q$ can be realized as a difference Galois group over $(\mathbb{F}_{q^i}(s,t), \phi_{q^i})$ for some $i \in \mathbb{N}$. This number i has to be chosen in such a way that the following holds:

- $\mathcal{G}$ splits over an intermediate field $\mathbb{F}_q \subseteq \mathbb{F}_{q'} \subseteq \mathbb{F}_{q^i}$
- there exists a regular element $g_0 \in \mathcal{G}(\mathbb{F}_{q'})$ contained in a maximal torus that splits over $\mathbb{F}_{q'}$
- a certain place $\mathfrak{p}$ of $\mathbb{F}_{q'}(s)$ (depending on g_0) splits into places of degree 1 inside $\mathbb{F}_{q^i}(s)$.

The strategy is to use a Theorem due to Nori that provides us with a finite Galois extension of $\mathbb{F}_{q^i}(s)$ with Galois group $\mathcal{G}(\mathbb{F}_{q'})$ and then lift this to a difference module over $\mathbb{F}_{q^i}(s,t)$ with Galois group scheme $\mathcal{G}$ using Theorem 4.3.1.

6.1 Galois Coverings of the Affine Line

The following result due to Nori can be found in [Nor94].

Theorem 6.1.1 (Nori)**.** *Let $\mathcal{G}$ be a semisimple and simply-connected linear algebraic group defined over a finite field $\mathbb{F}_q$. Then there is an absolutely irreducible unramified Galois covering of the affine line with Galois group $\mathcal{G}(\mathbb{F}_q)$.*

Recall that a ϕ_q-difference module over $(\mathbb{F}_q(s), \phi_q)$ is called a finite Frobenius module over $(\mathbb{F}_q(s), \phi_q)$. Any finite Frobenius module has a unique Picard-Vessiot ring inside $\overline{\mathbb{F}_q(s)}^{\text{sep}}$. The Picard-Vessiot ring E is then a finite Galois extension of $\mathbb{F}_q(s)$ which we call the Picard-Vessiot extension. The $\mathbb{F}_q$-rational points of the corresponding (finite) Galois group scheme

$\mathcal{G} \leq \mathrm{GL}_n$ are isomorphic to $\mathrm{Gal}(E/F)$ via identifying $\gamma \in \mathrm{Gal}(E/F)$ with $Y^{-1}\gamma(Y) \in \mathcal{G}(\mathbb{F}_q)$, where $Y \in \mathrm{GL}_n(E)$ denotes a fixed fundamental solution matrix (see Proposition 1.3.11). Every finite Galois extension can be obtained in this way using additive polynomials. Details can be found in [Mat04].

Corollary 6.1.2. *Let $\mathcal{G}$ be a semisimple, simply-connected linear algebraic group defined over $\mathbb{F}_q$. Then there exists a finite Frobenius module over $(\mathbb{F}_q(s), \phi_q)$ with representing matrix contained in $\mathcal{G}(\mathbb{F}_q(s))$, Picard-Vessiot extension $E/\mathbb{F}_q(s)$ linearly disjoint from $\overline{\mathbb{F}}_q$ over $\mathbb{F}_q$, and Galois group $\mathcal{G}(\mathbb{F}_q)$.*

Proof. By Theorem 5.2. in [Mat04], there exists an effective, finite Frobenius module corresponding to the Galois covering provided by Theorem 6.1.1, i.e., the representing matrix can be chosen inside $\mathcal{G}(\mathbb{F}_q(s))$. The Picard-Vessiot extension E is linearly disjoint from $\overline{\mathbb{F}}_q$ over $\mathbb{F}_q$ since the corresponding Galois covering is absolutely irreducible. □

6.2 The Finite Part

The following lower bound criterion for finite Frobenius modules due to Matzat can be found in [Mat04, Thm 4.5]. It also holds over finite extensions of $\mathbb{F}_q(s)$.

Theorem 6.2.1. *Let M be a finite Frobenius module over $(\mathbb{F}_q(s), \phi_q)$ with representing matrix $D \in \mathrm{GL}_n(\mathbb{F}_q(s))$ and Picard-Vessiot extension $E/\mathbb{F}_q(s)$. We fix a fundamental solution matrix $Y \in \mathrm{GL}_n(E)$. Let $\mathfrak{p}$ be a place of degree d of $\mathbb{F}_q(s)$ with corresponding valuation ring $\mathfrak{o} \subseteq \mathbb{F}_q(s)$. If D is contained in $\mathrm{GL}_n(\mathfrak{o})$ then the following holds:*

- *$E/\mathbb{F}_q(s)$ is unramified at $\mathfrak{p}$.*
- *For any extension $(\mathcal{O}, \mathcal{P})$ of $(\mathfrak{o}, \mathfrak{p})$ to E, Y is contained in $\mathrm{GL}_n(\mathcal{O})$.*
- *The Galois group $\mathrm{Gal}(E/\mathbb{F}_q(s)) \leq \mathrm{GL}_n(\mathbb{F}_q)$ of M contains the reduction of $Y^{-1}D\phi_q(D)\cdots\phi_{q^{d-1}}(D)Y$ modulo $\mathcal{P}$.*

The following Proposition provides a converse to Theorem 6.2.1:

Proposition 6.2.2. *Let M be a finite Frobenius module over $(\mathbb{F}_q(s), \phi_q)$ with representing matrix $D \in \mathrm{GL}_n(\mathbb{F}_q(s))$, Picard-Vessiot extension $E/\mathbb{F}_q(s)$, and Galois group $G \leq \mathrm{GL}_n(\mathbb{F}_q)$. We fix a fundamental solution matrix $Y \in \mathrm{GL}_n(E)$. Then there exist finitely many finite places $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$ of $\mathbb{F}_q(s)$ of degree $d_1, \ldots, d_l$, resp., such that the following holds:*

- *For $1 \leq j \leq l$, D is contained in $\mathrm{GL}_n(\mathfrak{o}_j)$, where $\mathfrak{o}_j$ denotes the valuation ring corresponding to $\mathfrak{p}_j$.*

- *For every $g \in G$ there exists an $j \leq l$ and an extension $\mathcal{P}_j$ of $\mathfrak{p}_j$ from $\mathbb{F}_q(s)$ to E such that g equals*

$$Y^{-1}D\phi_q(D)\cdots\phi_{q^{d_j-1}}(D)Y \mod \mathcal{P}_j.$$

The number l can be chosen as the number of conjugacy classes inside G.

Proof. Whenever we have a place $\mathfrak{p}$ or $\mathcal{P}$, we denote the corresponding valuation rings by $\mathfrak{o}$ and $\mathcal{O}$, resp.

Every entry of D has only finitely many poles and $\det(D)$ has only finitely many zeroes, hence $D \in \mathrm{GL}_n(\mathfrak{o})$ for all but finitely many places $\mathfrak{p}$ of $\mathbb{F}_q(s)$.

Let $g \in G \leq \mathrm{GL}_n(\mathbb{F}_q)$. Then g is of the form $g = Y^{-1}\gamma(Y)$ for an element $\gamma \in \mathrm{Gal}(E/\mathbb{F}_q(s))$. The Chebotarev Density Theorem (see [FJ08, Thm 6.3.1]) implies that there exist infinitely many places $\mathfrak{p}$ such that γ equals the Frobenius automorphism at some extension $\mathcal{P}$ of $\mathfrak{p}$. Hence there exists an (unramified) finite place $\mathfrak{p}$ of $\mathbb{F}_q(s)$ with an extension $\mathcal{P}$ to E such that $D \in \mathrm{GL}_n(\mathfrak{o})$ and such that γ is contained in the decomposition group of $\mathcal{P}/\mathfrak{p}$ and acts as ϕ_{q^d} on $\mathcal{O}/\mathcal{P}$ where d denotes the degree of $\mathfrak{p}$. We abbreviate the reduction modulo $\mathcal{P}$ of an element $x \in \mathcal{O}$ by $\overline{x}$. We use $g \in \mathrm{GL}_n(\mathbb{F}_q)$ and compute

$$\begin{aligned} g &= \overline{g} \\ &= \overline{Y^{-1}\gamma(Y)} \\ &= \overline{Y^{-1}} \cdot \overline{\gamma(Y)} \\ &= \overline{Y}^{-1}\phi_{q^d}(\overline{Y}), \end{aligned} \tag{6.1}$$

where we used that Y is contained in $\mathrm{GL}_n(\mathcal{O})$ by Theorem 6.2.1. Now Y is a fundamental solution matrix, hence $\phi_q(Y) = D^{-1}Y$. Inductively, we get

$$\begin{aligned} \phi_{q^d}(Y) &= \phi_{q^{d-1}}(D^{-1})\cdots\phi_q(D^{-1})D^{-1}Y \\ &= (D\phi_q(D)\cdots\phi_{q^{d-1}}(D))^{-1}Y. \end{aligned}$$

Evaluating Equation (6.1), we get

$$g = \overline{Y}^{-1}(\overline{D}\phi_q(\overline{D})\cdots\phi_{q^{d-1}}(\overline{D}))^{-1}\overline{Y}.$$

