JOURNAL OF COMMUTATIVE ALGEBRA
Volume 6, Number 4, Winter 2014

FINITE GROUPS OF LIE TYPE AS GALOIS GROUPS OVER $\mathbb{F}_p(t)$

DAMIAN STICHEL

ABSTRACT. In this paper a realization of all classical and most exceptional finite groups of Lie type defined over a field $\mathbb{F}_q$ (where $q = p^r$ is a prime power) as Galois groups over rational function fields over the prime field $\mathbb{F}_p$ is provided. Our approach runs by restricting the ground field of the groups and using criteria for bounds for Galois groups, derived from the theory of Frobenius modules.

1. Introduction. Let $q = p^r$ be a prime power. Classical Galois theory solves the problem of finding the Galois group of a given Galois extension (respectively, polynomial). Naturally, this also leads to the related question of which group occurs as a Galois group of some polynomial. This is known as the "inverse Galois problem." An overview of the known results and methods of receiving them is given in [**10**].

Naturally, the answer to the inverse problem depends on the ground field. Here the situation in positive characteristics is addressed. It is well known that, by the various patching methods, every finite group can be realized as Galois group over $\overline{\mathbb{F}}_p(\mathbf{t})$ (see, e.g., [**8,** Theorem 4.6]). Hence, there exists a power p^m of p such that the group can also be realized over $\mathbb{F}_{p^m}(\mathbf{t})$. However, the patching method gives no information about m. Considerable progress in this area was made by Abhyankar, who presented a number of nice equations for plenty of the classical groups over function fields over $\mathbb{F}_q$. In numerous papers (e.g., [**1, 2, 4**]) he also established a Galois descent principle which deforms previously constructed additive polynomials over $\mathbb{F}_{q^n}(\boldsymbol{t})$ to have incarnations over $\mathbb{F}_q(\boldsymbol{t})$ without changing their Galois groups, where n is a positive integer and q is a prime power. In his approach using generalized iterates of previously constructed polynomials, a Galois group could be enlarged from $\mathrm{GL}_m(\mathbb{F}_q)$ to $\mathrm{GL}_m(\mathbb{F}_{q^n})$ and, under

Keywords and phrases. Galois groups, additive polynomials, classical groups, Galois descent, ground field restriction.

Received by the editors on August 23, 2013.

DOI:10.1216/JCA-2014-6-4-587

suitable conditions, this gives rise to the descent of a Galois group being realizable over $\mathbb{F}_q$ to its realizability over $\mathbb{F}_p$. However, his interest mostly focused on the group $\mathrm{GL}_m(\mathbb{F}_q)$ and, unfortunately, there is no obvious generalization to proper subgroups.

In this paper, a method to realize all finite groups of Lie type defined over a field $\mathbb{F}_q$ (where $q = p^r$ is a prime power) as Galois groups over rational function fields of the form $\mathbb{F}_p(\boldsymbol{t})$ is developed.

The techniques we use are based on the theory of Frobenius modules due to Matzat [**9**]. This provides criteria for upper and lower bounds of Galois groups. Matzat's results were used by Albert and Maier in [**3**] to realize finite groups of Lie type defined over $\mathbb{F}_q$ as Galois groups over function fields over $\mathbb{F}_q$. We extend this method to realize these groups as Galois groups over function fields over $\mathbb{F}_p$. To receive this Galois descent, we firstly construct a homomorphism which, for groups defined over $\mathbb{F}_q$, delivers a representation as groups defined over $\mathbb{F}_p$. We also prove a formula describing the behavior of the characteristic polynomial of matrices under this transformation (see Proposition 6.8). By selecting suitable Frobenius modules over $\mathbb{F}_p$, the criteria for bounds can be applied in this more general case.

Finally, in Theorem 7.2, we prove that all classical groups and most exceptional finite groups of Lie type with entries in $\mathbb{F}_{p^r}$ occur as Galois groups over smaller fields of characteristic p than had previously been accomplished. We are able to present explicit representing matrices of Frobenius modules over $\mathbb{F}_p(\boldsymbol{t})$ having the desired groups as Galois groups. From the defining equation of the representing matrix, additive polynomials realizing the groups of our interest as Galois groups over $\mathbb{F}_p(\boldsymbol{t})$ can be found by solving a system of equations using Buchberger's algorithm. In the cases where it is possible to write these polynomials in a short and well-arranged shape, we give some examples of these polynomials.

Most results of this paper arose in [**15**], where more detailed proofs can be found.

2. Frobenius modules. We present the most important definitions and results on Frobenius modules and explain how they give rise to Galois extensions of fields whose Galois groups are isomorphic to a subgroup of $\mathrm{GL}_m(\mathbb{F}_q)$. Theorem 2.3 and Corollary 2.5 will be important

in what follows. For more detailed information, see [**9**].

Let $q = p^r$ be a prime power. A *Frobenius field* (F, ϕ_q) is a field F containing $\mathbb{F}_q$, together with the Frobenius endomorphism $\phi_q : F \to F$, $a \mapsto a^q$. A *Frobenius extension* (E, ϕ_q^E) of (F, ϕ_q) is a field $E \supseteq F$ together with its Frobenius endomorphism ϕ_q^E, extending ϕ_q. By abuse of notation, we often write ϕ_q instead of ϕ_q^E for the Frobenius endomorphism on E, as well. A pair (M, Φ_q) consisting of a finite dimensional F-vector space M and an injective ϕ_q-semilinear map $\Phi_q : M \to M$ is called a *Frobenius module* over a *Frobenius field* F. To simplify our notation, we sometimes write Φ instead of Φ_q, in the case where the base field is known.

We define the *solution space* of (M, Φ_q) as $\mathrm{Sol}^{\Phi_q}(M) := \{x \in M \mid \Phi_q(x) = x\}$. Simple calculations show that this set of vectors remaining fixed under Φ_q is a vector space over $\mathbb{F}_q$. (M, Φ_q) is said to be *trivial* if $\mathrm{Sol}^{\Phi_q}(M)$ already contains an F-basis of M.

For a Frobenius extension (E, ϕ_q^E) of F, the tensor product $M_E := E \otimes_F M$ becomes a Frobenius module over E in a natural way. We define the solution space of M over E as $\mathrm{Sol}_E^{\Phi_q}(M) := \mathrm{Sol}^{\Phi_q}(E \otimes_F M)$. It is called *trivial over* E, if $\mathrm{Sol}_E^{\Phi}(M)$ contains an E-basis of M_E.

