Frobenius Difference Equations with Classical Groups as Galois Groups

Annette Maier

September 11, 2012

Abstract

We construct explicit Frobenius difference equations with Galois groups SL_n, Sp_{2d}, SO_n and G_2. In addition, we show that these groups occur as Galois groups of certain pre-t-motives.

Introduction

The Galois theory of difference equations is built in analogy to the classical Galois theory of polynomial equations. Given a linear difference equation over a difference field (F, σ), there is the notion of a *Picard-Vessiot ring* which is defined as a simple difference ring without new constants that is generated by a full set of solutions to the given difference equation. If such a ring exists, the *difference Galois group* can be defined and it is an affine group scheme over the field of constants C. Similar to the inverse problem in classical Galois theory, it is a natural question to ask which affine group schemes over C occur as Galois groups of some difference equations over the fixed base (F, σ) .

We consider the case when $F = \mathbb{F}_q(s, t)$ 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. Then the constants of F are $C = \mathbb{F}_q(t)$. Linear difference equations over this difference field are sometimes called *Frobenius difference equations.* The main result of this manuscript 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. We give explicit difference equations for all of these groups (see Theorems 6.4, 7.3, 8.1, 8.2 and 9.2, respectively).

For an outline of the approach, suppose we are given a linear algebraic group $\mathcal{G}$. Suppose that we have a candidate 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 $\mathcal{G}$. It was shown in [Mai12] that if the representing matrix A is contained in $\mathcal{G}(\mathbb{F}_q(s)[t]_{(t)})$ and the coefficient matrices in its t-adic expansion can be bounded in a certain way, there always exists a Picard-Vesstiot ring and furthermore $\mathcal{H}_A \leq \mathcal{G}$ holds, where $\mathcal{H}_A$ denotes the Galois group scheme of the difference equation given by A.
In order to find a candidate A such that also $\mathcal{H}_A \geq \mathcal{G}$ holds, we use a lower bound criterion that was proven in [Mai12]. This criterion asserts that whenever A is contained in $\mathcal{G}(\mathbb{F}_q[s]_{(s-\alpha)}[[t]])$ for some $\alpha \in \mathbb{F}_q$, then $\mathcal{H}_A(\mathbb{F}_q[[t]])$ contains a certain conjugate of $A_\alpha \in \mathcal{G}(\mathbb{F}_q[t]_{(t)})$, the specialization of A via $s \mapsto \alpha$. Hence we need to choose A so that it specializes to elements which 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 4.7). Using the so called Steinberg cross section of $\mathcal{G}$, 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.

The upper and lower bound techniques described above have been used in [Mai12] to show that every semisimple and simply-connected linear algebraic group over $\mathbb{F}_q(t)$ occurs as a Galois group of some Frobenius difference equation over $\mathbb{F}_{q^i}(s,t)$ for some suitable $i \in \mathbb{N}$. It should also be mentioned that over $\hat{F} = \overline{\mathbb{F}}_q(s)((t))$, every linear algebraic group defined over $\mathbb{F}_q((t))$ occurs as a difference Galois group, as was shown in [Mat09, Thm. 2.3]. However, this result is based on taking t-adic limits, so it cannot be transferred to our non-complete base field $\mathbb{F}_q(s)(t)$ or even to $\overline{\mathbb{F}}_q(s)(t)$.

We also 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 a 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 which is of importance in the number theory of function fields.

This manuscript is organized as follows. The first section provides some background on the Galois theory of difference equations with not necessarily algebraically closed fields of constants. In Section 2, we set up some notation. In Section 3, we present the upper and lower bound techniques that guarantee that a difference equation has a certain difference Galois group. Section 4 deals with finding generators that generate classical groups even after certain conjugacy. In Section 5, we introduce the Steinberg cross section and explain how to obtain the desired difference equations. In Section 6-9, we then construct difference equations with Galois groups SL_n, Sp_{2d},

SO_n and G_2. In the last section, we translate our results to the language of pre-t-motives.

Acknowledgments. I would like to thank Julia Hartmann for several helpful conversations on this subject.

1 Basics of Difference Galois Theory

In this section we give a short introduction to the Galois theory of difference modules over not necessarily algebraically closed fields of constants. The standard reference is [vdPS97]; unfortunately, the authors restrict themselves to algebraically closed fields of constants and surjective difference homomorphisms ("inversive" difference fields). Arbitrary fields of constants (but still in the inversive case) are treated in [AM05]. A more general approach is taken in [Wib10] which allows certain non-linear difference equations. Most of the statements quoted in this section can be proven similarly to the classical case (inversive and algebraically closed fields of constants). They also follow from the more general theory in [Wib10]. Direct proofs can be found in [Mai11].

Definition 1.1.

- *A* difference ring (R, σ) *is a commutative ring R equipped with a ring homomorphism $\sigma\colon R \to R$. 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 σ. A* difference ideal *of a difference ring R is a σ-stable ideal of R and R is called a* simple difference ring *if its only difference ideals are* (0) *and R.*

- *Let (F, σ) be a difference field and $A \in \mathrm{GL}_n(F)$. Then $\sigma(Y) = AY$ is called a* (linear) difference equation *over F. Let R/F be an extension of difference rings. A matrix $Y \in \mathrm{GL}_n(R)$ satisfying $\sigma(Y) = AY$ (where σ is applied coordinate-wise to Y) is called a* fundamental solution matrix *for $\sigma(Y) = AY$.*

- *Let (F, σ) be a difference field. A* difference module *over F is a finite dimensional F-vector space M together with a σ-semilinear map $\Phi\colon M \to M$, (i.e., Φ is additive and for any $\lambda \in F$ and $x \in M$ we have $\Phi(\lambda x) = \sigma(\lambda)\Phi(x)$) such that there exists a representing matrix D contained in $\mathrm{GL}_n(F)$, where $n = \dim_F(M)$. (The* representing matrix *D with respect to a fixed basis $\mathcal{B}$ of M collects the images of $\mathcal{B}$ under Φ in its columns.) A* fundamental solution matrix *for M in some difference ring extension $R \geq F$ is defined to be a fundamental matrix for D^{-1} contained in $\mathrm{GL}_n(R)$. Such a matrix exists if an only if $M \otimes_F R$ is trivial, i.e., there exists a Φ-invariant basis of $M \otimes_F R$.*

Definition 1.2. *Let (F,σ) be a difference field with constants C and let (M,Φ) be a difference module over (F,σ) with representing matrix $D \in \mathrm{GL}_n(F)$. An extension of difference rings R/F is called a Picard-Vessiot ring for M 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., $D\sigma(Y) = Y$.*
- *R is generated as an 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 1.3. *Similarly, a Picard-Vessiot ring for a difference equation $\sigma(Y) = AY$ over F is a simple difference ring with no new constants that is generated as an F-algebra by the entries of a fundamental matrix Y, i.e., $\sigma(Y) = AY$.*

The next theorem guarantees the existence of Picard-Vessiot rings provided there exists a fundamental matrix contained in a difference field extension with no new constants.

Theorem 1.4. *Let (F,σ) be a difference field with field of constants C and let M be a difference module over F. Assume that L/F is a difference field extension such that*

a) The field of constants of L is C,

b) There exists a fundamental matrix $Y \in \mathrm{GL}_n(L)$, i.e., $D\sigma(Y) = Y$,

Then $R := F[Y,Y^{-1}] \subseteq L$ is a Picard-Vessiot ring for M.

We now sketch the 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. We will not assume our Picard-Vessiot ring to be integral.