Replacing g by g^{-1}, we see that g equals the reduction of $Y^{-1}D\phi_q(D)\cdots\phi_{q^{d-1}}(D)Y$ modulo $\mathcal{P}$. As $\mathcal{P}$ ranges over the extensions of $\mathfrak{p}$, the reductions of $Y^{-1}D\phi_q(D)\cdots\phi_{q^{d-1}}(D)Y$ range over the conjugates of $\gamma \in \mathrm{Aut}(E/F)$. Let $\mathcal{C}_1, \ldots, \mathcal{C}_l$ denote the conjugacy classes of G. Then for each $j \leq l$, we can choose a place $\mathfrak{p}_j$ as above. □

We can now describe our approach to realize a semisimple, simply-connected group $\mathcal{G}$ defined over $\mathbb{F}_q$ as a difference Galois group over $\mathbb{F}_q(s,t)$: First, we use Nori's result 6.1.1 to obtain a matrix $D_0 \in \mathcal{G}(\mathbb{F}_q(s))$ with finite Galois group $\mathcal{G}(\mathbb{F}_q)$. We will extend this to a matrix $D \in \mathcal{G}(\mathbb{F}_q(s)[t]_{(t)})$ with

$$D \equiv D_0 \mod t.$$

We choose D such that Theorem 3.1.3 and Theorem 3.2.4 can be applied, i.e., D has to meet certain assumptions on convergence. Then there exists a Picard-Vessiot extension for the difference equation given by D with Galois group $\mathcal{H} \leq \mathcal{G}$. We make sure that D is contained in $\mathrm{GL}_n(\mathfrak{o}[t]_{(t)})$ for all valuation rings $\mathfrak{o}$ corresponding to $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$ as in Proposition 6.2.2 (applied to D_0 and $G = \mathcal{G}(\mathbb{F}_q)$). Our lower bound criterion 3.3.11 then asserts that $\mathcal{H}(\mathbb{F}_q[[t]])$ contains the reduction modulo $\mathcal{P}_j$ of

$$Y^{-1} D\phi_q(D) \cdots \phi_{q^{d_j-1}}(D) Y$$

for all $1 \leq j \leq l$ and all extensions $\mathcal{P}_j$ of $\mathfrak{p}_j$. The constant term of Y is a fundamental solution matrix for D_0, hence the constant terms of these reductions range over $\mathcal{G}(\mathbb{F}_q)$, by Proposition 6.2.2. Therefore, every element in $\mathcal{G}(\mathbb{F}_q)$ occurs as the constant term of some element in $\mathcal{H}(\mathbb{F}_q[[t]])$. If we moreover assume that $\mathcal{G}$ splits over $\mathbb{F}_q$, Theorem 4.3.1 then asserts that it is sufficient to choose D in such a way that it specializes to an element which generates a dense subgroup of a split torus T. In order to be able to do that, we will have to assume that $T(\mathbb{F}_q)$ contains a regular element and that the corresponding place $\mathfrak{p}_i$ given by Proposition 6.2.2 is of degree 1. This can be achieved after passing to a finite extension of $\mathbb{F}_q$, since $T(\overline{\mathbb{F}}_q)$ contains a regular element.

Proposition 6.2.3. *Let M be a finite Frobenius module over $(\mathbb{F}_q(s), \phi_q)$ with representing matrix $D \in \mathrm{GL}_n(\mathbb{F}_q(s))$, Picard-Vessiot extension $E/\mathbb{F}_q(s)$ and Galois group G. Assume that E and $\overline{\mathbb{F}}_q$ are linearly disjoint over $\mathbb{F}_q$. Then for any $i \geq 1$, the finite Frobenius module M_i over $(\mathbb{F}_{q^i}(s), \phi_{q^i})$ given by*

$$D_i := D\phi_q(D) \ldots \phi_{q^{i-1}}(D)$$

has Picard-Vessiot extension $E\mathbb{F}_{q^i}$, and Galois group G.

Proof. Let $Y \in \mathrm{GL}_n(E)$ be a fundamental solution matrix for M. Hence $D\phi_q(Y) = Y$ which inductively implies

$$D_i \phi_{q^i}(Y) = Y,$$

so that Y is a fundamental solution matrix for M_i as well. As E is generated over $\mathbb{F}_q(s)$ by the entries of Y, we conclude that $E_i := E\mathbb{F}_{q^i}$ is generated over $\mathbb{F}_{q^i}(s)$ by the entries of Y. Hence E_i is a Picard-Vessiot extension of M_i and as E and $\mathbb{F}_{q^i}$ are linearly disjoint over $\mathbb{F}_q$ by assumption, we have $\mathrm{Gal}(E_i/\mathbb{F}_{q^i}(s)) = \mathrm{Gal}(E/\mathbb{F}_q(s)) = G$. □

Corollary 6.2.4. *Let $\mathcal{G}$ be a semisimple and simply-connected linear algebraic group defined over $\mathbb{F}_q$ and let $g_0 \in \mathcal{G}(\mathbb{F}_q)$. Then there exists an element $D \in \mathcal{G}(\mathbb{F}_q(s))$, a number $i \in \mathbb{N}$, and a place $\mathfrak{p}$ of degree 1 of $\mathbb{F}_{q^i}(s)$ such that*

- *the finite Frobenius module M_i over $(\mathbb{F}_{q^i}(s), \phi_{q^i})$ given by $D_i = D\phi_q(D)\dots\phi_{q^{i-1}}(D)$ has Galois group $\mathcal{G}(\mathbb{F}_q)$, and D_i is contained in $\mathrm{GL}_n(\mathfrak{o})$, where $\mathfrak{o}$ denotes the valuation ring inside $\mathbb{F}_{q^i}(s)$ corresponding to $\mathfrak{p}$.*
- *there exists a fundamental solution matrix $Y \in \mathcal{G}(\overline{\mathbb{F}_q(s)}^{\mathrm{sep}})$ for M_i such that the reduction of $Y^{-1}D_iY$ modulo some extension of $\mathfrak{p}$ from $\mathbb{F}_{q^i}(s)$ to a (non-discrete) valuation on $\overline{\mathbb{F}_q(s)}^{\mathrm{sep}}$ equals g_0.*

Proof. Corollary 6.1.2 provides us with a finite Frobenius module M over $(\mathbb{F}_q(s), \phi_q)$ with representing matrix $D \in \mathcal{G}(\mathbb{F}_q(s))$, Picard-Vessiot extension $E/\mathbb{F}_q(s)$ linearly disjoint from $\overline{\mathbb{F}}_q$ over $\mathbb{F}_q$, and Galois group $\mathcal{G}(\mathbb{F}_q)$. Fix a fundamental solution matrix $Y \in \mathcal{G}(E)$ for M (which exists thanks to the Lang isogeny, see [Bor91, V.16.4]). By Proposition 6.2.2, there exists a finite place $\mathfrak{p}_0$ of $\mathbb{F}_q(s)$ of some degree $d \in \mathbb{N}$ such that $D \in \mathrm{GL}_n(\mathfrak{o}_0)$ and such that the reduction of $Y^{-1}D\phi_q(D)\dots\phi_{q^{d-1}}(D)Y$ modulo some extension $\mathcal{P}_0$ of $\mathfrak{p}_0$ from $\mathbb{F}_q(s)$ to E equals g_0. Set $i := d$. Then M_i has Galois group $\mathcal{G}(\mathbb{F}_q)$, Y is a fundamental solution matrix for M_i, and the Picard-Vessiot extension associated to M_i equals $E_i = E\mathbb{F}_{q^i}$, by Proposition 6.2.3. Let $\mathcal{P}$ be an extension of $\mathcal{P}_0$ from E to $\overline{\mathbb{F}_q(s)}^{\mathrm{sep}}$ and set $\mathfrak{p} = \mathcal{P} \cap \mathbb{F}_{q^i}(s) \supseteq \mathfrak{p}_0$. Then $\mathfrak{p}$ is of degree 1, since $\mathfrak{p}_0$ is of degree d and thus splits into d places of degree 1 inside $\mathbb{F}_{q^i}(s) = \mathbb{F}_{q^d}(s)$. Note that D_i is contained in $\mathrm{GL}_n(\mathbb{F}_q(s))$, hence $Y^{-1}D_iY \in \mathrm{GL}_n(E)$ and reducing $Y^{-1}D_iY$ modulo $\mathcal{P}$ yields the same as reducing it modulo $\mathcal{P}_0$, that is, g_0. □

6.3 The Infinite Part

Proposition 6.3.1. *Let $\mathcal{G}$ be a connected, reductive linear algebraic group defined over $\mathbb{F}_q$ of rank r. Assume that there exists a maximal torus T that splits over $\mathbb{F}_q$ with $\mathbb{F}_q$-isomorphism $\gamma\colon \mathbb{G}_m^r \to T$. Then there exist irreducible polynomials $p_1, \dots, p_r \in \mathbb{F}_q[t]$ such that if we set $g = \gamma(p_1, \dots, p_r) \in T(\mathbb{F}_q(t))$ the following holds:*

- *g is contained in $T(\mathbb{F}_q[t]_{(t)})$ and $g \equiv I \mod t$.*
- *For any $g_0 \in T(\mathbb{F}_q)$, $g_0 g$ generates a dense subgroup of T. In particular, the centralizer of $g_0 g$ inside $\mathcal{G}$ equals T.*