If M is not already trivial over F, it is always possible to find a suitable Frobenius extension $E \geq F$ of finite degree, such that M becomes trivial over E. A minimal extension with this property is called a *solution field* of M. It turns out to be essentially unique and, in addition, Galois over F. We define the Galois group of the Frobenius module (M, Φ_q) as the Galois group of the solution field: $\mathrm{Gal}^{\Phi_q}(M) := \mathrm{Gal}\,(E/F)$.

Let (M, Φ_q) have dimension m over (F, ϕ_q), and choose a basis $B = \{b_1, \ldots, b_m\}$. Let, further, $x \in M$ be an arbitrary vector. By semi-linearity, $\Phi_q(x)$ is already determined by the images of the basis vectors.

Definition 2.1. The matrix whose jth column equals the coefficient vector of $\Phi_q(b_j)$ with respect to B is the *representing matrix* D of Φ_q with respect to the basis B.

Thus, $D = (d_{ij})_{i,j \in \{1,\ldots,m\}}$, where $\Phi_q(b_j) = \sum_{i=1}^m d_{ij} b_i$. To see how

the representing matrix of a semilinear map behaves under a change of basis, let B' be a second basis. The coordinate vectors of x with respect to the two bases are related by $x_{B'} = C^{-1}x_B$, where $C \in \mathrm{GL}_m(F)$, is the matrix describing the base change. Therefore, the representing matrix of Φ_q with respect to the basis B' is $C^{-1}D\phi_q(C)$. We call the matrices D and $C^{-1}D\phi_q(C)$ *Frobenius equivalent*. Note that Frobenius equivalent matrices define the same solution field. We consider a fixed basis B and all coordinates and representing matrices are chosen with respect to B. Let E be a solution field of M. We call a basis of the solution space $\mathrm{Sol}^{\Phi_q}(M)$ a *fundamental system of solutions*. A matrix $Y \in \mathrm{GL}_m(E)$ whose columns collect the coordinates of such a fundamental system is called *fundamental solution matrix*. It is characterized by the condition $D\phi_E^q(Y) = Y$.

Proposition 2.2. *The Galois group* $\mathrm{Gal}^{\Phi_q}(M)$ *of a finite Frobenius module* (M, Φ_q) *of dimension* m *is isomorphic to a subgroup of* $\mathrm{GL}_m(\mathbb{F}_q)$.

Proof. See [**9,** Corollary 4.2]. □

2.1. Bounds for the Galois group. We have seen that it is possible to interpret the Galois group $\mathrm{Gal}^{\Phi_q}(M)$ of M as a subgroup of the general linear group $\mathrm{GL}_m(\mathbb{F}_q)$. We now construct bounds for this group.

Theorem 2.3 (Matzat)**.** *Let* (M, Φ_q) *be a Frobenius module over a Frobenius field* (F, ϕ_q). *Let* $\mathcal{G}$ *be a reduced connected linear algebraic group defined over* $\mathbb{F}_q$. *Assume that there exists a basis* B *such that* $D_B(\Phi_q) \in \mathcal{G}(F)$. *Then* $\mathrm{Gal}^{\Phi_q}(M) \subseteq \mathcal{G}(\mathbb{F}_q)$.

Proof. See [**9,** Theorem 4.3.]. □

After receiving a criterion for upper bounds of $\mathrm{Gal}^{\Phi_q}(M)$, we now want to obtain lower bounds.

Theorem 2.4 (Matzat)**.** *Let* (M, Φ_q) *be a finite Frobenius module of dimension* m *over a valued field* (F, ϕ_q) *with* $F \geq \mathbb{F}_q$. *Let* $\mathcal{O}_\mathcal{Q} \leq F$ *be a valuation ring with valuation ideal* $\mathcal{P}_\mathcal{Q}$ *and with residue field* $F_\mathcal{Q} := \mathcal{O}_\mathcal{Q}/\mathcal{P}_\mathcal{Q} \leq \overline{\mathbb{F}}_q$, *and set* $f_\mathcal{Q} := [F_\mathcal{Q} : \mathbb{F}_q]$. *Assume that* $D = D_B(\Phi_q)$ *belongs to* $\mathrm{GL}_m(\mathcal{O}_\mathcal{Q})$ *with residue matrix* $\mathcal{D}_\mathcal{Q} \in \mathrm{GL}_m(F_\mathcal{Q})$. *Then*

$\mathrm{Gal}^{\Phi_q}(M) \leq \mathrm{GL}_m(\mathbb{F}_q)$ *contains a matrix* $C_{\mathcal{Q}}$ *in* $\mathrm{GL}_m(\overline{\mathbb{F}}_q)$ *conjugate to*

$$\langle \widehat{D} \rangle_{\mathcal{Q}} := D_{\mathcal{Q}} \phi_q(D_{\mathcal{Q}}) \cdots \phi_q^{f-1}(D_{\mathcal{Q}}).$$

Proof. See [**9,** Theorem 4.5]. □

We apply Theorem 2.4 to the situation where $q = p^1$ and $F = \mathbb{F}_p(t_1, \ldots, t_r)$ is a rational function field over $\mathbb{F}_p$ in several variables t_i which we are going to specialize to suitable elements $a_i \in \mathbb{F}_p$ to get a matrix $\widetilde{D}$ belonging to a prescribed conjugacy class. Let $R = \mathbb{F}_p[t_1, \ldots, t_r]$, and let $\mathfrak{p} = (t_1 - a_1, \ldots, t_r - a_r)$ be the maximal ideal of R corresponding to the planned specializations. We define $\chi : R \to \mathbb{F}_p$ to be the specialization homomorphism sending t_i to $a_i \in \mathbb{F}_p$.

Corollary 2.5. *Let* (M, Φ_p) *be a Frobenius module over the rational function field* $F = \mathbb{F}_p(t_1, \ldots, t_r)$ *and* $D = D_B(\Phi_p) \in \mathrm{GL}_m(R_{\mathfrak{p}})$ *the representing matrix of* Φ_p *with respect to a basis* B *of* M*. Let* χ *denote the specialization homomorphism mapping* t_i *to* a_i *for all* $i = 1, \ldots, r$*, where* $a_1, \ldots, a_r$ *are arbitrary elements of* $\mathbb{F}_p$*. Then:*

(i) $\mathrm{Gal}^{\Phi_p}(M)$ *contains a matrix* $C_{\mathcal{Q}} \in \mathrm{GL}_m(\mathbb{F}_p)$ *which inside* $\mathrm{GL}_m(\overline{\mathbb{F}}_p)$ *is conjugate to the specialized matrix* $\chi(D) \in \mathrm{GL}_m(\mathbb{F}_p)$.