Definition 1.5. *Let (F,σ) be a difference field with field of constants C and let R be a Picard-Vessiot ring for some difference module over 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 $\mathrm{Aut}^\sigma(R \otimes_C S/F \otimes_C S)$ of difference automorphisms fixing $F \otimes_C S$. Note that we consider $R \otimes_C S$ as difference ring via $\sigma \otimes \mathrm{id}$.*

Proposition 1.6. *Let (F,σ) be a difference field with constants C and let R/F be a Picard-Vessiot ring for a difference module over 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* $\sigma \otimes_F \sigma$ *and* $\sigma \otimes_C \mathrm{id}$*, and* $C_{R\otimes_F R}$ *denotes the constants of* $R \otimes_F R$*.*

Theorem 1.7. *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*. If moreover* R *is separable over* F*, then* $\mathcal{G} = \underline{Aut}(R/F)$ *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").*

Definition 1.8. *Let* (F, σ) *be a difference field with field of constants* C *and let* (M, Φ) *be a difference module over* (F, σ) *with a Picard-Vessiot ring* R*. Then we call* $\underline{Aut}(R/F)$ *the Galois group scheme of* M *(with respect to* R*, which is not unique, in general). Two different Picard-Vessiot rings for the same difference module yield Galois groups that are isomorphic over an algebraic closure of* C*.*

As a corollary to Proposition 1.6, one also gets the well-known identity between transcendence degree of Picard-Vessiot extensions and dimension of their Galois group scheme. An explicit linearization of $\mathcal{G} = \underline{Aut}(R/F)$ can be given using a fundamental solution matrix:

Proposition 1.9. *Let* R *be a Picard-Vessiot ring for a difference module over a difference field* (F, σ) *with fundamental matrix* $Y \in \mathrm{GL}_n(R)$*. 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*

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

Proposition 1.9 becomes particularly useful for obtaining upper bounds on the Galois group $\mathcal{G}$: Let R/F be a separable Picard-Vessiot ring with Galois group scheme $\mathcal{G}$. 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 $\mathcal{G} \cong \rho(\mathcal{G})$ is thus contained in $\tilde{\mathcal{G}}$.

2 Notation

q	a power of a prime p.
$(\mathbb{F}_q(s), \lvert\cdot\rvert)$	rational function field over $\mathbb{F}_q$ with s-adic absolute value $\lvert\cdot\rvert$.
$(K, \lvert\cdot\rvert)$	the completion of an algebraic closure of the completion of $\mathbb{F}_q(s)$ with respect to $\lvert\cdot\rvert$. Note that K is algebraically closed.
$(\mathcal{O}_{\lvert\cdot\rvert}, \mathfrak{m})$	the valuation ring $\mathcal{O}_{\lvert\cdot\rvert} \subset K$ corresponding to $\lvert\cdot\rvert$ with maximal ideal $\mathfrak{m}$.

$\overline{\mathbb{F}_q(s)}$, $\overline{\mathbb{F}_q(s)}^{\text{sep}}$	the (separable) algebraic closure of $\mathbb{F}_q(s)$ contained in K.
$K\{t\}$	the ring of power series that converge on the closed unit disk: $K\{t\} := \{\sum_{i=0}^{\infty} \alpha_i t^i \in K[[t]] \mid \lim\limits_{i\to\infty} \lvert\alpha_i\rvert = 0\}$.
L	the field of fractions of $K\{t\}$.
(K, ϕ_q)	$\phi_q \colon K \to K,\ \lambda \mapsto \lambda^q$ is the ordinary Frobenius endomorphism on K. The field of constants equals $\mathbb{F}_q$.
$(K((t)), \phi_q)$	the action of ϕ_q on Laurent series over K is defined coefficient-wise. The field of constants equals $\mathbb{F}_q((t))$.
(L, ϕ_q)	the action of ϕ_q on $K((t))$ induces a homomorphism on $L \subseteq K((t))$. The field of constants then equals $\mathbb{F}_q(t)$.
$(\mathbb{F}_q(s)(t), \phi_q)$	the difference structure on $\mathbb{F}_q(s)(t)$ is induced by that on $K(t) \subseteq L$, i.e., ϕ_q only acts on the coefficients of a rational function. The field of constants also equals $\mathbb{F}_q(t)$.
M_n	$n \times n$-matrices.
A^B	for a ring R, $A \in \mathrm{M}_n(R)$ and $B \in \mathrm{GL}_n(R)$, A^B denotes the conjugate $B^{-1}AB$.

3 Bounds on Difference Galois Groups

In this section we introduce upper and lower bounds on the Galois group of a difference equation over $(\mathbb{F}_q(s,t), \phi_q)$ that were proven in [Mai12].

Theorem 3.1. *Let $\mathcal{G} \leq \mathrm{GL}_n$ be a connected linear algebraic group defined over $\mathbb{F}_q(t)$. Let (M, Φ) be an n-dimensional ϕ_q-module over $\mathbb{F}_q(s,t)$ with representing matrix $D \in \mathcal{G}(\mathbb{F}_q(s,t))$*

a) Assume that D is contained in $\mathrm{GL}_n(\mathcal{O}_{\lvert\cdot\rvert}[[t]])$ with t-adic expansion $D = \sum_{l=0}^{\infty} D_l t^l$ such that there exists a $\delta < 1$ with

$$\lvert\lvert D_l \rvert\rvert \leq \delta^l$$

for all $l \in \mathbb{N}$ (where $\lvert\lvert\cdot\rvert\rvert$ denotes the maximum norm with respect to $\lvert\cdot\rvert$). Then there exists a fundamental solution matrix $Y \in \mathcal{G}(L \cap \mathcal{O}_{\lvert\cdot\rvert}[[t]])$ for M, i.e., $D\phi_q(Y) = Y$. Furthermore, all entries of Y are contained in $\overline{\mathbb{F}_q(s)}^{\text{sep}}((t))$.

b) Assume that there exists a fundamental solution matrix $Y \in \mathcal{G}(K[[t]])$ generating an integral and separable Picard-Vessiot ring $R/\mathbb{F}_q(s,t)$ of M. Let $\mathcal{H} \leq \mathcal{G}$ be the corresponding Galois group scheme. Then for any $\alpha \in \mathbb{F}_q$ with $D \in \mathcal{G}(\mathbb{F}_q[s]_{(s-\alpha)}[[t]])$, $\mathcal{H}(\mathbb{F}_q[[t]])$ contains a $\mathcal{G}(\overline{\mathbb{F}}_q[[t]])$-conjugate of D_α, where $D_\alpha \in \mathcal{G}(\mathbb{F}_q(t))$ denotes the matrix obtained from D via specializing $s \mapsto \alpha$.

The existence of a fundamental solution matrix inside GL_n under the assumptions of a) is shown in [Mai12, Theorem 4.3.] via an Henselian type of argument. If the constants are algebraically closed, it is a classical theorem that $D \in \mathcal{G}(\mathbb{F}_q(s,t))$ implies the existence of a fundamental solution matrix inside $\mathcal{G}$ (see [vdPS03, Prop. 1.31]). The proof doesn't carry over to the case of non-algebraically closed fields of constants; however with the assumptions in a) it can be shown to be true for difference equations over $(\mathbb{F}_q(s,t), \phi_q)$ (see [Mai12, Theorem 4.6]). The proof uses a theorem of Chevalley ([Spr09, Theorem 5.5.3]). To see that all entries of Y are contained in $\overline{\mathbb{F}_q(s)}^{\mathrm{sep}}((t))$, one expands the equation $D\phi_q(Y) = Y$ t-adically (see [Mai12, Prop. 4.10]).

Part b) is a special case of [Mai12, Theorem 4.12]. The proof also uses the theorem of Chevalley. The conjugating matrix inside $\mathcal{G}(\overline{\mathbb{F}}_q[[t]])$ is constructed as a certain specialization of the fundamental solution matrix.

4 Generating Classical Groups

Using the lower bound criterion (Theorem 3.1.b), 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 such conjugates still generate the given group $\mathcal{G}$ that we would like to realize as difference Galois group. For the series $\mathrm{SL}_n, \mathrm{Sp}_{2d}, \mathrm{SO}_n$, we lift known results on generators of the finite parts $\mathcal{G}(\mathbb{F}_q)$ due to Malle, Saxl and Weigel ([MSW94]). The group G_2 will be treated separately in Section 9.

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). 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 1.