Proof. Choose pairwise distinct irreducible polynomials $p_1, \dots, p_r \in \mathbb{F}_q[t]$ with constant terms 1 and set

$$g := \gamma(p_1, \dots, p_r).$$

Since γ is given $\mathbb{F}_q$-polynomially in $p_1^{\pm 1}, \ldots, p_r^{\pm 1}$ and every p_i has non-zero constant term (and is thus contained in $(\mathbb{F}_q[t]_{(t)})^\times$), g is contained in $T(\mathbb{F}_q[t]_{(t)})$. Hence we can consider the constant part $g_0 \in T(\mathbb{F}_q)$ of g which equals $\gamma(1, \ldots, 1) = I$, as we assumed that the constant parts of $p_1, \ldots, p_r$ are all equal to 1. Now let g_0 be an arbitrary element inside $T(\mathbb{F}_q)$, say $g_0 = \gamma(\mu_1, \ldots, \mu_r)$ with $\mu_i \in \mathbb{F}_q^\times$. Then $\mu_1 p_1, \ldots, \mu_r p_r$ are pairwise coprime polynomials inside $\mathbb{F}_q[t]$ and Lemma 4.2.6 asserts that the element $(\mu_1 p_1, \ldots, \mu_r p_r)$ generates a dense subgroup of $\mathbb{G}_m^r$. Hence
$g_0 g = \gamma(\mu_1 p_1, \ldots, \mu_r p_r)$ generates a dense subgroup of T. In particular, every element x in the centralizer of $g_0 g$ centralizes all of T (since the centralizer of x is a closed subgroup of $\mathcal{G}$ containing $g_0 g$). We assumed $\mathcal{G}$ reductive, hence the centralizer of T equals T. □

6.4 The Result

Theorem 6.4.1. *Let $\mathcal{G} \leq \mathrm{SL}_n$ be a semisimple, simply-connected linear algebraic group defined over $\mathbb{F}_q$. Then for a suitable $i \in \mathbb{N}$ there exists an n-dimensional difference module M over $(\mathbb{F}_{q^i}(s,t), \phi_{q^i})$ with a separable Picard-Vessiot ring $R/\mathbb{F}_{q^i}(s,t)$ and corresponding Galois group scheme isomorphic to $\mathcal{G}$ (as linear algebraic group over $\mathbb{F}_{q^i}(t)$).*

Proof. Let q' be a power of q such that there exists a maximal torus T of $\mathcal{G}$ that splits over $\mathbb{F}_{q'}$ and such that $T(\mathbb{F}_{q'})$ contains a regular element g_0. Then the dimension of the centralizer $\mathcal{C}_\mathcal{G}(g_0)$ equals r, the rank of $\mathcal{G}$. As $\mathcal{G}$ is semisimple and simply-connected, all centralizers of semisimple elements are connected (see [Car85, Thm 3.5.6]), hence

$$\mathcal{C}_\mathcal{G}(g_0) = T. \tag{6.2}$$

Let $D_0' \in \mathcal{G}(\mathbb{F}_{q'}(s))$, $i' \in \mathbb{N}$, and $\mathfrak{p}$ a finite place of degree 1 in $\mathbb{F}_{q'^{i'}}(s)$ be as in Corollary 6.2.4 and let i be such that $q^i = q'^{i'}$ holds. We set

$$D_0 = D_0' \phi_q(D_0') \ldots \phi_{q^{i'-1}}(D_0') \in \mathcal{G}(\mathbb{F}_{q'}(s)).$$

Then by Corollary 6.2.4, the finite Frobenius module M_0 over $(\mathbb{F}_{q^i}(s), \phi_{q^i})$ given by D_0 has Galois group $\mathcal{G}(\mathbb{F}_{q'})$. Let $Y_0 \in \mathcal{G}(\overline{\mathbb{F}_q(s)}^{\mathrm{sep}})$ be a fundamental solution matrix of M_0 as in Corollary 6.2.4, that is, we can fix an extension $\mathcal{P}$ of $\mathfrak{p}$ from $\mathbb{F}_{q^i}(s)$ to $\overline{\mathbb{F}_q(s)}^{\mathrm{sep}}$ such that the reduction of $Y_0^{-1} D_0 Y_0$ modulo $\mathcal{P}$ equals $g_0 \in \mathcal{G}(\mathbb{F}_{q'})$. Denote the reduction of D_0 modulo $\mathfrak{p}$ by $\overline{D}_0 \in \mathcal{G}(\mathbb{F}_{q^i})$. Then $\overline{D}_0$ is conjugate to g_0 over $\mathcal{G}(\overline{\mathbb{F}}_q)$ and we can use Equation (6.2) together with Lemma 4.4.1 to obtain an element $x \in \mathcal{G}(\mathbb{F}_{q^i})$ with

$$\overline{D}_0 = g_0^x. \tag{6.3}$$

Fix irreducible elements $p_1, \ldots, p_r \in \mathbb{F}_{q'}[t]$ as in Proposition 6.3.1 and set $g = \gamma(p_1, \ldots, p_r) \in T(\mathbb{F}_{q'}[t]_{(t)})$ (with $\gamma\colon \mathbb{G}_m^r \xrightarrow{\sim} T$ defined over $\mathbb{F}_{q'}$). Then

$g_0 g$ generates a dense subgroup of T and $g \equiv I \mod t$. Fix a finite place $\mathfrak{q} \neq \mathfrak{p}$ of $\mathbb{F}_{q^i}(s)$ such that D_0 is contained in $\mathrm{GL}_n(\mathfrak{o}_\mathfrak{q})$, where $\mathfrak{o}_\mathfrak{q}$ denotes the corresponding valuation ring inside $\mathbb{F}_{q^i}(s)$. Let $f_\mathfrak{q} \in \mathbb{F}_{q^i}[s]$ be a generator of $\mathfrak{q}$. Recall that $\mathfrak{p}$ is of degree 1 in $\mathbb{F}_{q^i}(s)$, hence there exists an $\alpha \in \mathbb{F}_{q^i}$ such that $\mathfrak{p} = (s - \alpha)$. Then $f_\mathfrak{q}(\alpha) \in \mathbb{F}_{q^i}^\times$, as we assumed $\mathfrak{q} \neq \mathfrak{p}$. Let $p_{jl} \in \mathbb{F}_{q'}$ denote the coefficients of p_j, i.e.,

$$p_j = \sum_{l=0}^{n_j} p_{jl} t^l \in \mathbb{F}_{q'}[t],$$

for all $1 \leq j \leq r$. We set

$$\tilde{p}_j = \sum_{l=0}^{n_j} p_{jl} \left(\frac{f_\mathfrak{q}}{f_\mathfrak{q}(\alpha)} \right)^l t^l \in \mathbb{F}_{q^i}(s)[t],$$

for all $1 \leq j \leq r$. Note that $\tilde{p}_1, \ldots, \tilde{p}_r$ are invertible inside $\mathbb{F}_{q^i}(s)[t]_{(t)}$, hence we can define

$$\tilde{g} := \gamma(\tilde{p}_1, \ldots, \tilde{p}_r) \in T(\mathbb{F}_{q^i}(s)[t]_{(t)}).$$

Also, $\tilde{p}_i \equiv p_i \mod t$, hence we can use that γ is defined over $\mathbb{F}_{q'}$ to conclude that the constant term of $\tilde{g}$ equals the constant term of g, that is,

$$\tilde{g} \equiv I \mod t.$$

We can now define the representing matrix $D \in \mathcal{G}(\mathbb{F}_{q^i}(s,t))$ of the desired difference module as

$$\boxed{D = D_0 \tilde{g}^x \in \mathcal{G}(\mathbb{F}_{q^i}(s)[t]_{(t)})}$$

with

$$D \equiv D_0 \mod t.$$

Let M be the corresponding difference module over $(\mathbb{F}_{q^i}(s,t), \phi_{q^i})$.