(ii) *If, furthermore,* $D \in \mathcal{G}(R_{\mathfrak{p}})$ *for a connected linear algebraic group* $\mathcal{G}$*, defined over* $\mathbb{F}_p$*,* $\mathrm{Gal}^{\Phi_p}(M)$ *contains an element which inside* $\mathcal{G}(\overline{\mathbb{F}}_p)$ *is conjugate to* $\chi(D) \in \mathrm{GL}_m(\mathbb{F}_p)$.

Proof. The homomorphism χ has a natural extension to a homomorphism from $\mathrm{GL}_m(R)$ to $\mathrm{GL}_m(\mathbb{F}_p)$. By Chevalley's extension theorem ([**6,** Theorem 3.1.1]) there exists a valuation ring $\mathcal{O}_{\mathcal{Q}}$ of F with maximal ideal $\mathcal{P}_{\mathcal{Q}}$ such that $R \subseteq \mathcal{O}_{\mathcal{Q}}$ and $\mathcal{P}_{\mathcal{Q}} \cap R = \mathfrak{p}$. The residue field $F_{\mathcal{Q}} = \mathcal{O}_{\mathcal{Q}}/\mathcal{P}_{\mathcal{Q}}$ equals $\mathbb{F}_p$; therefore, $f_{\mathcal{Q}} = 1$. Hence, the statements of Corollary 2.5 follow directly from the theorem. □

2.2. Cyclic Frobenius modules.

Definition 2.6. Let (M, Φ_q) be a Frobenius module of dimension m over a Frobenius field (F, ϕ_q). We call M *cyclic*, if it possesses a Φ_q-

cyclic basis, i.e., an element $b \in M$ such that $\{b, \Phi_q(b), \dots, \Phi_q^{m-1}(b)\}$ forms a basis of M.

An important result on cyclic Frobenius modules is:

Theorem 2.7 (Matzat)**.** *Let (F, ϕ_q) be a finite Frobenius field and (M, Φ_q) a Frobenius module over F with $\dim_F(M) = m$. Assume F contains more than $\binom{q^m}{2}$ elements. Then M is cyclic.*

A proof of Theorem 2.7 can be found in [**9,** Theorem 2.1]. For our purposes, we only need the following weaker result.

Proposition 2.8. *Let F, M be as above. Assume F contains more than $\binom{q^m}{2}$ elements. The Buchberger algorithm (see* [**5**]*) leads from the defining matrix equation of a solution field E of (M, Φ_q) to a monic separable and additive polynomial $f(X) \in F(X)$ of degree q^m.*

Proof. Let E/F be a solution field of M and

$$x = B\boldsymbol{y} = \sum_{i=1}^{m} b_i y_i \in \mathrm{Sol}_E^{\Phi}(M), \quad \text{i.e., } \boldsymbol{y} = D\phi_q(\boldsymbol{y}) = D\boldsymbol{y}^q.$$

We apply the Buchberger algorithm with the variables $y_1, \dots, y_{m-1}, z$ in lexicographic ordering. Since F possesses more than $\binom{q^m}{2}$ elements, there exists an F-linear combination $z = \sum_{i=1}^{m} c_i y_i$, where $c_m = 1$, such that z is a cyclic element. Thus, the algorithm leads to a polynomial equation $f(z) = 0$ where $f(X) = \sum_{i=0}^{m} a_i X^{q^i} \in F[X]$ is monic separable and additive of degree q^m, as claimed. □

Note that, in the present work, we consider (infinite) function fields of the form $\mathbb{F}_p(\boldsymbol{t})$ implying that the condition of Proposition 2.8 is always fulfilled.

3. Additive polynomials. Let $\mathcal{G}(\mathbb{F}_q)$ be one of the finite classical groups defined over $\mathbb{F}_q$. The aim of this work is to realize $\mathcal{G}(\mathbb{F}_q)$ as a Galois group of Frobenius modules defined over the smaller ground field $\mathbb{F}_p$, respectively, as a Galois group over a rational function field of the form $\mathbb{F}_p(t_1, \dots, t_m)$ over $\mathbb{F}_p$. Firstly, we introduce the notion

of *additive polynomials*. We consider polynomials of the special shape $f(T) = \sum_{i=0}^{n} a_i T^{p^i}$ with $a_i \in F \geq \mathbb{F}_p$. Precisely, all non-vanishing terms have as an exponent a power of p. Consequently, the sum of two roots of f is again a root, since we are working over a finite field F containing $\mathbb{F}_p$. Hence, we call these *additive* polynomials. Further, any $\mathbb{F}_p$-scalar multiple of a root is again a root. This yields: Let $V(f)$ denote the set containing all roots of f; then $V(f)$ forms a $\mathbb{F}_p$-vector space in the algebraic closure $\overline{F}$. This is why these polynomials sometimes are called "vectorial." We consider the Galois group $\mathrm{Gal}\,(f)$ of an additive (vectorial) polynomial f. It acts on the set of roots $V(f)$ by permuting the roots. However, since every element of the Galois group is an automorphism of the splitting field of f, and since $\mathrm{Gal}\,(f)$ restricted on $F \geq \mathbb{F}_p$ is the identity map, it turns out that $\mathrm{Gal}\,(f)$ acts as a group of $\mathbb{F}_p$-linear transformations on $V(f)$. Therefore, the Galois group of an additive polynomial is represented as a linear group. The finite groups of Lie type are linear groups. Hence, additive polynomials become very useful in the realization of the these groups as Galois groups.