$\mathcal{G}$	$n_1(q)$	$n_2(q)$
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 1: Definition of $n_1(q)$ and $n_2(q)$

Theorem 4.1 (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*

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

Remark 4.2. *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 Section 6.*

For $\mathcal{G} \in \{\mathrm{SL}_n, \mathrm{Sp}_{2d}, \mathrm{SO}_n\}$, 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 $\mathcal{G}$. It is then easy to see that 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 2: Definition of σ_1, σ_2

Definition 4.3. *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 in Table 2. 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 4.4. *Let* $\mathcal{G}$, T_1 *and* T_2 *be as in Definition 4.3. 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 that T_1 and T_2 are defined over $\mathbb{F}_q$ with $\mathbb{F}_q$-rational points

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

Elementary calculations then yield $|T_i(\mathbb{F}_q)| = n_i(q),\ i = 1, 2.$ □

Our aim 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. A proof can be found in [Mai12, Prop. 5.1]

Proposition 4.5. *Let K_1 be an infinite field and let $\mathcal{G} \le \mathrm{GL}_n$ 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.*

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) from $\mathbb{F}_q$ to an infinite field $\mathbb{F}$.

Proposition 4.6. *Let $\mathcal{G}$ be one of the following classical groups*

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

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 4.3. Let l_0 be the least common multiple of the order of σ_1 and σ_2. Then for the infinite field $\mathbb{F} := \bigcup_{l \in \mathbb{N}:\ l \equiv 1 \bmod l_0} \mathbb{F}_{q^l} \subseteq \overline{\mathbb{F}}_q$ 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 $\phi_q(g_i) = w_i^{-1} g_i$ holds. Hence for any l with $l \equiv 1 \mod l_0$ we have $\phi_{q^l}(g_i) = \phi_{q^{l-1}}(w_i^{-1} g_i) = \dots = w_i^{-l} \cdot g_i$, where we used that w_i is contained in $\mathcal{G}(\mathbb{F}_q)$. We conclude $g_i \phi_{q^l}(g_i)^{-1} = w_i^l$. Now w_i^l is again monomial with respect to $\sigma_i^l = \sigma_i$. It thus follows from Proposition 4.4 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 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 4.7. *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 4.3. Then for any $A, B \in \mathcal{G}(\mathbb{F}_q + t\overline{\mathbb{F}}_q[[t]])$, 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 4.6. By Proposition 4.5 (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 $\mathcal{G}(\mathbb{F}_q + t\overline{\mathbb{F}}_q[[t]])$, it follows that A_0 and B_0 are contained in $\mathcal{G}(\mathbb{F}_q)$. By Proposition 4.6, 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 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 $\mathcal{G}(\mathbb{F}_q + t\overline{\mathbb{F}}_q[[t]])$-conjugates of the maximal tori T_1 and T_2 are contained in $\mathcal{H}$.

The lower bound criterion (Theorem 3.1 b)) provides us with $\mathcal{G}(\overline{\mathbb{F}}_q[[t]])$-conjugates of certain elements that are contained in the Galois group. The following proposition (see [Mai12, Prop. 5.3] for a proof) allows 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:

Proposition 4.8. *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 $\mathcal{G}(\mathbb{F}_q + t \cdot \overline{\mathbb{F}}_q[[t]])$.*

The following lemma (which can be proven easily using elementary linear algebra) will also be useful.

Lemma 4.9. *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 $\mathrm{GL}_n(\mathbb{F}[[t]])$.*

5 The Steinberg Cross Section

In this section, we explain how we construct the representing matrices D of the difference modules with classical Galois groups. Given a difference module M over F with representing matrix D, we know that the Galois group contains conjugates of all permissible specializations of D, by Theorem 3.1. On the other hand, Theorem 4.7 provides elements that generate a given classical group $\mathcal{G}$ even after certain conjugations.

Theorem 5.1 (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 $\{\alpha_i \mid 1 \leq i \leq r\}$ 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.*

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

Let now $\mathcal{G}$ be a classical group and 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 $f_1, \ldots f_r$ will be chosen inside $\mathbb{F}_q(s,t)$ in a suitable way. Consider specializations $s \mapsto \alpha \in \mathbb{F}_q$. Assume that $f_1, \ldots f_r \in \mathbb{F}_q(s,t)$ have been fixed and that they specialize to elements $\overline{f}_1, \ldots, \overline{f}_r \in \mathbb{F}_q(t)$ (i.e., no coefficient of $f_i \in \mathbb{F}_q(s)(t)$ has denominator divisible by $(s-\alpha)$, for $1 \leq i \leq r$). Then $D_{(f_1,\ldots,f_r)}$ specializes to $D_{(\overline{f}_1,\ldots,\overline{f}_r)}$, an element in the cross section over $\mathbb{F}_q(t)$. Now Theorem 5.1 asserts that

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

contains elements in every regular conjugacy class of $\mathcal{G}(\overline{\mathbb{F}_q(t)})$, if $\mathcal{G}$ is simply-connected. Hence the elements $\{f_1, \ldots, f_r\}$ have to be chosen in such a way that they specialize to the elements $\{\overline{f}_1, \ldots, \overline{f}_r\}$ corresponding to conjugates of the desired generators. Not all of the groups treated later on are simply-connected (SO_n is not), so Theorem 5.1 doesn't apply. However, this does not affect us much as we don't actually apply the theorem but only use it as starting point how to choose the matrix D.

6 Special Linear Groups

For any elements $f_1, \ldots, f_{n-1}$, we set

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

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

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

Remark 6.1. *It is straightforward to compute that the equation*

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

corresponds to the scalar difference equation

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

The aim of this section is to construct elements $f_1, \ldots, f_{n-1} \in \mathbb{F}_q(s,t)$ such that $D_{(f_1,\ldots,f_{n-1})}$ defines a difference module over $(\mathbb{F}_q(s,t), \phi_q)$ with difference Galois group SL_n.

Lemma 6.2. *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*

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

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 (1)). Note that all p_i are invertible inside $\overline{\mathbb{F}}_q[[t]]$, since their product equals 1. By Lemma 4.9, 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. □

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 Definition 4.3 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 are monomial matrices inside $\mathrm{SL}_n(\mathbb{F}_q)$ corresponding to the permutations $\sigma_1 = (1, 2, \dots, n)$ and $\sigma_2 := (1, 2, \dots, n-1)$.

Proposition 6.3. *Let $n \geq 2$ and assume $(n, q) \neq (2, 2)$ and $(n, q) \neq (2, 3)$. Then for $i = 1, 2$, t_i as defined in Table 3 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 $\mathrm{diag}(p_1, \dots, p_n)$ and $\mathrm{diag}(\tilde{p}_1, \dots, \tilde{p}_n)$ 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 $p_1, \dots, p_n$ as well as $\tilde{p}_1, \dots, \tilde{p}_n$ are contained in $\overline{\mathbb{F}}_q[[t]]^\times$. Therefore, $\mathrm{diag}(p_1, \dots, p_n)$ and $\mathrm{diag}(\tilde{p}_1, \dots, \tilde{p}_n)$ 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 $\phi_q(p_1) = p_2, \dots, \phi_q(p_{n-1}) = p_n, \phi_q(p_n) = p_1$ holds, as $\zeta_1^{q^n} = \zeta_1$. Hence

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

Similarly, $\phi_q(t_2) = t_2$ holds, as $\phi_q(\tilde{p}_1) = \tilde{p}_2, \dots, \phi_q(\tilde{p}_{n-1}) = \tilde{p}_1$ 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