We first show that there exists a Picard-Vessiot extension for M. Let $|\cdot|$ be the absolute value on $\mathbb{F}_{q^i}(s)$ corresponding to $\mathfrak{q}$ with $|f_\mathfrak{q}| = \frac{1}{2}$ and let K be the completion of an algebraic closure of the completion of $\mathbb{F}_{q^i}(s)$ with respect to $|\cdot|$. We use the corresponding notation (such as $\mathcal{O}_{|\cdot|}$, $\mathfrak{m}$ and L) set up in Section 2.1 with $k = \mathbb{F}_{q^i}(s)$. By construction, the absolute value of the l-th coefficient of $\tilde{p}_i$ is at most $\left(\frac{1}{2}\right)^l$ and the same holds for $\tilde{p}_i^{-1}$ (see Lemma 3.1.4b)). Every entry of $\tilde{g} = \gamma(\tilde{p}_1, \ldots, \tilde{p}_r)$ is given $\mathbb{F}_{q'}$-polynomially in $\tilde{p}_1, \ldots, \tilde{p}_r$ and their inverses, hence every entry of the l-th coefficient matrix $\tilde{g}_l$ of $\tilde{g}$ is bounded by $\left(\frac{1}{2}\right)^l$, as well (see Lemma 3.1.4c)). We conclude

$$||\tilde{g}_l|| \leq \left(\frac{1}{2}\right)^l$$

for every $l \in \mathbb{N}$ (with $||\cdot||$ denoting the maximum norm on a matrix). As x is contained in $\mathcal{G}(\mathbb{F}_{q^i})$, conjugating $\tilde{g}$ with x is given $\mathbb{F}_{q^i}$-linearly in the entries of $\tilde{g}$ and thus doesn't affect the convergence. Finally, we assumed $D_0 \in \mathrm{GL}_n(\mathfrak{o}_\mathfrak{q})$, hence

$$||D_0|| = 1$$

and we conclude

$$||D_l|| = ||D_0 \tilde{g}_l^x|| \leq \left(\frac{1}{2}\right)^l$$

for all $l \in \mathbb{N}$ (where $D_l \in \mathrm{M}_n(\mathbb{F}_{q^i}(s))$ denotes the l-th coefficient matrix of D). We can now apply Theorem 3.1.3 (with $\delta = \frac{1}{2}$) and obtain a fundamental solution matrix $Y \in \mathrm{GL}_n(\mathcal{O}_{|\cdot|}[[t]]) \cap \mathrm{M}_n(\mathcal{O}_{|\cdot|}\{t\})$. We would like to apply Theorem 3.2.4. Note that $\mathcal{O}_{|\cdot|}/\mathfrak{m} \cong \overline{\mathbb{F}}_q$ embeds into K. The reduction of any $\tilde{p}_j$ mod $\mathfrak{m}$ is contained in $\mathbb{F}_{q'} \subseteq K$, as all non-constant coefficients of $\tilde{p}_j$ are divisible by $f_\mathfrak{q} \in \mathfrak{m}$. As γ is defined over $\mathbb{F}_{q'} \subseteq \overline{\mathbb{F}}_q$, it commutes with the reduction modulo $\mathfrak{m}$ and we conclude that the reduction of $\tilde{g}$ is a constant matrix. The constant part of $\tilde{g}$ equals the identity matrix, so the reduction of $\tilde{g}$ modulo $\mathfrak{m}$ actually equals the identity. Therefore, the reduction of D equals the reduction of D_0 and is thus contained in $\mathcal{G}(\mathbb{F}_{q^i}) \subseteq \mathcal{G}(K)$ and all assumptions to Theorem 3.2.4 are satisfied. We obtain another fundamental solution matrix Y' that is contained in $\mathcal{G}(L \cap \mathcal{O}_{|\cdot|}[[t]])$. Then the constant part Y_0' of this new fundamental solution matrix is contained in $\mathcal{G}(K)$ and it is a fundamental solution matrix for D_0. After multiplying Y' from the right with $Y_0'^{-1}Y_0 \in \mathcal{G}(\mathbb{F}_q)$, we may thus assume that the constant part of Y' equals our previously chosen Y_0. From now on, we simply denote Y' by Y. Then $R := \mathbb{F}_{q^i}(s,t)[Y, Y^{-1}] \subseteq L$ is a Picard-Vessiot ring for M by Theorem 1.2.11. All entries of Y are contained in $\overline{\mathbb{F}_q(s)}^{\mathrm{sep}}((t))$, by Proposition 3.3.3 a) (with $\tilde{k} = K$), hence $R/\mathbb{F}_{q^i}(s,t)$ is separable by Proposition 5.2.1. We conclude that the Galois group scheme $\mathcal{H} := \mathcal{G}_{M,R}$ of M is a linear algebraic group (see Theorem 1.3.10) defined over $\mathbb{F}_{q^i}(t)$ and it is a closed subgroup of $\mathcal{G}$ by Proposition 1.3.11.

We will now use the lower bound criterion 3.3.11 to show that $\mathcal{H}$ is all of $\mathcal{G}$. By Theorem 4.3.1, it suffices to show that every element inside $\mathcal{G}(\mathbb{F}_{q'})$ occurs as a constant term inside $\mathcal{H}(\overline{\mathbb{F}}_q[[t]])$ and that $\mathcal{H}$ contains a $\mathcal{G}(\mathbb{F}_{q'} + t\overline{\mathbb{F}}_q[[t]])$-conjugate of the $\mathbb{F}_{q'}$-split torus T. The key point is to show that this is really a $\mathcal{G}(\mathbb{F}_{q'} + t\overline{\mathbb{F}}_q[[t]])$-conjugate and not just a $\mathcal{G}(\mathbb{F}_{q^i} + t\overline{\mathbb{F}}_q[[t]])$-conjugate.

First of all, note that for any finite place $\mathfrak{q}'$ of $\mathbb{F}_{q^i}(s)$ with valuation ring $\mathfrak{o}' \subseteq \mathbb{F}_{q^i}(s)$, the polynomials $\tilde{p}_1, \ldots, \tilde{p}_r$ are contained in $(\mathfrak{o}'[t]_{(t)})^\times$, since their constant coefficients are contained in $\mathbb{F}_{q'}^\times \subseteq \mathfrak{o}'^\times$ and all higher coefficients are $\mathbb{F}_{q^i}$-polynomials in s. Hence $\tilde{g} = \gamma(\tilde{p}_1, \ldots, \tilde{p}_r)$ and also $\tilde{g}^x$ are contained in $\mathrm{GL}_n(\mathfrak{o}'[[t]])$. We conclude that D is contained in $\mathrm{GL}_n(\mathfrak{o}'[[t]])$ if and only if D_0 is contained in $\mathrm{GL}_n(\mathfrak{o}')$.

Consider $\mathfrak{q}' = \mathfrak{p}$ with corresponding valuation ring $\mathfrak{o}$. Then D_0 is contained in $\mathrm{GL}_n(\mathfrak{o})$ by the choice of $\mathfrak{p}$. Let $\mathcal{O}$ be the (non-discrete) valuation ring inside $\overline{\mathbb{F}_q(s)}^{\mathrm{sep}}$ corresponding to the fixed extension $\mathcal{P}$ of $\mathfrak{p}$ coming from Corollary 6.2.4 and let $\kappa\colon \mathcal{O}[[t]] \to \overline{\mathbb{F}}_q[[t]]$ denote the coefficient-wise reduction modulo $\mathcal{P}$. By Corollary 3.3.11 (with $k = \mathbb{F}_{q^i}(s)$ and $\tilde{k} = K$), $\mathcal{H}(\mathbb{F}_{q^i}[[t]])$ contains $h := \kappa(Y^{-1}DY)$ (since $\mathfrak{o}/\mathfrak{p} \cong \mathbb{F}_{q^i}$, hence $d = 1$). We use $\kappa(s) = \alpha$, hence $\kappa(\tilde{p}_j) = p_j$ for all j to compute

$$\begin{aligned}\kappa(D) &= \kappa(D_0)\kappa(\tilde{g})^x \\ &= \overline{D_0}\gamma(\kappa(\tilde{p}_1), \ldots, \kappa(\tilde{p}_r))^x \\ &= g_0^x\gamma(p_1, \ldots, p_r)^x \\ &= (g_0 g)^x,\end{aligned}$$

where we also used Equation (6.3). Therefore, h is conjugate to $g_0 g$ via $x \cdot \kappa(Y) \in \mathcal{G}(\overline{\mathbb{F}}_q[[t]])$. On the other hand, the constant term of h equals the reduction of $Y_0^{-1}D_0Y_0$ at $\mathcal{P}$, which equals g_0 by construction. Hence h is contained in $\mathcal{G}(\mathbb{F}_{q'} + t\mathbb{F}_{q^i}[[t]])$ and is thus conjugate to $g_0 g \in \mathcal{G}(\mathbb{F}_{q'}[[t]])$ not only over $\mathcal{G}(\overline{\mathbb{F}}_q[[t]])$ but also over $\mathcal{G}(\mathbb{F}_{q'} + t\overline{\mathbb{F}}_q[[t]])$, by Proposition 4.4.3. Let $A \in \mathcal{G}(\mathbb{F}_{q'} + t\overline{\mathbb{F}}_q[[t]])$ be such that $(g_0 g)^A$ equals h. Recall that $g_0 g$ generates a dense subgroup of T. Hence $(g_0 g)^A$ generates a dense subgroup of T^A, and $\mathcal{H}$ thus contains T^A.