Remark 3.1. For a given additive polynomial f, it is possible to construct a Frobenius module (M, Φ) over F such that

$$\mathrm{Gal}^{\Phi}(M) = \mathrm{Gal}\,(f).$$

Proof. Let $f = \sum_{i=0}^{n} a_i X^i$ where $a_i = 0$ for all i which are not powers of p. Let (M, Φ) be the Frobenius module over F such that representing matrix of Φ is the companion matrix of f. Then, by the defining equation for the solution field of M, the following holds:

$$V(f) = \mathrm{Sol}^{\Phi}(M).$$

This implies $\mathrm{Gal}^{\Phi}(M) = \mathrm{Gal}\,(f)$. □

4. Strong generating sets. Each finite classical group $\mathcal{G}(\mathbb{F}_q)$ is generated by a pair of regular semisimple elements $\{\Gamma_1, \Gamma_2\}$, which is proven in [**11**]. The only important properties of Γ_1 and Γ_2 are regularity and that they lie in finite maximal tori of $\mathcal{G}$ with certain prescribed orders. The essential fact for our application is that both of these properties are invariant under conjugation.

Definition 4.1. Let $\mathcal{G}$ be a reduced connected linear algebraic group and $G = \mathcal{G}(\mathbb{F}_q)$. Let $\{\Gamma_1, \ldots, \Gamma_k\}$ be a set of elements that generates G. Suppose any set

$$\left\{\widetilde{\Gamma}_1, \ldots, \widetilde{\Gamma}_k \mid \widetilde{\Gamma}_i \in G \text{ is a } \mathrm{GL}_n(\mathbb{F}_q)\text{-conjugate of } \Gamma_i \text{ for } i = 1, \ldots, k\right\}$$

generates the whole group G, as well. Then we call $\{\Gamma_1, \ldots, \Gamma_k\}$ a *strong generating set.*

Remark 4.2. Each finite classical group $\mathcal{G}(\mathbb{F}_q)$ is generated by a strong generating pair $\{\Gamma_1, \Gamma_2\}$.

Proof. Based on the results in **[11]** a generating pair of each group is explicitly constructed in **[3]**. □

5. The cross section. In order to apply Corollary 2.5 to the groups of interest, we need to construct a Frobenius module (M, Φ), whose representing matrix can be specialized to a strong generating set for the respective group. We present an important tool for obtaining these.

Let $\mathcal{G}$ be a connected semisimple linear algebraic group. Steinberg presented a construction of a (closed, irreducible) system of representatives of the regular conjugacy classes of $\mathcal{G}$ (see **[14]**) which he calls "cross section" (of the regular classes) of $\mathcal{G}$. It is isomorphic to affine k-space and thus can be parametrized by k variables. The cross section is given as the product of certain root subgroups and Weyl representatives corresponding to a system of simple roots of $\mathcal{G}$, and its construction reveals how to set up an explicit parametrization. From this, we derive for each classical group a "generic matrix model" (with a suitable number of indeterminates) for the elements in the cross section. Specializing the indeterminates to elements of $\mathbb{F}_q$ yields matrices over $\mathbb{F}_q$, that generate the finite classical group $G = \mathcal{G}(\mathbb{F}_q)$ with various different specializations of the indeterminates to $\mathbb{F}_q$. The construction of the cross section matrices is described in Theorem 5.1.

Theorem 5.1 (Steinberg)**.** *Let $\mathcal{G}$ be a reduced connected semisimple linear algebraic group of rank r. Let $\mathcal{T}$ be a maximal torus in $\mathcal{G}$ and $\{\alpha_i \mid 1 \le i \le r\}$ a system of simple roots relative to $\mathcal{T}$. For each i, let $\mathcal{X}_i$ be the root subgroup corresponding to the root α_i, and let w_i be a*

Weyl group representative corresponding to α_i. Let

$$\mathcal{N} = \prod_{i=1}^{r} (\mathcal{X}_i w_i) = \mathcal{X}_1 w_1 \mathcal{X}_2 w_2 \cdots \mathcal{X}_r w_r.$$

Then $\mathcal{N}$ is a cross section of the collection of regular conjugacy classes of $\mathcal{G}$.

Proof. See [**14, 13,** Appendix 1]. □

Remark 5.2. The cross section matrices for all groups of our interest can be found in [**3**].

6. Restriction of the ground field. To be able to apply the criteria for bounds for Galois groups, it is important to find a representation of a group $G = \mathcal{G}(\mathbb{F}_q)$ over $\mathbb{F}_p$. This requires the construction of a homomorphism of groups which maps a classical group $\mathcal{G}(\mathbb{F}_q)$ to the $\mathbb{F}_p$-rational points of a linear algebraic group defined over $\mathbb{F}_p$. The construction presented here is based on the following proposition.

Proposition 6.1.

(i) *Let F be a field and E a finite extension of F. Let $\mathcal{G}$ be a linear algebraic group over E. There exists an affine F-Variety $\Pi\mathcal{G}$ together with a surjective E-morphism $\chi : \Pi\mathcal{G} \to \mathcal{G}$ such that the following holds: for any affine F-variety $\mathcal{Y}$ together with an E-morphism $\phi : \mathcal{Y} \to \mathcal{G}$, there is a unique F-morphism $\pi : \mathcal{Y} \to \Pi\mathcal{G}$ with $\phi = \chi \circ \pi$. The pair $(\Pi\mathcal{G}, \chi)$ is unique up to isomorphism.*

(ii) *$\Pi\mathcal{G}$ is a linear algebraic group over F. The morphism $\chi : \Pi\mathcal{G} \to \mathcal{G}$ is a surjective homomorphism of linear algebraic groups over E, with the following universal property: if $\mathcal{H}$ is a linear algebraic group over F and $\phi : \mathcal{H} \to \mathcal{G}$ a homomorphism of linear algebraic groups over E, there is an unique homomorphism π of linear algebraic groups over F $\pi : \mathcal{H} \to \Pi\mathcal{G}$ such that $\phi = \chi \circ \pi$.*

Proof.

(i) This follows from [**16,** Theorems 11.4.16 and 11.4.20 (1)].

(ii) This is a corollary from [**16,** Proposition 12.4.2]. □

Now we give a somewhat more concrete description of the group $\Pi\mathcal{G}$. Let $\overline{F} > E > F$ denote the algebraic closure of F. $\Pi\mathcal{G}$ is given as the point group $\Pi\mathcal{G}(\overline{F})$. From **[16,** Theorem 11.4.6], we conclude that there exists a bijection of $\Pi\mathcal{G}(\overline{F})$ onto the group $\mathcal{G}(E\otimes_F\overline{F})$ of $(E\otimes_F\overline{F})$-valued points of $\mathcal{G}$. There is a group homomorphism $\Pi\mathcal{G}(\overline{F}) \to \mathcal{G}(E\otimes_F \overline{F})$.