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

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
$p_i \in \overline{\mathbb{F}}_q[t]_{(t)}$ $\tilde{p}_i \in \overline{\mathbb{F}}_q[t]_{(t)}$	$p_1 := \frac{t+\zeta_1}{t+\zeta_1^q},\ p_2 := \frac{t+\zeta_1^q}{t+\zeta_1^{q^2}}, \dots,\ p_n := \frac{t+\zeta_1^{q^{n-1}}}{t+\zeta_1}$ $\tilde{p}_1 := t + \zeta_2,\ \tilde{p}_2 := t + \zeta_2^q, \dots,\ \tilde{p}_{n-1} := t + \zeta_2^{q^{n-2}},$ $\tilde{p}_n := (\tilde{p}_1 \cdots \tilde{p}_{n-1})^{-1}$
t_1 t_2	$t_1 := \operatorname{diag}(p_1, \dots, p_n)^{g_1}$ $t_2 := \operatorname{diag}(\tilde{p}_1, \dots, \tilde{p}_n)^{g_2}$
$h_i \in \mathbb{F}_q[t]_{(t)}$ $\tilde{h}_i \in \mathbb{F}_q[t]_{(t)}$	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
$H_i \in \mathbb{F}_q(s,t)$ $\tilde{H}_i \in \mathbb{F}_q(s,t)$	$H_i := \frac{s \sum_{j=0}^{n} a_{ij} t^j}{b_{i0} + s \sum_{j=1}^{n} b_{ij} t^j},\ \ 1 \leq i \leq n-1$ $\tilde{H}_i := \frac{\frac{s}{\alpha} \sum_{j=0}^{2n-2} \tilde{a}_{ij} t^j}{\tilde{b}_{i0} + \frac{s}{\alpha} \sum_{j=1}^{n-1} \tilde{b}_{ij} t^j},\ \ 1 \leq i \leq n-1$
$f_i \in \mathbb{F}_q(s,t)$	$f_i := \frac{s-\alpha}{1-\alpha} H_i + \frac{s-1}{\alpha-1} \tilde{H}_i,\ \ 1 \leq i \leq n-1$

Table 3: Definition of $f_1, \dots, f_{n-1}$ for $\mathcal{G} = \mathrm{SL}_n$.

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 $T_0^{g_1} = T_1$.
Similarly, one concludes that the centralizer of $t_{2,0}$ equals T_2 using the assumption $(n,q) \neq (2,3),(2,2)$.

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 (see [Bor91, Cor. 8.2]). Any character of T_0 is of the form $\chi_1^{e_1}\dots\chi_{n-1}^{e_{n-1}}$ for an $(e_1,\dots,e_{n-1}) \in \mathbb{Z}^{n-1}$, where χ_i denotes the projection on the i-th diagonal entry. Assume that $\chi(t_1^{g_1^{-1}}) = 1$, i.e. $1 = \chi(\mathrm{diag}(p_1,\dots,p_n)) = p_1^{e_1}\dots p_{n-1}^{e_{n-1}}$. By definition of $p_1,\dots,p_n$, this implies

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

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

Theorem 6.4. *Assume $q > 2$ and $n \ge 2$ 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 $D_{(f_1,\dots,f_{n-1})}$ as on page 12 with $f_i \in F$ as defined in Table 3. 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 of M with respect to R is isomorphic to SL_n (as linear algebraic group over $\mathbb{F}_q(t)$).*

Proof. We abbreviate $D := D_{(f_1,\dots,f_{n-1})}$. All non-constant coefficients of the numerators and denominators of H_i and $\tilde{H}_i$ $(1 \le i \le n-1)$ 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 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, $1 \le i \le n-1$. We conclude $D = \sum_{l=0}^\infty D_l t^l \in \mathrm{SL}_n(\mathcal{O}_{|\cdot|}[[t]])$ satisfies $||D_l|| \le \delta^l$ for all $l \in \mathbb{N}$. By part a) of Theorem 3.1, there exists a fundamental solution matrix $Y = \sum_{l=0}^\infty Y_l t^l \in \mathrm{SL}_n(L \cap K[[t]])$. Then $R := F[Y,Y^{-1}] \subseteq L$ is a Picard-Vessiot ring for M by Theorem 1.4. Again by Theorem 3.1.a), all entries of Y are contained in $\overline{\mathbb{F}_q(s)}^{\mathrm{sep}}((t))$, hence R/F is separable (as $\overline{\mathbb{F}_q(s)}^{\mathrm{sep}}((t))$ is a separable extension of F). We conclude that the Galois group scheme $\mathcal{H}$ of (M,Φ) with respect to R is a linear algebraic group (see Theorem 1.7) defined over $\mathbb{F}_q(t)$ that is a closed subgroup of SL_n

(see Proposition 1.9). We will now use the lower bound criterion (Part b) of Theorem 3.1) to show that $\mathcal{H}$ is all of SL_n.

Set $\mathfrak{o}_1 := \mathbb{F}_q[s]_{(s-1)}$ and $\mathfrak{o}_2 := \mathbb{F}_q[s]_{(s-\alpha)}$. Note that $H_i \in \mathfrak{o}_j[[t]]$ for $1 \leq i \leq n-1$, $j = 1, 2$ 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 Part b) of Theorem 3.1 to conclude that $\mathcal{H}(\mathbb{F}_q[[t]])$ contains $\mathrm{SL}_n(\overline{\mathbb{F}}_q[[t]])$-conjugates of the specializations D_1 and D_α of D.

Specializing $s \mapsto 1$ maps f_i to h_i $(1 \leq i \leq n-1)$, thus $D_1 = D_{(h_1,\ldots,h_{n-1})}$. Similarly, $D_\alpha = D_{(\tilde{h}_1,\ldots,\tilde{h}_{n-1})}$ as specializing $s \mapsto \alpha$ maps f_i to $\tilde{h}_i$. Set

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

Lemma 6.2 implies that D_1 and D_α are conjugate to d_1 and 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 x_1 and x_2 of $t_1 = d_1^{g_1}$ and $t_2 = d_2^{g_2}$ which are themselves contained in $\mathrm{SL}_n(\mathbb{F}_q[[t]])$ (see Proposition 6.3). By Proposition 4.8 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 6.3, so $\mathcal{H}$ contains $< T_1^{A_1}, T_2^{A_2} >$. For $n \geq 3$, Theorem 4.7 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. 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 and the constant term of t_1 equals $\mathrm{diag}(\zeta_1^{1-q}, \zeta_1^{-1+q})^{g_1}$. 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 6.5. *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 Part a) of Theorem 3.1).*

7 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

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

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

$$g(X) = X^{2d} - \sum_{i=1}^{d-1} f_i X^{2d-i} - f_d X^d - \sum_{i=1}^{d-1} f_i X^i + 1. \tag{3}$$

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

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:

$$X^{2d} + a_1 X^{2d-1} + \cdots + a_{d-1}X^{d+1} + a_d X^d + a_{d-1}X^{d-1} + \cdots + a_1 X + 1 \quad (4)$$

Lemma 7.1. *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*

$$\prod_{i=1}^{d}(X - p_i)(X - p_i^{-1}) = X^{2d} - \sum_{i=1}^{d-1} h_i X^{2d-i} - h_d X^d - \sum_{i=1}^{d-1} h_i X^i + 1. \quad (5)$$

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 Equation 4, 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 (3), 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 $t_0 = \mathrm{diag}(p_{\sigma(1)}, \ldots, p_{\sigma(2d)})$ holds. Now t_0 is symplectic, 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 $1 \leq i \leq d$. Therefore, σ gives rise to a symplectic permutation matrix $A_\sigma \in \mathcal{G}(\mathbb{F}_q)$. 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 $\mathcal{G}(\overline{\mathbb{F}}_q[[t]])$. Lemma 4.9 implies that there exists a $C \in \mathrm{GL}_n(\overline{\mathbb{F}}_q[[t]])$ with $D^C_{(h_1,\ldots,h_d)} = \mathrm{diag}(p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1}) = t_0$. 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

$$\begin{aligned} C^{\mathrm{tr}} J C &= \mathrm{diag}(\alpha_1, \ldots, \alpha_d, 1 \ldots, 1) g^{\mathrm{tr}} J g \, \mathrm{diag}(\alpha_1, \ldots, \alpha_d, 1 \ldots, 1) \\ &= \mathrm{diag}(\alpha_1, \ldots, \alpha_d, 1 \ldots, 1) J \, \mathrm{diag}(\alpha_1, \ldots, \alpha_d, 1 \ldots, 1) \\ &= \left(\begin{array}{ccc|ccc} & & & & & -\alpha_1 \\ & & & & \iddots & \\ & & & -\alpha_d & & \\ \hline & & \alpha_d & & & \\ & \iddots & & & & \\ \alpha_1 & & & & & \end{array} \right), \end{aligned} \tag{6}$$

so all entries of $C^{\mathrm{tr}} J C$ away from the "reversed diagonal" (by which we mean the $(i, 2d+1-i)$-th coordinates, $1 \le i \le 2d$) are zero, that is, C is already quite close to being symplectic. Equation (6) 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 $\mathrm{Sp}_{2d} \le \mathrm{SL}_{2d}$), 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 $g \in \mathcal{G}(\overline{\mathbb{F}}_q[[t]])$. □