For the finite part, let $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$ be the finite places of $\mathbb{F}_{q^i}(s)$ provided by Proposition 6.2.2 applied to the finite Frobenius module M_0 over $(\mathbb{F}_{q^i}(s), \phi_{q^i})$. Let $\mathfrak{o}_1, \ldots, \mathfrak{o}_l$ denote the corresponding valuation rings inside $\mathbb{F}_{q^i}(s)$ and $d_1, \ldots, d_l \in \mathbb{N}$ the degrees of $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$. Then $D_0 \in \mathrm{GL}_n(\mathfrak{o}_j)$ and thus $D \in \mathrm{GL}_n(\mathfrak{o}_j[[t]])$ for all $1 \leq j \leq l$. Let further $\mathcal{P}_1, \ldots, \mathcal{P}_l$ be arbitrary extensions of $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$ from $\mathbb{F}_{q^i}(s)$ to $\overline{\mathbb{F}_q(s)}^{\mathrm{sep}}$. Then by Corollary 3.3.11, $\mathcal{H}(\mathbb{F}_{q^i}[[t]])$ contains

$$\kappa_j(Y^{-1}D\phi_q(D)\ldots\phi_{q^{d_j-1}}(D)Y)$$

for all $1 \leq j \leq l$, where κ_j denotes the coefficient-wise reduction modulo $\mathcal{P}_j$. Looking at constant parts, we deduce that the reduction of

$$Y_0^{-1}D_0\phi_q(D_0)\ldots\phi_{q^{d_j-1}}(D_0)Y_0 \mod \mathcal{P}_j$$

occurs as a constant term in $\mathcal{H}(\mathbb{F}_{q^i}[[t]])$. These reductions range over all of $\mathcal{G}(\mathbb{F}_{q'})$ (which is the Galois group of the finite Frobenius module M_0), by Proposition 6.2.2. Hence every element in $\mathcal{G}(\mathbb{F}_{q'})$ occurs as a constant term inside $\mathcal{H}(\mathbb{F}_{q^i}[[t]])$ which concludes the proof. □

6.5 Example

Let now $\mathcal{G} = \mathrm{SL}_n$, assume $q > n(n+1)/2$, and let T be the diagonal torus inside SL_n. If $\zeta \in \mathbb{F}_q$ is a $(q-1)$-th primitive root of unity, then $T(\mathbb{F}_q)$ contains the regular element

$$g_0 := \mathrm{diag}(\zeta, \zeta^2, \ldots, \zeta^{n-1}, \zeta^{-\frac{n(n-1)}{2}}).$$

It was shown in [AM10] that there exists $f_i \in \mathbb{F}_q[s]$ of the form $f_i = s\alpha_i + (1-s)\beta_i$ for some $\alpha_i, \beta_i \in \mathbb{F}_q$ such that the finite Frobenius module over $(\mathbb{F}_q(s), \phi_q)$ given by

$$D_0 = \begin{pmatrix} f_1 & \ldots & f_{n-1} & (-1)^{n-1} \\ 1 & & & \\ & \ddots & & \\ & & 1 & 0 \end{pmatrix}$$

has Galois group $\mathrm{SL}_n(\mathbb{F}_q)$. Let $\gamma_1, \ldots, \gamma_{n-1}$ be the coefficients of the characteristic polynomial of g_0. Fix an element $\alpha \in \mathbb{F}_q \backslash \{0, 1\}$. Then it is easy to see that if we alter f_i to

$$f_i = s\alpha_i + (1-s)\beta_i + \frac{s(s-1)}{\alpha(\alpha-1)}(\gamma_i - \alpha\alpha_i - (1-\alpha)\beta_i),$$

the corresponding Frobenius module M_0 over $(\mathbb{F}_q(s), \phi_q)$ has the same Galois group. For this new Frobenius module, there exists a place $\mathfrak{p}$ of degree 1 of $\mathbb{F}_q(s)$, namely $\mathfrak{p} = (s - \alpha)$, such that the specialization of D_0 at $\mathfrak{p}$ is conjugate to g_0 over $\mathcal{G}(\mathbb{F}_q)$. Hence the number i in Theorem 6.4.1 can be chosen as $i = 1$. The elements p_j in Proposition 6.3.1 can be chosen as $p_j = (1 + \zeta^j t)$ for $1 \leq j \leq n-1$. (Note that $\gamma : \mathbb{G}_m^{n-1} \tilde{\to} T, (\lambda_1, \ldots, \lambda_{n-1}) \mapsto \mathrm{diag}(\lambda_1, \ldots, \lambda_{n-1}, (\lambda_1 \cdots \lambda_{n-1})^{-1})$.) Following the proof of Theorem 6.4.1, we obtain that the difference module M over $(\mathbb{F}_q(s,t), \phi_q)$ given by

$$\boxed{D = D_0 \cdot \mathrm{diag}(\tilde{p}_1, \ldots, \tilde{p}_{n-1}, (\tilde{p}_1 \cdots \tilde{p}_{n-1})^{-1})^x}$$

has Galois group SL_n where the elements $\tilde{p}_j \in \mathbb{F}_q[s,t]$ and $x \in \mathcal{G}(\mathbb{F}_q)$ can also be chosen explicitly: We fix the finite place $\mathfrak{q} = (s)$, hence $f_\mathfrak{q} = s$ and we can define $\tilde{p}_j$ as

$$\tilde{p}_j := 1 + \zeta^j \frac{s}{\alpha} t$$

for $1 \leq j \leq n-1$. Finally, $x \in \mathrm{SL}_n(\mathbb{F}_q)$ is a matrix such that the reduction of $\overline{D_0}$ of D_0 at $\mathfrak{p} = (s - \alpha)$ equals g_0^x. We have

$$\overline{D}_0 = \begin{pmatrix} \gamma_1 & \ldots & \gamma_{n-1} & (-1)^{n-1} \\ 1 & & & \\ & \ddots & & \\ & & 1 & 0 \end{pmatrix}$$

and it is easy to see that x can be chosen as

$$x = \begin{pmatrix} \det(A)^{-1} & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \cdot A$$

with A the Vandermonde-matrix corresponding to

$$(\zeta^{-1}, \zeta^{-2}, \ldots, \zeta^{-n+1}, \zeta^{\frac{n(n-1)}{2}}).$$

Chapter 7

t-Motives

7.1 The Category of t-Motives

Following [Pap08] and [Tae09], we give the basic definitions of t-motives which were originally introduced by Anderson in [And86]. Although t-motives can be defined over any field K containing $\mathbb{F}_q$ (see [Tae09]), we restrict ourselves to the following situation:

k**:**	$k = \mathbb{F}_q(\theta)$, a rational function field.
$\lvert\cdot\rvert_\infty$**:**	the ∞-adic valuation on k with $\lvert\theta\rvert_\infty = q$.
$(K, \lvert\cdot\rvert_\infty)$**:**	the completion of an algebraic closure of the completion of k with unique extension $\lvert\cdot\rvert_\infty$ from k to K.
$\overline{k}$**:**	the algebraic closure of k inside K.
T**:**	the ring of restricted power series over K, i.e., power series $\sum_{i=0}^{\infty} a_i t^i$ such that $\lim_{i\to\infty} \lvert a_i\rvert_\infty = 0$.
L**:**	fraction field of T.
σ**:**	on $\overline{k}$ and K, σ is the inverse of the Frobenius and σ extends to $\overline{k}(t)$, T and L by acting coefficient-wise, i.e., $\sigma(t) = t$.

Compared to our previous setup from Chapter 5, we renamed the variable s by θ^{-1} (hence we consider the ∞-adic valuation instead of the s-adic one) and we work with $\sigma = \phi_q^{-1}$ instead of ϕ_q. Note that $L^\sigma = k^\sigma = \mathbb{F}_q(t)$ holds by Lemma 2.1.3 (or [Pap08, 3.3.2]).

Definition 7.1.1. *[Pap08, 3.2.1]*
A pre-t-motive *is a left $\overline{k}(t)[\sigma, \sigma^{-1}]$-module that is finite dimensional over $\overline{k}(t)$. In other words, a pre-t-motive is a difference module $(P, \boldsymbol{\sigma})$ over $(\overline{k}(t), \sigma)$ as defined in Definition 1.1.10. Let $\mathcal{B}$ be a basis of an n-dimensional pre-t-motive $(P, \boldsymbol{\sigma})$ over $\overline{k}(t)$. Then the matrix $\Phi \in \mathrm{GL}_n(\overline{k}(t))$ collecting the images of the elements of $\mathcal{B}$ in its rows is said to* represent multiplication by $\boldsymbol{\sigma}$ on P *and we call it the* representing matrix*, for short.*

Remark 7.1.2. *Previously, we defined the representing matrix of a difference module to be the matrix collecting the images of a basis in its columns and not its rows. In this chapter, we use the row-convention instead to conform to the notation in [Pap08], i.e., we transpose our representing matrices.*

Example 7.1.3. *The* Carlitz pre-t-motive C *is the pre-t-motive* $(\overline{k}(t), \boldsymbol{\sigma})$ *with* $\boldsymbol{\sigma}$ *given by* $\boldsymbol{\sigma}(f) = (t-\theta)\sigma(f)$. *Then* $\Phi = (t-\theta)$ *represents multiplication on* C *with respect to the basis* $\{1\}$ *of* C.

Definition 7.1.4. *[Pap08, 3.3.1]*
A pre-t-motive $(P, \boldsymbol{\sigma})$ *is called* rigid analytically trivial, *if* $P \otimes_{\overline{k}(t)} L$ *has a* $\boldsymbol{\sigma}$*-invariant* L*-basis.*

Proposition 7.1.5. *[Pap08, 3.3.9]*
A pre-t-motive P is rigid analytically trivial if and only if there exists a rigid analytic trivialization *of P, i.e., a matrix $\Psi \in \mathrm{GL}_n(L)$ satisfying*

$$\sigma(\Psi) = \Phi\Psi.$$

In particular, P is rigid analytically trivial if and only if there exists a Picard-Vessiot ring of P contained in L.