We construct a representation of $\mathcal{G}(E)$ as linear group defined over F. The universal property of Proposition 6.1 (ii) shows that there is a homomorphism (of linear algebraic groups over E) $\mathcal{G} \to \Pi\mathcal{G}$.

Proposition 6.2. *Let $\Pi\mathcal{G}$ be as in Proposition* 6.1. *Assume E/F is Galois.*

(i) *There exists an isomorphism*

$$\rho : \prod_{\sigma\in \mathrm{Gal}(E/F)} \mathcal{G}^\sigma(E) \longrightarrow \Pi\mathcal{G}(E).$$

(ii) *The map $\chi \circ \rho$ is the projection onto the factor defined by $(id) \in \mathrm{Gal}(E/F)$.*

Proof. This is an immediate consequence of **[16,** Proposition 11.4.22] and **[16,** 12.4.5]. □

Corollary 6.3. *Let $E[\mathcal{G}]$ denote the affine algebra of $\mathcal{G}$. The following holds*:

$$E[\Pi\mathcal{G}] \cong \bigotimes_{\sigma\in \mathrm{Gal}(E/F)} E[\mathcal{G}]^\sigma.$$

Remark 6.4. If $\mathcal{G}$ is connected, then so is $\Pi\mathcal{G}$.

Proof. This follows from **[16,** 12.4.7 (3)]. □

Now we construct an explicit monomorphism providing the ground field restriction. For further general information about restriction of the ground field and theoretical details, see **[16,** Chapters 11, 12] and **[12,** Section 4].

We consider the Galois extension $\mathbb{F}_q/\mathbb{F}_p$. Let α be a primitive element of this extension. To construct a homomorphism embedding

$\mathrm{GL}_n(\mathbb{F}_{p^r})$ into $\mathrm{GL}_{rn}(\mathbb{F}_p)$, in fact a map ψ describing the embedding

$$\begin{aligned}\mathrm{GL}_n(\mathbb{F}_{p^r}) &= \{\phi \in \mathrm{Aut}(\mathbb{F}_{p^r}^n) \,|\, \det(\phi) \neq 0\} \overset{\psi}{\hookrightarrow} \{\phi \in \mathrm{Aut}(\mathbb{F}_p^{rn}) \,|\, \det(\phi) \neq 0\} \\ &= \mathrm{GL}_{rn}(\mathbb{F}_p)\end{aligned}$$

must be determined. Let $P(T) \in \mathbb{F}_p[T]$ of degree r be an irreducible polynomial such that α is a root of P. Let $A \in \mathrm{GL}_n(\mathbb{F}_{p^r})$. Due to the fact that α is a primitive element for $\mathbb{F}_{p^r}/\mathbb{F}_p$, we can rewrite A as a sum $A = A_0 + \alpha A_1 + \alpha^2 A_2 + \cdots + \alpha^{r-1} A_{r-1}$, where $A_0, A_1, A_2, \ldots, A_{r-1}$ are matrices with entries in $\mathbb{F}_p$.

For $\mathbb{F}_{p^r}^n$, there is a $\mathbb{F}_{p^r}$-basis $(e_1, e_2, \ldots, e_n)$ and, since $\mathbb{F}_{p^r} = \mathbb{F}_p(\alpha)$ for $\mathbb{F}_p^{rn}$, there is a $\mathbb{F}_p$-basis $(e_1, e_2, \ldots, e_n, \alpha e_1, \alpha e_2, \ldots, \alpha e_n, \ldots, \alpha^{r-1} e_1, \ldots, \alpha^{r-1} e_n)$, depending on the primitive element α or, respectively, the irreducible polynomial P.

We consider the map given by A and the images of the basis elements of the "enlarged" basis; thus, the $n \times n$-matrix $A \in \mathrm{GL}_n(\mathbb{F}_{p^r})$ is identified with a matrix in $\mathrm{GL}_{rn}(\mathbb{F}_p)$, which we denote by $\psi(A)$. In this way, an injective map $\psi : \mathrm{GL}_n(\mathbb{F}_{p^r}) \to \mathrm{GL}_{rn}(\mathbb{F}_p)$ is defined.

Remark 6.5. The map ψ defined as above is a homomorphism of groups.

Corollary 6.6. *Let $\mathcal{G}$ be a subgroup of GL_n. Then $\psi(\mathcal{G}(\mathbb{F}_{p^r}))$ is a subgroup of $\mathrm{GL}_{rn}(\mathbb{F}_p)$ which is isomorphic to $\mathcal{G}(\mathbb{F}_{p^r})$.*

Proposition 6.7. *If $\mathcal{G} = \mathrm{GL}_n$ and $E/F = \mathbb{F}_{p^r}/\mathbb{F}_p$ in Proposition 6.1, then $\Pi\mathcal{G}(F)$ is isomorphic to $\psi(\mathcal{G}(E)) =: \mathcal{H}(F) \subset \mathrm{GL}_{rn}(F)$.*

Proof. Let $H := \psi(\mathcal{G}(\mathbb{F}_{p^r}))$ be the group obtained from the ground field restriction, and let $\mathcal{H}$ be the constant group scheme for this group $H = \mathcal{H}(\mathbb{F}_p)$; hence, there is an injective homomorphism $\phi : \mathcal{H} \to \mathcal{G}$ of linear algebraic groups over E. If χ denotes the homomorphism (of linear algebraic groups over E) $\chi : \Pi\mathcal{G} \to \mathcal{G}$, then by Proposition 6.1, there is a unique homomorphism π of linear algebraic groups over F, $\pi : \mathcal{H} \to \Pi\mathcal{G}$, such that $\phi = \chi \circ \pi$.