Proposition 7.2. *Let $n = 2d \ge 4$ such that $(n, q) \ne (4, 2)$. Let $T_0 \le \mathrm{Sp}_{2d}$ 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 4.3. Then t_i as defined in Table 4 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. We omit the proof as it is very similar to that of Proposition 6.3. □

Theorem 7.3. *Assume $q > 2$ and $n = 2d \ge 4$.*
Let $M = (F^n, \Phi)$ be the ϕ_q-difference module over $F = \mathbb{F}_q(s, t)$ given by $D_{(f_1, \ldots, f_d)}$ as on page 17 with $f_i \in F$ as defined in Table 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 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 6.4. By replacing every occurrence of "SL_n" and "$n-1$" by "Sp_{2d}" and "d" in the first paragraph of the proof of Theorem 6.4, 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

n q α	$n = 2d \geq 4$ prime power such that $q > 2$ a fixed element in $\mathbb{F}_q^\times \backslash \{1\}$ (e.g. $\alpha = -1$ if q is odd)
$\zeta_1 \in \mathbb{F}_{q^{2d}}$ $\zeta_2 \in \mathbb{F}_{q^d}$	primitive $(q^{2d}-1)$-th root of unity primitive $(q^d - 1)$-th root of unity
$p_i \in \overline{\mathbb{F}}_q[t]_{(t)}^\times$ $\tilde{p}_i \in \overline{\mathbb{F}}_q[t]_{(t)}^\times$	$p_1 := \frac{t+\zeta_1}{t+\zeta_1^{q^d}},\ p_2 := \frac{t+\zeta_1^q}{t+\zeta_1^{q^{d+1}}}, \ldots,\ p_d := \frac{t+\zeta_1^{q^{d-1}}}{t+\zeta_1^{q^{2d-1}}}$ $\tilde{p}_1 := t+\zeta_2,\ \tilde{p}_2 := t+\zeta_2^q, \ldots,\ \tilde{p}_d := t+\zeta_2^{q^{d-1}}$
$g_1,\, g_2 \in \mathrm{Sp}_{2d}(\overline{\mathbb{F}}_q)$	as defined in Definition 4.3
t_1 t_2	$t_1 := \mathrm{diag}(p_1, \ldots, p_d, p_d^{-1}, \ldots, p_1^{-1})^{g_1}$ $t_2 := \mathrm{diag}(\tilde{p}_1, \ldots, \tilde{p}_d, \tilde{p}_d^{-1}, \ldots, \tilde{p}_1^{-1})^{g_2}$
$h_i \in \mathbb{F}_q[t]_{(t)}$ $\tilde{h}_i \in \mathbb{F}_q[t]_{(t)}$	defined via $\prod_{i=1}^{d} (X - p_i)(X - p_i^{-1})$ $= X^{2d} - \sum_{i=1}^{d-1} h_i X^{2d-i} - h_d X^d - \sum_{i=1}^{d-1} h_i X^i + 1$ defined via $\prod_{i=1}^{d} (X - \tilde{p}_i)(X - \tilde{p}_i^{-1})$ $= X^{2d} - \sum_{i=1}^{d-1} \tilde{h}_i X^{2d-i} - \tilde{h}_d X^d - \sum_{i=1}^{d-1} \tilde{h}_i X^i + 1$
$a_{ij}, b_{ij} \in \mathbb{F}_q$ $\tilde{a}_{ij}, \tilde{b}_{ij} \in \mathbb{F}_q$	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
$H_i \in \mathbb{F}_q(s,t)$ $\tilde{H}_i \in \mathbb{F}_q(s,t)$	$H_i := \frac{s \sum_{j=0}^{2d} a_{ij} t^j}{b_{i0} + s \sum_{j=1}^{2d} b_{ij} t^j},\ \ 1 \leq i \leq d$ $\tilde{H}_i := \frac{\frac{s}{\alpha} \sum_{j=0}^{2d} \tilde{a}_{ij} t^j}{\tilde{b}_{i0} + \frac{s}{\alpha} \sum_{j=1}^{d} \tilde{b}_{ij} t^j},\ \ 1 \leq i \leq d$
$f_i \in \mathbb{F}_q(s,t)$	$f_i := \frac{s-\alpha}{1-\alpha} H_i + \frac{s-1}{\alpha-1} \tilde{H}_i,\ \ 1 \leq i \leq d$

Table 4: Definition of $f_1, \ldots, f_d$ for $\mathcal{G} = \mathrm{Sp}_{2d}$.

$\mathcal{H} \leq \mathrm{Sp}_{2d}$ is a linear algebraic group (defined over $\mathbb{F}_q(t)$).

As in the proof of Theorem 6.4, we set $\mathfrak{o}_1 := \mathbb{F}_q[s]_{(s-1)}$ and $\mathfrak{o}_2 := \mathbb{F}_q[s]_{(s-\alpha)}$ inside $k = \mathbb{F}_q(s)$. The same argument as in the proof of Theorem 6.4 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 Part b) of Theorem 3.1 to conclude that $\mathcal{H}(\mathbb{F}_q[[t]])$ contains $\mathrm{Sp}_{2d}(\overline{\mathbb{F}}_q[[t]])$-conjugates of the specialized matrices D_1 and D_α.

Specializing $s \mapsto 1$ maps f_i to h_i ($1 \leq i \leq d$), thus $D_1 = D_{(h_1,\ldots,h_d)}$ and similarly $D_\alpha = D_{(\tilde{h}_1,\ldots,\tilde{h}_d)}$. By Proposition 7.1, $\mathcal{H}(\mathbb{F}_q[[t]])$ thus contains $\mathrm{Sp}_{2d}(\overline{\mathbb{F}}_q[[t]])$-conjugates of t_1 and t_2 as in Proposition 7.2. Applying Proposition 4.8 together with Proposition 7.2, 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 7.2, and $< T_1^{A_1}, T_2^{A_2} >= \mathrm{Sp}_{2d}$ holds by Theorem 4.7, so we conclude $\mathcal{H} = \mathrm{Sp}_{2d}$. □

8 Special Orthogonal Groups

In this section we are only working in characteristic $\neq 2$. Consider the special orthogonal group $\mathcal{G} = \mathrm{SO}_n$ with respect to the orthogonal form given by

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

Everything works along the same line as in the case of the symplectic group, so we skip the proofs.

8.1 Odd Dimension

Theorem 8.1. *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

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

where $f_i \in F$ are as defined in Table 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 of M with respect to R is isomorphic to SO_{2d+1} (as linear algebraic group over $\mathbb{F}_q(t)$).