Proof. Recall that Φ was chosen with respect to a fixed basis $\mathcal{B}$. We use this basis to write any element in $P \otimes_{\overline{k}(t)} L$ as element in L^n, where $n = \dim_{\overline{k}(t)}(P)$. For any such element $p \in P \otimes_{\overline{k}(t)} L$ we then have $\boldsymbol{\sigma}(p) = \Phi^{\mathrm{tr}}\sigma(p)$. Set $Y = \Psi^{-1,\mathrm{tr}}$. Then $\sigma(\Psi) = \Phi\Psi$ if and only if ${}^{\mathrm{tr}}\Phi\sigma(Y) = Y$ which holds if and only if the columns of Y form an $\boldsymbol{\sigma}$-invariant basis of $P \otimes_{\overline{k}(t)} L$. Hence P is rigid analytically trivial if and only if such a Ψ exists.
In other words, P is rigid analytically trivial if and only if there exists a fundamental solution matrix $Y \in \mathrm{GL}_n(L)$ for the difference equation ${}^{\mathrm{tr}}\Phi\sigma(Y) = Y$. By Theorem 1.2.11, $\overline{k}(t)[Y, Y^{-1}] \subseteq L$ is then a Picard-Vessiot extension for P. □

Theorem 7.1.6. *[Pap08, 3.3.15]*
The category $\mathcal{R}$ of rigid analytically trivial pre-t-motives is a neutral Tannakian category over $\mathbb{F}_q(t)$ with fiber functor mapping a pre-t-motive to the vector space of solutions inside $P \otimes_F L$.

Definition 7.1.7. *[Tae09, 2.1.1]*
An effective t-motive *of rank n is a pair $(M, \boldsymbol{\sigma})$ consisting of a free and finitely generated $\overline{k}[t]$-module M of rank n together with a σ-semilinear map $\boldsymbol{\sigma}\colon M \to M$ such that the determinant of the representing matrix of $\boldsymbol{\sigma}$ with respect to some basis of M is of the form $u(t-\theta)^i$ for an $i \in \mathbb{N}$ and $u \in \overline{k}^\times$. (Note that $i = 0$ is not excluded).*

Example 7.1.8. *Consider* $C = (\overline{k}[t], \boldsymbol{\sigma})$ *with* $\boldsymbol{\sigma}$ *given by* $\boldsymbol{\sigma}(f) = (t-\theta)\sigma(f)$. *Then* C *is an effective* t*-motive, called the* Carlitz motive.

Definition 7.1.9. *[Tae09, 3.2.8]*
An effective t*-motive* $(M, \boldsymbol{\sigma})$ *is called* rigid analytically trivial*, if* $M \otimes_{\overline{k}[t]} T$ *has a* $\boldsymbol{\sigma}$*-invariant* T*-basis.*

Proposition 7.1.10. *a) An effective* t*-motive* $(M, \boldsymbol{\sigma})$ *is rigid analytically trivial if and only if the corresponding pre-*t*-motive* $M \otimes_{\overline{k}[t]} \overline{k}(t)$ *is rigid analytically trivial.*

b) An effective t*-motive* $(M, \boldsymbol{\sigma})$ *is rigid analytically trivial if and only if there exists a rigid analytic trivialization* $\Psi \in \mathrm{GL}_n(T)$ *of* M*.*

Proof. This was proven in [Pap08, 3.3.9] and [Tae09, 3.2.8]. □

Example 7.1.11. *The Carlitz motive is rigid analytically trivial with rigid analytic trivialization*

$$\Omega := (\sqrt[q-1]{-\theta})^{-q} \prod_{i=1}^{\infty} (1 - t/\theta^{q^i}) \in T.$$

Details can be found in [Pap08, 3.3.4].

The category of effective t-motives can be considered as subcategory of $\mathcal{P}$ by identifying M with $M \otimes_{\overline{k}[t]} \overline{k}(t)$ (see [Pap08, 3.4.9] for details).

Definition 7.1.12. *[Pap08, 3.4.10]*
The category $\mathcal{T}$ *of* t-motives *is defined to be the strictly full Tannakian subcategory of* $\mathcal{R}$ *generated by the rigid analytically trivial effective* t*-motives up to isogeny.*

Remark 7.1.13. *In [Pap08, 3.4.10],* $\mathcal{T}$ *is actually defined to be the Tannakian subcategory of* $\mathcal{R}$ *generated by the those rigid analytically trivial effective* t*-motives (up to isogeny) that are finitely generated over* $\overline{k}[\sigma]$*. However, these generate the same Tannakian category. More precisely, it is shown in [Tae09, 5.3.2] that if* M *is an rigid analytically trivial effective* t*-motive, then for all* $r >> 0$*,* $M \otimes_{\overline{k}[t]} C^{\otimes r}$ *is finitely generated over* $\overline{k}[\sigma]$*.*

Definition 7.1.14. *Let* M *be a* t*-motive. Then there exists a unique Picard-Vessiot extension of* M *inside* L*. The corresponding difference Galois group scheme* $\mathcal{G}$ *defined over* $\mathbb{F}_q(t)$ *(see Definition 1.3.6) is called the* Galois group *of* M*.*

Remark 7.1.15. *The Galois group of* M *is* $\mathbb{F}_q(t)$*-isomorphic to the Galois group scheme assigned to* M *using the Tannakian formalism. This was proven in [Pap08, Thm 4.5.10].*

Example 7.1.16. *The Carlitz t-motive has Galois group $\mathbb{G}_m$ (see [Pap08, 3.5.4]).*

Difference Galois theory has proved very powerful in transcendence theory over function fields, due to the fact that the dimension of the difference Galois group equals the transcendence degree of the Picard-Vessiot ring. In 2008, [Pap08], Papanikolas proved a function field analog of the classical conjecture on logarithms of algebraic numbers, namely that they are algebraically independent over $\overline{\mathbb{Q}}$ if they are linearly independent over $\mathbb{Q}$. The function field analog of the exponential function is the so-called Carlitz exponential function $\exp_C$, which again is similar to the exponential function $\exp_E\colon \mathbb{C} \to E(\mathbb{C}), z \mapsto (\wp(z) : \wp'(z) : 1)$ assigned to an elliptic curve E. There is also a function field analog of the Riemann ζ-function and in [CY07], Chang and Yu proved a classical conjecture concerning algebraic relations among $\zeta(2), \zeta(3), \zeta(4), \dots$ in the function field case using difference Galois theory.
It would be interesting to know whether there are difference equations arising from questions in transcendence theory where our lower bound criterion 3.3.11 might be helpful.

7.2 Pre-t-Motives with Semisimple Galois Groups

We can now lift our results from Chapter 5 and 6 where we realized certain semisimple groups as difference Galois groups over $k(t)$ to $\overline{k}(t)$ to get pre-t-motives with interesting Galois groups.

Theorem 7.2.1. *a) Let $n \geq 2$ and $q > 2$ be such that $(n, q) \neq (2, 3)$. Consider the pre-t-motive $P = (\overline{k}(t)^n, \boldsymbol{\sigma})$ with $\boldsymbol{\sigma}$ given by*

$$\Phi = \begin{pmatrix} \phi_1 & \dots & \phi_{n-1} & (-1)^{n-1} \\ 1 & & & \\ & \ddots & & \\ & & 1 & 0 \end{pmatrix}$$

where $\phi_i := f_i(1/\theta, t) \in k(t)$ for $f_i(s,t) \in \mathbb{F}_q(s,t)$ as defined in Table 5.1 on page 72. Then P is rigid analytically trivial and has Galois group SL_n.

b) Let $n = 2d \geq 4$ and assume $q > 2$. Consider the pre-t-motive $P =$

$(\overline{k}(t)^n, \boldsymbol{\sigma})$ with $\boldsymbol{\sigma}$ given by

$$\Phi = \left(\begin{array}{cccc|cccc} \phi_1 & \cdots & \phi_{d-1} & \phi_d & 1 & & & \\ 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & 0 & & & & \\ \hline & & & \phi_{d-1} & 0 & 1 & & \\ & & & \vdots & \vdots & & \ddots & \\ & & & \phi_1 & 0 & & & 1 \\ & & & -1 & 0 & & & 0 \end{array}\right)$$

where $\phi_i := f_i(1/\theta, t) \in k(t)$ for $f_i(s,t) \in \mathbb{F}_q(s,t)$ as defined in Table 5.2 on page 81. Then P is rigid analytically trivial and has Galois group Sp_{2d}.

c) Let $n = 2d+1 \geq 7$ and assume q odd. Consider the pre-t-motive $P = (\overline{k}(t)^n, \boldsymbol{\sigma})$ with $\boldsymbol{\sigma}$ given by

$$\Phi = \left(\begin{array}{cccc|c|cccc} \phi_1 & \cdots & \phi_{d-1} & \phi_d & -2\phi_d & -2\phi_d & & & \\ 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & 0 & & & & & \\ \hline & & & 1 & -1 & & & & \\ \hline & & & \frac{\phi_{d-1}}{2\phi_d} & & 0 & 1 & & \\ & & & \vdots & & & & \ddots & \\ & & & \frac{\phi_1}{2\phi_d} & & & & & 1 \\ & & & -\frac{1}{2\phi_d} & & & & & 0 \end{array}\right)$$

where $\phi_i := f_i(1/\theta, t) \in k(t)$ for $f_i(s,t) \in \mathbb{F}_q(s,t)$, $f_d \in \mathbb{F}_q(s,t)^\times$ as defined in Table 5.3 on page 87. Then P is rigid analytically trivial and has Galois group SO_{2d+1}.