We consider the corresponding homomorphism of abstract groups

$$\mathcal{H}(F) \xrightarrow{\tilde{\pi}} \Pi\mathcal{G}(F) \xrightarrow{\tilde{\chi}} \mathcal{G}(E),$$

where $\widetilde{\chi}\circ\widetilde{\pi} = \psi^{-1}$. Now let $\Pi\mathcal{G}/\mathrm{Gal}\,(E/F)$ denote the set of $\mathrm{Gal}\,(E/F)$-orbits on $\Pi\mathcal{G}(E)$. Then $\Pi\mathcal{G}(F) = \Pi\mathcal{G}(E)/\mathrm{Gal}\,(E/F)$ and, by Proposition 6.2, we have

$$\Pi\mathcal{G}(F) \cong \mathcal{G}(E).$$

The fact that $\widetilde{\chi}$ and $\widetilde{\chi}\circ\widetilde{\pi}$ are isomorphisms implies $\Pi\mathcal{G}(F) \cong \mathcal{H}(F) \subset \mathrm{GL}_{rn}(F)$. □

Proposition 6.8. *Let $A \in \mathrm{GL}_n(\mathbb{F}_{p^r})$ with characteristic polynomial $g_A(T)$. Then*

$$g_{\psi(A)}(T) = \prod_{\sigma\in\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)} g_{A^\sigma}(T).$$

Proof. Let $\mathrm{Gal}\,(\mathbb{F}_{p^r}/\mathbb{F}_p) = \{\sigma_1,\dots,\sigma_r\}$. For all $A \in \mathrm{GL}_n(\mathbb{F}_{p^r})$, there exists a base change matrix $S \in \mathrm{GL}_{rn}(\mathbb{F}_{p^r})$, so that $S\cdot\psi(A)\cdot S^{-1} = \mathrm{diag}\,(\sigma_1(A),\dots,\sigma_r(A))$ holds. (The base change over $\mathbb{F}_{p^r}$ does not depend on A and can be written down explicitly from the construction above). Therefore, the statement follows directly from Proposition 6.2, because the characteristic polynomial is invariant under constant extensions and under change of basis. □

7. Finite groups of Lie type as Galois groups over $\mathbb{F}_p(t)$. Let $q = p^r$ be a prime power. For a group $G = \mathcal{G}(\mathbb{F}_q)$, let $H = \mathcal{H}(\mathbb{F}_p) := \psi(\mathcal{G}(\mathbb{F}_q))$.

Remark 7.1. If $\{\Gamma_1,\Gamma_2\}$ is a strong generating pair of $G = \mathcal{G}(\mathbb{F}_q)$, then every pair of elements of $\mathcal{H}(\mathbb{F}_p)$ which are $\psi(\mathrm{GL}_n(\mathbb{F}_q))$-conjugates of $\{\psi(\Gamma_1),\psi(\Gamma_2)\}$ generates $\mathcal{H}(\mathbb{F}_p)$.

Proof. The map $\psi|_{\mathcal{G}(\mathbb{F}_q)}$ is an isomorphism and does not change conjugacy classes. □

Now let $\mathcal{G}(\mathbb{F}_q)$ be one of the groups $\mathrm{SL}_n(\mathbb{F}_q)$, $\mathrm{Sp}_{2n}(\mathbb{F}_q)$, $\mathrm{SO}_{2k+1}(\mathbb{F}_q)$, $\mathrm{SO}^+_{2k}(\mathbb{F}_q)$ (for odd q, $k\geq 2$, $(q,2k)\neq(3,4)$), $\mathrm{SU}_n(\mathbb{F}_q)$ (for $n\geq 3$ and $(n,q)\neq(3,2)$), $\mathrm{SO}^-_{2k}(\mathbb{F}_q)$ (for odd q), ${}^2\mathrm{B}_2(\mathbb{F}_q)$ (for $q = 2^{2m+1}, m\geq 0$), $\mathrm{G}_2(\mathbb{F}_q)$, ${}^2\mathrm{G}_2(\mathbb{F}_q)$ (for $q = 3^{2m+1}, m\geq 0$), ${}^3\mathrm{D}_4(\mathbb{F}_q)$. By choosing a suitable variant of the cross section as representing matrix of a Frobenius module, Albert and Maier realized these groups as Galois groups over fields of the form $\mathbb{F}_q(\mathbf{t})$. Let $C_{\mathcal{G}} \in \mathcal{G}(\mathbb{F}_q(\mathbf{t}))$ denote the

respective representing matrix in [**3**]. This matrix is called "cross section matrix." For example, the cross section matrix for SL_n contains $k = n - 1$ indeterminates and is given by

$$C_{\mathrm{SL}_n} = \begin{pmatrix} -t_1 & \cdots & -t_k & 1 \\ -1 & & & \\ & \ddots & & \\ & & -1 & 0 \end{pmatrix}.$$

Our purpose is to find a suitable matrix in $\mathcal{H}(\mathbb{F}_p(\mathbf{t}))$, which allows for the right specializations (over $\mathbb{F}_p$). Therefore, we choose a primitive element α for the extension $\mathbb{F}_{p^r}/\mathbb{F}_p$ and modify $C_{\mathcal{G}}$ by transforming all indeterminates t_i to $t_i^* = \sum_{j=0}^{r-1} t_{i,j}\alpha^j$ for all $i \in \{1, \ldots, k\}$. The matrix obtained by this transformation is called "modified cross section matrix" for $\mathcal{G}$ and denoted by $D_{\mathcal{G}}$.

Theorem 7.2. *Let (M, Φ_p) be the Frobenius module over $F = \mathbb{F}_p(\boldsymbol{t})$ such that the representing matrix of Φ_p equals $D_B(\Phi_p) = \psi(D_{\mathcal{G}})$ with respect to some basis B. Then*

$$\mathrm{Gal}^{\Phi_p}(M) \cong \mathcal{G}(\mathbb{F}_{p^r}).$$

Proof. The cross section matrix of the group $\mathcal{G}(\mathbb{F}_q(\boldsymbol{t}))$ naturally belongs to $\mathcal{G}(\mathbb{F}_q(\boldsymbol{t}))$. Of course, the modified cross section matrix belongs to $\mathcal{G}(\mathbb{F}_q(\boldsymbol{t}))$, too. By Proposition 6.7, it holds that $\mathcal{H}(\mathbb{F}_p) \cong (\Pi\mathcal{G})(\mathbb{F}_p)$, where $\Pi\mathcal{G}$ is the variety defined in Proposition 6.1. The isomorphism can be treated as basis change; thus, there is a basis $\widetilde{B}$ such that $D_{\widetilde{B}}(\Phi) \in (\Pi\mathcal{G})(\mathbb{F}_p)$. Since $(\Pi\mathcal{G})$ is connected by Remark 6.4, by Theorem 2.3 the Galois group of the Frobenius module defined by $\psi(D)$ as representing matrix is contained in the group $(\Pi\mathcal{G})(\mathbb{F}_p)$. Thus, we have

$$\mathrm{Gal}^{\Phi}(M) \subseteq (\Pi\mathcal{G})(\mathbb{F}_p) \cong \mathcal{H}(\mathbb{F}_p) \cong \mathcal{G}(\mathbb{F}_q).$$