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
$p_i \in \overline{\mathbb{F}}_q[t]_{(t)}^{\times}$ $\tilde{p}_i \in \overline{\mathbb{F}}_q[t]_{(t)}^{\times}$	$p_1 := \frac{t+\zeta_1}{t+\zeta_1^{q^d}},\ p_2 := \frac{t+\zeta_1^q}{t+\zeta_1^{q^{d+1}}}, \dots,\ p_d := \frac{t+\zeta_1^{q^{d-1}}}{t+\zeta_1^{q^{2d-1}}}$ $\tilde{p}_1 := t+\zeta_2,\ \tilde{p}_2 := t+\zeta_2^q, \dots,\ \tilde{p}_d := t+\zeta_2^{q^{d-1}}$
$h_i \in \mathbb{F}_q[t]_{(t)}$ $\tilde{h}_i \in \mathbb{F}_q[t]_{(t)}$	defined via $h_0 := -1$ and $(X-1)\prod_{i=1}^{d}(X-p_i)(X-p_i^{-1})$ $= X^{2d+1} - \sum_{i=1}^d (h_i + h_{i-1})X^{2d+1-i} + \sum_{i=1}^d (h_i+h_{i-1})X^i - 1$ defined via $\tilde{h}_0 := -1$ and $(X-1)\prod_{i=1}^{d}(X-\tilde{p}_i)(X-\tilde{p}_i^{-1})$ $= X^{2d+1} - \sum_{i=1}^d (\tilde{h}_i + \tilde{h}_{i-1})X^{2d+1-i} + \sum_{i=1}^d (\tilde{h}_i+\tilde{h}_{i-1})X^i - 1$
$a_{ij}, b_{ij} \in \mathbb{F}_q$ $\tilde{a}_{ij}, \tilde{b}_{ij} \in \mathbb{F}_q$	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
$H_i \in \mathbb{F}_q(s,t)$ $\tilde{H}_i \in \mathbb{F}_q(s,t)$	$H_i := \frac{s\sum_{j=0}^{2d} a_{ij}t^j}{b_{i0}+s\sum_{j=1}^{2d} b_{ij}t^j},\ \ 1 \leq i \leq d$ $\tilde{H}_i := \frac{-s\sum_{j=0}^{2d} \tilde{a}_{ij}t^j}{\tilde{b}_{i0}-s\sum_{j=1}^{d} \tilde{b}_{ij}t^j},\ \ 1 \leq i \leq d$
$f_i \in \mathbb{F}_q(s,t)$	$f_i := \frac{s+1}{2}H_i + \frac{1-s}{2}\tilde{H}_i,\ \ 1 \leq i \leq d-1$ $f_d := \frac{s+1}{2}H_d + \frac{1-s}{2}\tilde{H}_d + (s+1)(1-s)$

Table 5: Definition of $f_1, \dots, f_d$ for $\mathcal{G} = \mathrm{SO}_{2d+1}$.

8.2 Even Dimension

Let $n = 2d$ be even. We define the elements $f_1, \dots, f_d \in \mathbb{F}_q(s,t)$. The construction depends on the residue class of d modulo 4.

`if` $d \equiv 1 \mod 2$	
$\zeta \in \mathbb{F}_{q^2}$ $\zeta_1 \in \mathbb{F}_{q^{2d-2}}$ $\zeta_2 \in \mathbb{F}_{q^d}$	primitive (q^2-1)-th root of unity primitive $(q^{2(d-1)}-1)$-th root of unity primitive (q^d-1)-th root of unity
$p_i \in \overline{\mathbb{F}}_q[t]_{(t)}$ $p_d \in \overline{\mathbb{F}}_q[t]_{(t)}$ $\tilde{p}_i \in \overline{\mathbb{F}}_q[t]_{(t)}$	$p_i := \frac{t+\zeta_1^{q^{i-1}}}{t+\zeta_1^{q^{d+i-2}}},\ \ 1 \le i \le d-1$ $p_d := \frac{t+\zeta}{t+\zeta^q}$ $\tilde{p}_i := t + \zeta_2^{q^{i-1}},\ \ 1 \le i \le d$
`if` $d = 2m \equiv 2 \mod 4$	
$\zeta \in \mathbb{F}_{q^2}$ $\zeta_1 \in \mathbb{F}_{q^{2d-2}}$ $\alpha, \beta \in \mathbb{F}_{q^m}$	primitive (q^2-1)-th root of unity primitive $(q^{2(d-1)}-1)$-th root of unity primitive (q^m-1)-th roots of unity 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.
$p_i \in \overline{\mathbb{F}}_q[t]_{(t)}$ $p_d \in \overline{\mathbb{F}}_q[t]_{(t)}$ $\tilde{p}_i \in \overline{\mathbb{F}}_q[t]_{(t)}$	$p_i := \frac{t+\zeta_1^{q^{i-1}}}{t+\zeta_1^{q^{d+i-2}}},\ \ 1 \le i \le d-1$ $p_d := \frac{t+\zeta}{t+\zeta^q}$ $\tilde{p}_i := t + \alpha^{q^{i-1}}, 1 \le i \le m$ $\tilde{p}_{m+i} := t + \beta^{q^{i-1}}, 1 \le i \le m$
`if` $d = 2m \equiv 0 \mod 4$	
$\zeta \in \mathbb{F}_{q^2}$ $\zeta_1 \in \mathbb{F}_{q^{2d-2}}$ $\alpha, \beta \in \mathbb{F}_{q^{2m}}$	primitive (q^2-1)-th root of unity primitive $(q^{2(d-1)}-1)$-th root of unity primitive $(q^{2m}-1)$-th roots of unity such that $\alpha^{\pm(1-q^m)}, \alpha^{\pm(q-q^{m+1})}, \ldots, \alpha^{\pm(q^{m-1}-q^{2m-1})}$, $\beta^{\pm(1-q^m)}, \beta^{\pm(q-q^{m+1})}, \ldots, \beta^{\pm(q^{m-1}-q^{2m-1})}$ are pairwise distinct.
$p_i \in \overline{\mathbb{F}}_q[t]_{(t)}$ $p_d \in \overline{\mathbb{F}}_q[t]_{(t)}$ $\tilde{p}_i \in \overline{\mathbb{F}}_q[t]_{(t)}$	$p_i := \frac{t+\zeta_1^{q^{i-1}}}{t+\zeta_1^{q^{d+i-2}}},\ \ 1 \le i \le d-1$ $p_d := \frac{t+\zeta}{t+\zeta^q}$ $\tilde{p}_i := \frac{t+\alpha^{q^{i-1}}}{t+\alpha^{q^{m+i-1}}},\ \ 1 \le i \le m$ $\tilde{p}_{m+i} := \frac{t+\beta^{q^{i-1}}}{t+\beta^{q^{m+i-1}}},\ \ 1 \le i \le m$

$h_i \in \mathbb{F}_q[t]_{(t)}$	defined via $h_0 := -1$, $h_{-1} := 0$ and $\prod_{i=1}^{d}(X-p_i)(X-p_i^{-1})$ $= X^{2d} + \sum_{i=1}^{d-1}(-h_i + h_{i-2})X^{2d-i} + (-h_d + 2h_{d-2} - \frac{h_{d-1}^2}{h_d})X^d$ $+ \sum_{i=1}^{d-1}(-h_i + h_{i-2})X^i + 1$
$\tilde{h}_i \in \mathbb{F}_q[t]_{(t)}$	defined via $\tilde{h}_0 := -1$, $\tilde{h}_{-1} := 0$ and $\prod_{i=1}^{d}(X-\tilde{p}_i)(X-\tilde{p}_i^{-1})$ $= X^{2d} + \sum_{i=1}^{d-1}(-\tilde{h}_i + \tilde{h}_{i-2})X^{2d-i} + (-\tilde{h}_d + 2\tilde{h}_{d-2} - \frac{\tilde{h}_{d-1}^2}{\tilde{h}_d})X^d$ $+ \sum_{i=1}^{d-1}(-\tilde{h}_i + \tilde{h}_{i-2})X^i + 1$
$a_{ij}, b_{ij} \in \mathbb{F}_q$	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 $\tilde{h}_i$: $\tilde{h}_i(t) = \frac{\sum_{j=0}^{2d} \tilde{a}_{ij}t^j}{\sum_{j=0}^{2d} \tilde{b}_{ij}t^j}$; $\tilde{b}_{i0} \neq 0$ for all i
$H_i \in \mathbb{F}_q(s,t)$	$H_i := \frac{s\sum_{j=0}^{2d} a_{ij}t^j}{b_{i0} + s\sum_{j=1}^{2d} b_{ij}t^j}$, $1 \le i \le d$
$\tilde{H}_i \in \mathbb{F}_q(s,t)$	$\tilde{H}_i := \frac{-s\sum_{j=0}^{2d} \tilde{a}_{ij}t^j}{\tilde{b}_{i0} - s\sum_{j=1}^{2d} \tilde{b}_{ij}t^j}$, $1 \le i \le d$
$f_i \in \mathbb{F}_q(s,t)$	$f_i := \frac{s+1}{2}H_i + \frac{1-s}{2}\tilde{H}_i$, $1 \le i \le d-1$ $f_d := \frac{s+1}{2}H_d + \frac{1-s}{2}\tilde{H}_d + (s+1)(1-s)$

Table 6: Definition of $f_1, \ldots, f_d$ for $\mathcal{G} = \mathrm{SO}_{2d}$.