d) Let $n = 2d \geq 8$ and assume q odd. Consider the pre-t-motive $P =$

$(\overline{k}(t)^n, \boldsymbol{\sigma})$ with $\boldsymbol{\sigma}$ given by

$$\Phi = \left(\begin{array}{cccc|cccccc} \phi_1 & \dots & \phi_{d-1} & \phi_d & \phi_{d-1} & -\phi_d & & & & \\ 1 & & & & & & & & & \\ & \ddots & & & & & & & & \\ & & 1 & 0 & 1 & & & & & \\ \hline & & \frac{\phi_{d-1}}{\phi_d} & 1 & 0 & & & & & \\ & & \frac{\phi_{d-2}}{\phi_d} & & 0 & 0 & 1 & & & \\ & & \vdots & & & & & \ddots & & \\ & & \frac{\phi_1}{\phi_d} & & & & & & 1 & \\ & & -\frac{1}{\phi_d} & & & & & & 0 & \end{array}\right)$$

where $\phi_i := f_i(1/\theta, t) \in k(t)$ for $f_i(s,t) \in \mathbb{F}_q(s,t)$, $f_d \in \mathbb{F}_q(s,t)^\times$ as defined in Table 5.4 on page 100. Then P is rigid analytically trivial and has Galois group SO_{2d}.

e) Assume q odd. Consider the pre-t-motive $P = (\overline{k}(t)^7, \boldsymbol{\sigma})$ with $\boldsymbol{\sigma}$ given by

$$\Phi = \begin{pmatrix} -\phi_1 & -\phi_2 & 1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -\phi_1^2 & 0 & -\phi_1 & \phi_2 & 1 & 0 \\ 0 & -2\phi_1 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -\phi_1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

where $\phi_i := f_i(1/\theta, t) \in k(t)$ for $f_i(s,t) \in \mathbb{F}_q(s,t)$ as defined in Table 5.5 on page 108. Then P is rigid analytically trivial and has Galois group G_2.

f) Assume $q > 2$ even. Consider the pre-t-motive $P = (\overline{k}(t)^6, \boldsymbol{\sigma})$ with $\boldsymbol{\sigma}$ given by

$$\Phi = \begin{pmatrix} \phi_1 & \phi_2 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \phi_1^2 & 0 & \phi_2 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \phi_1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

where $\phi_i := f_i(1/\theta, t) \in k(t)$ for $f_i(s,t) \in \mathbb{F}_q(s,t)$ as defined in Table 5.5 on page 108. Then P is rigid analytically trivial and has Galois group G_2.

Proof. We proved in Theorem 5.4.4, 5.5.4, 5.6.4, 5.7.7, 5.8.4, resp., that the ϕ_q-difference module M over $k(t)$ given by Φ (this time with respect to the

column-convention) has a fundamental solution matrix $Y \in \mathrm{GL}_n(L)$ with Picard-Vessiot ring $R := k(t)[Y, Y^{-1}] \subseteq L$ with Galois group SL_n, Sp_{2d}, SO_{2d+1}, SO_{2d}, G_2, resp. Hence R and $\overline{k}(t)$ are both contained in L and the corresponding Galois group is connected, so we can apply Theorem 1.4.2 to conclude that $M \otimes_k \overline{k}$ has Picard-Vessiot ring $R \otimes_k \overline{k} = \overline{k}(t)[Y, Y^{-1}] \subseteq L$ over $\overline{k}(t)$ and the same Galois group. Set $\Psi = \phi_q(Y) \in \mathrm{GL}_n(L)$. As Y is a fundamental solution matrix for M, we have

$$\Phi\phi_q(Y) = Y$$

which translates to

$$\Phi\Psi = \sigma(\Psi).$$

Hence Ψ is a rigid analytic trivialization of P and

$$R \otimes_k \overline{k} = \overline{k}(t)[Y, Y^{-1}] = \overline{k}(t)[\Psi, \Psi^{-1}]$$

is also a Picard-Vessiot ring for P. Hence the Galois group schemes of P and $M \otimes_k \overline{k}$ coincide (they both equal $\underline{\mathrm{Aut}}(R \otimes_k \overline{k}/\overline{k}(t))$). □

Note that the notion "pre-t-motive" depends on q, since $\sigma = \phi_q^{-1}$. When considering pre-t-motives with respect to different q's at the same time, we will clarify this by calling a pre-t-motive corresponding to $\sigma = \phi_q^{-1}$ a *pre-q-t-motive*. If q has been fixed, a pre-q^i-t-motive is sometimes called a *pre-t-motive of level i*.

Theorem 7.2.2. *Let $\mathcal{G} \leq \mathrm{SL}_n$ be a semisimple and simply-connected linear algebraic group defined over $\mathbb{F}_q$. Then there exists an $i \in \mathbb{N}$ and a pre-q^i-t-motive that is rigid analytically trivial and has Galois group isomorphic to $\mathcal{G}$ as linear algebraic group over $\mathbb{F}_{q^i}(t)$.*

Proof. Again, this is just Theorem 6.4.1 together with Theorem 1.4.2. □

7.3 t-Motives

Proposition 7.3.1. *Let M be an n-dimensional t-motive. Then there exists a $\overline{k}(t)$-basis of M such that the corresponding representing matrix Φ is contained in $\mathrm{GL}_n((t-\theta)^{-\mathbb{N}}\overline{k}[t])$.*

Proof. As M is contained in the Tannakian category generated by rigid analytically trivial effective t-motives, it can be constructed from finitely many effective t-motives using direct sums, subquotiens, tensor products, duals, and internal Hom's. The representing matrix Φ_e of an effective t-motive with respect to a $\overline{k}[t]$-basis has entries in $\overline{k}[t]$ and its determinant equals $u(t-\theta)^i$ for some $u \in \overline{k}^\times$ and $i \in \mathbb{N}$. Hence $\det(\Phi_e)$ is invertible inside $(t-\theta)^{-\mathbb{N}}\overline{k}[t]$ and Φ_e is thus contained in $\mathrm{GL}_n((t-\theta)^{-\mathbb{N}}\overline{k}[t])$. The

representing matrix of the dual equals $\Phi_e^{\mathrm{tr},-1} \in \mathrm{GL}_n((t-\theta)^{-\mathbb{N}}\overline{k}[t])$. Let P and Q be pre-t-motives. Then the internal Hom is the pre-t-motive $R = \mathrm{Hom}_{\overline{k}(t)}(P,Q)$ with $\boldsymbol{\sigma}(\gamma) = \boldsymbol{\sigma}\gamma\boldsymbol{\sigma}^{-1}$. It is easy to see that the representing matrix of R with respect to the canonical basis equals $(\Phi_{M_2} \otimes \Phi_{M_1}^{\mathrm{tr},-1}) \cdot w$, where w denotes a permutation matrix. That is, the matrices remain inside $\mathrm{GL}_n((t-\theta)^{-\mathbb{N}}\overline{k}[t])$ under taking duals and internal Hom's. If P and Q are pre-t-motives such that their representing matrices Φ_P and Φ_Q are contained in $\mathrm{GL}_n((t-\theta)^{-\mathbb{N}}\overline{k}[t])$, then the same is true for the representing matrix $\Phi_P \oplus \Phi_Q$ of $P \oplus Q$, for the representing matrix $\Phi_P \otimes \Phi_Q$ of $P \otimes Q$ and for the representing matrix of any subquotient of P (using base extension). □

The only explicit examples of Galois group schemes of t-motives known to the author are extensions of one copy of $\mathbb{G}_m$ by several copies of $\mathbb{G}_a$ such as those occuring in transcendence theory (see [Pap08], [CY07]). One cannot expect every linear algebraic group over $\mathbb{F}_q(t)$ to occur as the Galois group of a t-motive, as the following Proposition demonstrates.