We consider a strong generating pair $\{\Gamma_i, i = 1, 2\}$ of the group $G = \mathcal{G}(\mathbb{F}_{p^r})$. Let $\Gamma_i \in \{\Gamma_1, \Gamma_2\}$. In [**3**] it is proven that there is a specialization homomorphism which maps the indeterminates t_i^* in the cross section matrix to elements $a_i^* \in \mathbb{F}_q$ for all $i \in \{1, \ldots, k\}$ satisfying that the matrix A_i obtained by the specialization of $C_{\mathcal{G}}$ and Γ_i have the same characteristic polynomial. (Naturally, the specializations may be different for Γ_1 and Γ_2). We rewrite a_i^* by setting $a_i^* =:$

$\sum_{j=0}^{r-1} a_{i,j}\alpha^j$ with coefficients $a_{i,j} \in \mathbb{F}_p$ for $i \in \{1,\dots,k\}$ and $j \in \{0,\dots,r-1\}$. Now we consider $D_B(\Phi_p) = \psi(D_{\mathcal{G}})$. We define a specialization homomorphism $\chi : t_{i,j} \mapsto a_{i,j}$ for all $i \in \{1,\dots,k\}$ and $j \in \{0,\dots,r-1\}$. Hence, $\psi(A_i)$ is a specialization (over $\mathbb{F}_p$) of $D_B(\Phi_p)$. By the lower bound theorem (Corollary 2.5), the Galois group of the Frobenius module with representing matrix $D_B(\Phi)$ contains $\psi(\mathrm{GL}_n(\overline{\mathbb{F}}_q))$-conjugates of $\psi(A_1)$ and $\psi(A_2)$. From **[11]**, it is known that Γ_i is diagonalizable (over the algebraic closure $\overline{\mathbb{F}}_q$) and has pairwise distinct eigenvalues; hence, A_i is diagonalizable, too, with the same Jordan normal form. Therefore, A_i is conjugate to Γ_i in $\mathrm{GL}_n(\overline{\mathbb{F}}_{p^r})$. By **[7,** Corollary 6.7.1], A_i is also conjugate to Γ_i in $\mathrm{GL}_n(\mathbb{F}_{p^r})$. Hence, there is an $S_i \in \mathrm{GL}_n(\mathbb{F}_{p^r})$, so that $S_i \cdot A_i \cdot S_i^{-1} = \Gamma_i$. Thus,

$$\psi(\Gamma_i) = \psi(S_i \cdot A_i \cdot S_i^{-1}) = \psi(S_i) \cdot \psi(A_i) \cdot \psi(S_i)^{-1},$$

implying that $\psi(A_i)$ and $\psi(\Gamma_i)$ are conjugate in $\psi(\mathrm{GL}_n(\mathbb{F}_q))$. By Remark 7.1, $\psi(A_1)$ and $\psi(A_2)$ generate $\mathcal{H}(\mathbb{F}_p)$. Hence,

$$\mathcal{H}(\mathbb{F}_p) \subseteq \mathrm{Gal}^{\Phi}(M). \qquad \square$$

Theorem 7.3. *It is possible to transform the defining equation $\psi(D_{\mathcal{G}}) \cdot v^p = v$ for a vector $v \in M$ to an additive polynomial f depending on only one indeterminate. The solution field of M is generated by the roots of f, in particular,*

$$\mathrm{Gal}^{\Phi_p}(f) \cong \mathcal{G}(\mathbb{F}_{p^r}).$$

Proof. We recall the defining equation $\psi(D_{\mathcal{G}}) \cdot v^p = v$ of a solution field E of (M, Φ_p). In particular, it is a system of equations. Since F possesses more than $\binom{p^{rn}}{2}$ elements, the condition of Proposition 2.8 is fulfilled. Thus, by eliminating variables using Buchberger's algorithm, the equation can be solved recursively (possibly using a transformation of indeterminates as described in the proof of Proposition 2.8). This leads to a single polynomial f whose splitting field coincides with the solution field E. Since the Galois group of M is defined as $\mathrm{Gal}\,(E/F)$, it equals the Galois group of f. $\square$

8. Explicit polynomials. By Theorem 7.3, we are finally able to compute explicit polynomials in $\mathbb{F}_p(\underline{t})[Y]$, whose Galois groups are finite groups of Lie type defined over $\mathbb{F}_{p^r}$.

Let $D_{\mathcal{G}}$ be the respective modified cross section matrix. Let F be a function field over $\mathbb{F}_p$, and let (M, Φ_p) be the Frobenius module over F. Let $D = D_B(\Phi_p) := \psi(D_{\mathcal{G}})$ be the representing matrix of its Frobenius endomorphism Φ_p (with respect to some basis). The fundamental equation to be solved is $Dv^p = v$ for a vector $v \in M$. In fact, this is a system of equations which can be solved recursively using Buchberger's algorithm.

Explicit polynomials for SL_n**.** Let $\mathcal{G}(\mathbb{F}_q) = \mathrm{SL}_n(\mathbb{F}_q)$, $k = n-1$, $q = p^2 = 4$. Set $t_{i,0} =: -s_i, t_{i,1} =: -t_i$ for all i. Then, for a vector $x = (x_1, \ldots, x_n, y_1, \ldots, y_n) \in M$, the fundamental equation $\psi(D_{\mathrm{SL}_n})v^p = v$ leads to the equation system:

$$\left(\begin{array}{cccc|ccccc} s_1 & \ldots & s_k & 1 & t_1 & \cdots & t_k & 0 \\ -1 & & & & & & & \\ & \ddots & & & & & & \\ & & -1 & 0 & & & & \\ \hline t_1 & \cdots & t_k & 0 & s_1+t_1 & \cdots & s_k+t_k & 1 \\ & & & & -1 & & & \\ & & & & & \ddots & & \\ & & & & & & -1 & 0 \end{array}\right) \cdot \begin{pmatrix} x_1^p \\ \vdots \\ \vdots \\ x_n^p \\ y_1^p \\ \vdots \\ \vdots \\ y_n^p \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ \vdots \\ x_n \\ y_1 \\ \vdots \\ \vdots \\ y_n \end{pmatrix}.$$

Example 8.1. Let

$$f(Y) = Y^{16} + (s_1^4 + t_1^4 + s_1^2 t_1^2) \cdot Y^8 + (t_1^6 + s_1^2 t_1^4 + t_1^3 + 1 + s_1^4 t_1^2) \cdot Y^4 + (s_1 t_1^3 + t_1^4 + s_1^2 t_1^2) \cdot Y^2 + t_1^3 \cdot Y.$$

Then, $\mathrm{Gal}_{\mathbb{F}_2(t_1,s_1)}(f) \cong \mathrm{SL}_2(\mathbb{F}_{2^2}) \cong \mathrm{Sp}_2(\mathbb{F}_{2^2})$.