Theorem 8.2. *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*

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

where $f_i \in F$ are as defined in Table 6. 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 of M with respect to R is isomorphic to SO_{2d} (as linear algebraic group over $\mathbb{F}_q(t)$).

9 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 and 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. We set

$$D^{(\mathrm{odd})}_{(f_1,f_2)} = \begin{pmatrix} -f_1 & -f_2 & 1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -f_1^2 & 0 & -f_1 & f_2 & 1 & 0 \\ 0 & -2f_1 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -f_1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

and

$$D^{(\mathrm{even})}_{(f_1,f_2)} = \begin{pmatrix} f_1 & f_2 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & f_1^2 & 0 & f_2 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & f_1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

(these are generic elements in the Steinberg cross section of G_2).

Proposition 9.1. *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 $\mathbb{F} := \bigcup_{l\in\mathbb{N}:\ l\equiv 1 \bmod 6} \mathbb{F}_{q^l} \subseteq \overline{\mathbb{F}}_q$. Then $\mathbb{F}$ is a field of infinite order. We apply Proposition 4.5 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 $\mathcal{H}(\overline{\mathbb{F}}_q[[t]])$. The lists of maximal subgroups of G_2 (see [Kle88, Thm.A] for q odd and [Coo81, 2.3-2.5.] for q even) imply that $h_{l,0}$ and $\tilde{h}_{l,0}$ generate $G_2(\mathbb{F}_{q^l})$ if $q^l > 8$ and the claim follows easily. □

Theorem 9.2. *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 $D := D^{(\text{odd})}_{(f_1,f_2)}$ if q is odd and $D := D^{(\text{even})}_{(f_1,f_2)}$ if q is even and $f_1, f_2 \in F$ are as defined in Table 7. 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 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 paragraph of the proof of Theorem 6.4 we obtain a fundamental matrix inside $G_2(K[[t]] \cap L)$ with entries in $\overline{\mathbb{F}_q(s)}^{\text{sep}}((t))$. Then $R := F[Y, Y^{-1}] \subseteq \overline{\mathbb{F}_q(s)}^{\text{sep}}((t))$ is a separable Picard-Vessiot ring for M with Galois group scheme $\mathcal{H}$ a linear algebraic group contained in G_2.

Similar to the second paragraph of the proof of Theorem 6.4, 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 $D_\alpha = D_{(\tilde{h}_1,\tilde{h}_2)}$ (via $s \mapsto \alpha$), where $D_{(h_1,h_2)}$ is understood to equal either $D := D^{(\text{odd})}_{(h_1,h_2)}$ or $D := D^{(\text{even})}_{(h_1,h_2)}$ depending on the parity of q. Let d_1 and d_2 denote the following elements of $T_0(\mathbb{F}_{q^6}[[t]])$:

$$\begin{aligned}
d_1 &:= \operatorname{diag}(p_1, p_2, p_1p_2^{-1}, 1, p_1^{-1}p_2, p_2^{-1}, p_1^{-1}) \text{ for odd } q\\
d_2 &:= \operatorname{diag}(\tilde{p}_1, \tilde{p}_2, \tilde{p}_1\tilde{p}_2^{-1}, 1, \tilde{p}_1^{-1}\tilde{p}_2, \tilde{p}_2^{-1}, \tilde{p}_1^{-1}) \text{ for odd } q\\
d_1 &:= \operatorname{diag}(p_1, p_2, p_1p_2^{-1}, p_1^{-1}p_2, p_2^{-1}, p_1^{-1}) \text{ for even } q\\
d_2 &:= \operatorname{diag}(\tilde{p}_1, \tilde{p}_2, \tilde{p}_1\tilde{p}_2^{-1}, \tilde{p}_1^{-1}\tilde{p}_2, \tilde{p}_2^{-1}, \tilde{p}_1^{-1}) \text{ for even } q.
\end{aligned}$$

It is easy to check that the constant parts of d_1 and d_2 have pairwise distinct eigenvalues. Hence we can apply Lemma 4.9 and obtain matrices $A_1, A_2 \in \mathrm{GL}_n(\overline{\mathbb{F}}_q[[t]])$ satisfying

$$\begin{aligned}
D_1 = D_{(h_1,h_2)} &= d_1^{A_1}\\
D_\alpha = D_{(\tilde{h}_1,\tilde{h}_2)} &= d_2^{A_2}.
\end{aligned}$$

q α	prime power ≥ 3 fixed element in $\mathbb{F}_q^\times \backslash \{1\}$
$\zeta_1 \in \mathbb{F}_{q^6}$ $\zeta_2 \in \mathbb{F}_{q^6}$	primitive (q^6-1)-th root of unity primitive (q^3-1)-th root of unity
$p_1, p_2 \in \mathbb{F}_{q^6}[t]_{(t)}$ $\tilde{p}_1, \tilde{p}_2 \in \mathbb{F}_{q^6}[t]_{(t)}$	$p_1 := \frac{(t+\zeta_1^{q^4})(t+\zeta_1^{q^3})}{(t+\zeta_1^q)(t+\zeta_1)},\ p_2 := \frac{(t+\zeta_1^{q^3})(t+\zeta_1^{q^2})}{(t+\zeta_1)(t+\zeta_1^{q^5})}$ $\tilde{p}_1 := \frac{t+\zeta_2^q}{t+\zeta_2},\ \tilde{p}_2 := \frac{t+\zeta_2^{q^2}}{t+\zeta_2}$
$h_1, h_2 \in \mathbb{F}_q[t]_{(t)}$	unique elements such that $D^{(\text{odd})}_{(h_1,h_2)}$ and $\operatorname{diag}(p_1, p_2, p_1p_2^{-1}, 1, p_1^{-1}p_2, p_2^{-1}, p_1^{-1})$ are conjugate if q is odd and $D^{(\text{even})}_{(h_1,h_2)}$ and $\operatorname{diag}(p_1, p_2, p_1p_2^{-1}, p_1^{-1}p_2, p_2^{-1}, p_1^{-1})$ are conjugate if q is even
$\tilde{h}_1, \tilde{h}_2 \in \mathbb{F}_q[t]_{(t)}$	unique elements such that $D^{(\text{odd})}_{(\tilde{h}_1,\tilde{h}_2)}$ and $\operatorname{diag}(\tilde{p}_1, \tilde{p}_2, \tilde{p}_1\tilde{p}_2^{-1}, 1, \tilde{p}_1^{-1}\tilde{p}_2, \tilde{p}_2^{-1}, \tilde{p}_1^{-1})$ are conjugate if q is odd and $D^{(\text{even})}_{(\tilde{h}_1,\tilde{h}_2)}$ and $\operatorname{diag}(\tilde{p}_1, \tilde{p}_2, \tilde{p}_1\tilde{p}_2^{-1}, \tilde{p}_1^{-1}\tilde{p}_2, \tilde{p}_2^{-1}, \tilde{p}_1^{-1})$ are conjugate 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 $\tilde{h}_i$: $\tilde{h}_i(t) = \frac{\sum_{j=0}^{12} \tilde{a}_{ij}t^j}{\sum_{j=0}^{12} \tilde{b}_{ij}t^j}$; $\tilde{b}_{i0} \neq 0$
$H_1, H_2 \in \mathbb{F}_q(s,t)$ $\tilde{H}_1, \tilde{H}_2 \in \mathbb{F}_q(s,t)$	$H_i := \frac{s\sum_{j=0}^{12} a_{ij}t^j}{b_{i0}+s\sum_{j=1}^{12} b_{ij}t^j}$ $\tilde{H}_i := \frac{\frac{s}{\alpha}\sum_{j=0}^{12} \tilde{a}_{ij}t^j}{\tilde{b}_{i0}+\frac{s}{\alpha}\sum_{j=1}^{12} \tilde{b}_{ij}t^j}$
$f_1, f_2 \in \mathbb{F}_q(t,s)$	$f_i := \frac{s-\alpha}{1-\alpha}H_i + \frac{s-1}{\alpha-1}\tilde{H}_i$

Table 7: Definition of f_1, f_2 for $\mathcal{G} = G_2$.