Proposition 7.3.2. *Let $n \geq 2$. Then $\mathbb{G}_m^n$ does not occur as t-motivic Galois group.*

Proof. The following argument was communicated to the author by Lenny Taelman.
Assume that M is a t-motive with Galois group $\mathbb{G}_m^n$. Then the Tannakian subcategory $\mathcal{T}_M$ of $\mathcal{T}$ generated by M is equivalent to the Tannakian category of finite dimensional representations of $\mathbb{G}_m^n$ over $\mathbb{F}_q(t)$ ([Pap08, Thm. 4.5.10.]). As $\mathbb{G}_m^n$ is an $\mathbb{F}_q(t)$-diagonalizable group, any $\mathbb{F}_q(t)$-representation splits into a direct sum of one-dimensional $\mathbb{F}_q(t)$-representations. It follows that M is isomorphic to a direct sum of one-dimensional t-motives. Let $(N, \boldsymbol{\sigma})$ be a one-dimensional t-motive. By Proposition 7.3.1, there exists a basis of N consisting of $0 \neq v \in N$ such that $\boldsymbol{\sigma}(v) = \Phi v$ with Φ invertible inside $(t-\theta)^{-\mathbb{N}}\overline{k}[t]$. Hence Φ is of the form $u(t-\theta)^n$ for an $u \in \overline{k}^\times$ and $n \in \mathbb{Z}$. By multiplying v by a solution $y \in \overline{k}^\times$ of the algebraic equation $\sigma(y) = u^{-1}y$, we may assume $u = 1$. Hence $N = C^{\otimes n}$ if $n \geq 0$ or $N = (C^\vee)^{\otimes(-n)}$ if $n < 0$, where $C^\vee$ denotes the dual of the Carlitz t-motive C (recall that $C^\vee$ has representing matrix $(t-\theta)^{\mathrm{tr},-1} = (t-\theta)^{-1}$). We conclude that N is contained in the Tannakian category $\mathcal{T}_C$ generated by C. As a direct sum of such objects, M is contained in $\mathcal{T}_C$, as well. Therefore, the Galois group $\mathbb{G}_m^n$ of M is a quotient of the Galois group $\mathbb{G}_m$ of C ([Pap08, 3.5.2]), a contradiction. □

On the other hand, it is very easy to construct pre-t-motives with Galois group $\mathbb{G}_m^n$, as the following example demonstrates.

Example 7.3.3. *Let P be the pre-t-motive $(\overline{k}(t), \boldsymbol{\sigma})$ given by*

$$\Phi = \mathrm{diag}(1+\theta t, 1+\theta t^2, \ldots, 1+\theta t^n).$$

By Theorem 3.1.3 together with Theorem 3.2.4, there exists a rigid analytic trivialization $\Psi \in \mathbb{G}_m^n(L)$ *(this can actually be seen very easily by hand without using Theorems 3.1.3 and 3.2.4). The corresponding Galois group scheme* $\mathcal{H}$ *is therefore contained in* $\mathbb{G}_m^n$*. The lower bound criterion 3.3.10 asserts that* $\mathcal{H}(\mathbb{F}_q[[t]])$ *contains a conjugate* h *of*

$$\overline{\Phi} = \operatorname{diag}(1+t, 1+t^2, \ldots, 1+t^n),$$

the specialization of Φ *via* $\theta \mapsto 1$*. As* h *is diagonal and has the same eigenvalues as* $\overline{\Phi}$*, we conclude that there exists a permutation* $\sigma \in \mathrm{S}_n$ *such that* h *equals* $\overline{\Phi}^\sigma$*. Hence* h *generates a dense subgroup of* $\mathbb{G}_m^n$*, by Lemma 4.2.6 and we conclude* $\mathcal{H} = \mathbb{G}_m^n$*. To be more precise, we should note that we cannot apply the lower bound criterion 3.3.10 directly to* P *but only to the corresponding difference module over* $k(t)$ *given by* Φ*. We then lift the result to* $\overline{k}(t)$ *using Theorem 1.4.2.*

Bibliography

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[AM05] Katsutoshi Amano and Akira Masuoka. Picard-Vessiot extensions of Artinian simple module algebras. *J. Algebra*, 285(2):743–767, 2005.

[AM10] Maximilian Albert and Annette Maier. Additive Polynomials for Finite Groups of Lie Type. *Preprint. To appear in: Israel Journal of Mathematics*, 2010.

[And86] Greg W. Anderson. t-motives. *Duke Math. J.*, 53(2):457–502, 1986.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[Bor91] Armand Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 1991.

[Bou90] N. Bourbaki. *Algebra. II. Chapters 4–7*. Elements of Mathematics (Berlin). Springer, Berlin, 1990.

[BP11] W. Dale Brownawell and Matthew A. Papanikolas. A rapid introduction to drinfeld modules t-modules and t-motives. *Preprint; available online*, 2011.

[Car35] Leonard Carlitz. On certain functions connected with polynomials in a Galois field. *Duke Math. J.*, 1(2):137–168, 1935.

[Car85] Roger W. Carter. *Finite groups of Lie type*. Pure and Applied Mathematics (New York). John Wiley & Sons Inc., New York, 1985. Conjugacy classes and complex characters, A Wiley-Interscience Publication.

[Cha10] Chieh-Yu Chang. Frobenius difference equations and difference galois groups. *Preprint; available online*, 2010.

[Coo81] Bruce N. Cooperstein. Maximal subgroups of $G_2(2^n)$. *J. Algebra*, 70(1):23–36, 1981.

[CY07] Chieh-Yu Chang and Jing Yu. Determination of algebraic relations among special zeta values in positive characteristic. *Adv. Math.*, 216(1):321–345, 2007.

[Dri74] V. G. Drinfeld. Elliptic modules. *Mat. Sb. (N.S.)*, 94(136):594–627, 656, 1974.

[EP05] Antonio J. Engler and Alexander Prestel. *Valued fields*. Springer, Berlin, 2005.

[FJ08] Michael D. Fried and Moshe Jarden. *Field arithmetic*. Springer, Berlin, third edition, 2008.

[FvdP04] Jean Fresnel and Marius van der Put. *Rigid analytic geometry and its applications*. Birkhäuser Boston Inc., 2004.

[HS99] Peter A. Hendriks and Michael F. Singer. Solving difference equations in finite terms. *J. Symbolic Comput.*, 27(3):239–259, 1999.

[Kle88] Peter B. Kleidman. The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, the Ree groups ${}^2G_2(q)$, and their automorphism groups. *J. Algebra*, 117(1):30–71, 1988.

[Kuh10] F.-V. Kuhlmann. Maps on ultrametric spaces, Hensel's Lemma, and differential equations over valued fields. *To appear in: Comm. in Alg; available at arXiv:1003.5677v1*, 2010.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer, New York, third edition, 2002.

[Mal03] Gunter Malle. Explicit realization of the Dickson groups $G_2(q)$ as Galois groups. *Pacific J. Math.*, 212(1):157–167, 2003.

[Mat89] Hideyuki Matsumura. *Commutative ring theory*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, second edition, 1989.

[Mat01] B. Heinrich Matzat. *Differential Galois Theory in Positive Characteristic*. Notes from a class given by B.H. Matzat. IWR-Preprint No. 2001-35, available on http://www.iwr.uni-heidelberg.de/organization/sfb359/Preprints2001.html, 2001.

[Mat04] B. Heinrich Matzat. Frobenius modules and Galois groups. In *Galois theory and modular forms*, volume 11, pages 233–267. Kluwer Acad. Publ., Boston, 2004.

[Mat09] B. Heinrich Matzat. Frobenius modules and Galois representations. *Ann. Inst. Fourier (Grenoble)*, 59(7):2805–2818, 2009.

[MS96] C. Mitschi and M. F. Singer. Connected linear groups as differential Galois groups. *J. Algebra*, 184(1):333–361, 1996.

[MSW94] Gunter Malle, Jan Saxl, and Thomas Weigel. Generation of classical groups. *Geom. Dedicata*, 49(1):85–116, 1994.

[Nor94] Madhav V. Nori. Unramified coverings of the affine line in positive characteristic. In *Algebraic geometry and its applications (West Lafayette, IN, 1990)*, pages 209–212. Springer, New York, 1994.

[Pap08] Matthew A. Papanikolas. Tannakian duality for Anderson-Drinfeld motives and algebraic independence of Carlitz logarithms. *Invent. Math.*, 171(1):123–174, 2008.

[Spr09] T. A. Springer. *Linear algebraic groups*. Birkhäuser Boston Inc., second edition, 2009.

[Ste65] Robert Steinberg. Regular elements of semisimple algebraic groups. *Inst. Hautes Études Sci. Publ. Math.*, (25):49–80, 1965.

[SV00] Tonny A. Springer and Ferdinand D. Veldkamp. *Octonions, Jordan algebras and exceptional groups*. Springer, Berlin, 2000.

[Tae09] Lenny Taelman. Artin t-motifs. *J. Number Theory*, 129(1):142–157, 2009.

[vdPS97] Marius van der Put and Michael F. Singer. *Galois theory of difference equations*, volume 1666 of *Lecture Notes in Mathematics*. Springer, Berlin, 1997.

[vdPS03] Marius van der Put and Michael F. Singer. *Galois theory of linear differential equations*. Springer, Berlin, 2003.

[Wib10a] M. Wibmer. A Chevalley theorem for difference equations. *To appear in: Math.Ann. Available on arXiv:1010.5066*, 2010.

[Wib10b] M. Wibmer. *Geometric Difference Galois Theory*. PhD Thesis, Heidelberg, 2010.

[Wil09] Robert A. Wilson. *The finite simple groups*, volume 251 of *Graduate Texts in Mathematics*. Springer London Ltd., London, 2009.

Lebenslauf

Persönliche Daten

Name	Annette Sophie Maier
Geburtsdatum	28.06.1985
Geburtsort	Freiburg
Staatsangehörigkeit	deutsch

Qualifikationen

Juni 2004	Abitur am Friedrich Gymnasium Freiburg
2004-2008	Ruprecht-Karls-Universität Heidelberg, Studium Mathematik mit Nebenfach Physik
2007-2008	Cornell University, Ithaca, New York, USA
Dezember 2008	Diplom
2009-2011	Promotion an der RWTH Aachen unter Betreuung von Prof. Dr. Julia Hartmann