Hence $\mathcal{H}(\mathbb{F}_q[[t]])$ 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_n equal the diagonal torus, 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 4.8 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 $\mathcal{H}(\mathbb{F}_q[[t]])$.

It is easy to verify that no non-trivial character of T_0 maps d_1 or d_2 to zero, hence both d_1 and d_2 generate dense subgroups of T_0 (see [Bor91, Cor. 8.2]). 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. We conclude that $\mathcal{H} \leq G_2$ 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 deduce that $w_i := B_i\phi_q(B_i)^{-1}$ 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: $T_i(\mathbb{F}_q((t))) = \{g_0 \in T_0(\overline{\mathbb{F}}_q((t))) \mid \phi_q(g_0) = g_0^{\sigma_i}\}^{B_i}$. 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., $p_3 := p_1p_2^{-1}$, $p_{-i} := p_i^{-1}$ 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 conclude

$$T_i(\mathbb{F}_{q^l}[[t]]) = \{g_0 \in T_0(\overline{\mathbb{F}}_q[[t]]) \mid \phi_{q^l}(g_0) = g_0^{\sigma_i}\}^{B_i} \qquad (7)$$

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

$$\begin{aligned} x_l &:= \mathrm{diag}(\gamma_l, \gamma_l^{-(q^l)^2}, \gamma_l^{q^l}, (1,)\ \gamma_l^{-(q^l)}, \gamma_l^{(q^l)^2}, \gamma_l^{(q^l)^3}) \\ y_l &:= \mathrm{diag}(\xi_l, \xi_l^{-(q^l)^2}, \xi_l^{-q^l}, (1,)\ \xi_l^{q^l}, \xi_l^{(q^l)^2}, \xi^{-1}). \end{aligned}$$

Then $\gamma_l^{(q^l)^3} = \gamma_l^{-1}$ and $\xi_l^{(q^l)^3} = \xi_l$, hence $\phi_{q^l}(x_l) = x_l^{\sigma_1}$ and $\phi_{q^l}(y_l) = y_l^{\sigma_2}$. Therefore, Equation (7) 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 9.1. □

10 Pre t-motives

We can translate our results to the language of pre-t-motives. In order to conform with the common notation for pre-t-motives, we rename the variable s by θ^{-1} (hence we consider the ∞-adic valuation on $k := \mathbb{F}_q(\theta)$ instead of the s-adic one) and we work with $\sigma = \phi_q^{-1}$ on $\overline{\mathbb{F}_q(\theta)}(t)$ instead of ϕ_q. A pre-t-motive is a σ-difference module over $\overline{\mathbb{F}_q(\theta)}(t)$ and it is called rigid analytically trivial if there exists a Picard-Vessiot ring inside L.

We can now lift our results from $k(t) = \mathbb{F}_q(\theta)(t)$ to $\overline{k}(t) = \overline{\mathbb{F}_q(\theta)}(t)$ to get pre-t-motives with classical Galois groups.

Theorem 10.1. *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 3 on page 14. 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

$$\Phi = \left(\begin{array}{cccc|cccc} \phi_1 & \dots & \phi_{d-1} & \phi_d & 1 & & & \\ 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & 0 & & & & \\ \hline & & & \phi_{d-1} & 0 & 1 & & \\ & & & \vdots & \vdots & & \ddots & \\ & & & \phi_1 & 0 & & & 1 \\ & & & -1 & 0 & & & 0 \end{array}\right)$$

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 4 on page 20. 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

$$\Phi = \left(\begin{array}{cccc|c|cccc}
\phi_1 & \dots & \phi_{d-1} & \phi_d & -2\phi_d & -2\phi_d & & & \\
1 & & & & & & & & \\
 & \ddots & & & & & & & \\
 & & 1 & 0 & & & & & \\
\hline
 & & & 1 & -1 & & & & \\
\hline
 & & & \frac{\phi_{d-1}}{2\phi_d} & & 0 & 1 & & \\
 & & & \vdots & & & & \ddots & \\
 & & & \frac{\phi_1}{2\phi_d} & & & & & 1 \\
 & & & -\frac{1}{2\phi_d} & & & & & 0
\end{array}\right)$$

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 on page 22. 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

$$\Phi = \left(\begin{array}{cccc|cccc}
\phi_1 & \dots & \phi_{d-1} & \phi_d & \phi_{d-1} & -\phi_d & & \\
1 & & & & & & & \\
 & \ddots & & & & & & \\
 & & 1 & 0 & 1 & & & \\
\hline
 & & \frac{\phi_{d-1}}{\phi_d} & 1 & 0 & & & \\
 & & \frac{\phi_{d-2}}{\phi_d} & & 0 & 0 & 1 & \\
 & & \vdots & & & & & \ddots \\
 & & \frac{\phi_1}{\phi_d} & & & & & 1 \\
 & & -\frac{1}{\phi_d} & & & & & 0
\end{array}\right)$$

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 6 on page 24. 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 7 on page 27. 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 7 on page 27. Then* P *is rigid analytically trivial and has Galois group* G_2*.*

Proof. We proved in Theorem 6.4, 7.3, 8.1, 8.2, 9.2, resp., that the above matrices give rise to difference modules over $k(t)$ that possess Picard-Vessiot rings inside L with Galois groups SL_n, Sp_{2d}, SO_n and G_2, respectively. Hence the corresponding difference modules over $\overline{k}(t)$ also have Picard-Vessiot rings inside L (these are generated over $\overline{k}(t)$ by the same fundamental matrix $Y \in \mathrm{GL}_n(L)$ as before) and the pre-t-motives are thus rigid analytically trivial. As all of the groups listed above are connected, the Galois groups stay the same when making a base change from $k(t)$ to the algebraic extension $\overline{k}(t)$. □

It would be interesting to know whether one could also construct t-motives with classical groups as Galois groups. A t-motive is a rigid analytically trivial pre-t-motive such that the representing matrix with respect to some basis has entries inside $\overline{k}[t]$ and determinant $u(t-\theta)^i$ for some $u \in \overline{k}^{\times}$ and $i \in \mathbb{N}$. It is known that extensions of one copy of $\mathbb{G}_m$ by several copies of $\mathbb{G}_a$ occur as Galois groups of t-motives (see [Pap08], [CY07]) whereas $\mathbb{G}_m^n$ (which can easily be realized as the Galois group of a pre-t-motive) does not occur as a t-motivic Galois group for $n \geq 2$.

References

[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.

[Bor91] Armand Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 1991.

[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.

[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.

[Mai11] Annette Maier. *Difference Equations with Semisimple Galois Groups in Positive Characteristic.* PhD Thesis, RWTH Aachen University (available at http://darwin.bth.rwth-aachen.de/opus3/volltexte/2012/3909/), 2011.

[Mai12] Annette Maier. A Difference Version of Nori's Theorem. *Preprint. arXiv:1203.1176v1*, 2012.

[Mat09] B. Heinrich Matzat. Frobenius modules and Galois representations. *Ann. Inst. Fourier (Grenoble)*, 59(7):2805–2818, 2009.

[MSW94] Gunter Malle, Jan Saxl, and Thomas Weigel. Generation of classical groups. *Geom. Dedicata*, 49(1):85–116, 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.

[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.

[Wib10] 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.