Example 8.2. Let

$$\begin{aligned} f(Y) = {} & Y^{2^6} + (t_1^4 s_2^2 + t_1^2 t_2^2 s_1^2 + t_1 t_2^3 + t_2^8 + t_2^4 s_2^4 + s_2^8) \cdot Y^{2^5} \\ & + (t_1^8 + t_1^6 s_1^2 + t_1^5 t_2 + t_1^4 t_2^4 s_2^2 + t_1^4 s_2^6 + t_1^2 t_1^6 s_1^2 + t_1^2 t_2^4 s_1^2 s_2^2 \\ & + t_1^2 t_2^2 s_1^2 s_2^4 + t_1 t_2^7 + t_1 t_2^5 s_2^2 + t_1 t_2^3 s_2^4 + t_2^{12} + t_2^8 s_2^4 + t_2^6 s_1^4 + t_2^4 s_2^8 + s_1^8) \\ & \cdot Y^{2^4} + (t_1^8 t_2^2 + t_1^8 s_2^2 + t_1^7 + t_1^6 s_1^2 s_2^2 + t_1^5 t_2 s_2^2 + t_1^4 t_2^8 + t_1^4 t_2^6 s_2^2 + t_1^4 t_2^4 s_2^4 \\ & + t_1^4 s_1^4 s_2^2 + t_1^3 t_2^4 s_2^2 + t_1^2 t_2^8 s_1^2 + t_1^2 t_2^6 s_1^2 s_2^2 + t_1^2 t_2^4 s_1^2 s_2^4 + t_1^2 t_2^2 s_1^6 + t_1 t_2^9 \end{aligned}$$

$$
\begin{aligned}
&+ t_1t_2^7s_2^2+t_1t_2^6s_1^2+t_1t_2^5s_2^4+t_1t_2^3s_1^4+t_2^8s_1^4+t_2^7+t_2^6s_1^4s_2^2+t_2^4s_1^4s_2^4+1)\\
&\cdot Y^{2^3} + (t_1^{10} + t_1^8s_2^2 + t_1^7s_2 + t_1^6t_2^4s_2^2 + t_1^6s_1^4 + t_1^5t_2s_1^2 + t_1^4t_2^6s_1^2\\
&+ t_1^4t_2^4s_1^2s_2^2 + t_1^4s_2^2 + t_1^3t_2^7 + t_1^3t_2^4s_2^3 + t_1^2t_2^6s_1^4 + t_1^2t_2^4s_1^4s_2^2 + t_1^2t_2^2s_1^2\\
&+ t_1t_2^7s_1^2 + t_1t_2^6s_1^2s_2 + t_1t_2^5s_1^2s_2^2 + t_1t_2^3 + t_2^8 + t_2^7s_2 + t_2^6s_1^6 + t_2^4s_2^4)\\
&\cdot Y^{2^2} + (t_1^8 + t_1^7s_1 + t_1^6s_1^2 + t_1^5t_2 + t_1^4t_2^4s_2^2 + t_1^3t_2^4s_1s_2^2 + t_1^2t_2^6s_1^2\\
&+ t_1^2t_2^4s_1^2s_2^2 + t_1t_2^7 + t_1t_2^6s_1^3 + t_1t_2^5s_2^2 + t_2^7s_1 + t_2^6s_1^4)\cdot Y^2\\
&+ (t_1^7 + t_1^3t_2^4s_2^2 + t_1t_2^6s_1^2 + t_2^7)\cdot Y.
\end{aligned}
$$

Then, $\mathrm{Gal}_{\mathbb{F}_2(t_1,t_2,s_1,s_2)}(f) \cong \mathrm{SL}_3(\mathbb{F}_{2^2})$.

Example 8.3. Let $p > 2$ and $\beta = \alpha^2 \in \mathbb{F}_p$. Let

$$
\begin{aligned}
f(Y) = Y^{p^4} &+ (-s_1^{p^2} - s_1^p t_1^{p(p-1)})\cdot Y^{p^3}\\
&+ (-\beta t_1^{p(p+1)} + t_1^{p^2-1} + 1 + s_1^{2p}t^{p(p-1)})\cdot Y^{p^2}\\
&+ (-s_1 t_1^{p^2-1} - s_1^p t_1^{p(p-1)})\cdot Y^p + t_1^{p^2-1}\cdot Y.
\end{aligned}
$$

Then, $\mathrm{Gal}_{\mathbb{F}_p(t_1,s_1)}(f) \cong \mathrm{SL}_2(\mathbb{F}_{p^2})$.

Acknowledgments. I would like to express my gratitude to all those who provided me the possibility to complete this report. A special appreciation I give to the supervisor of my Diplom thesis, Prof. B.H. Matzat, whose stimulating suggestions and encouragement helped me to coordinate my project.

REFERENCES

1. Shreeram S. Abhyankar and Nicolas F. Inglis, *Galois groups of some vectorial polynomials*, Trans. Math. Soc. **353** (2001), 2941–2969.

2. Shreeram S. Abhyankar and Pradikumar H. Keskar, *Descent principle in modular Galois theory*, Proc. Indian Acad. Sci., Math. Sci. **11** (2001), 139–149.

3. Maximilian Albert and Annette Maier, *Additive polynomials for finite groups of Lie type*, Israel J. Math. **186** (2011), 125–195.

4. Shreeram S. Abhyankar and Ganapathy S. Sundaram, *Galois groups of generalized iterates of generic vectorial polynomials*, Finite Fields Appl. **7** (2001), 92–109.

5. Bruno Buchberger, *Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems*, Aequat. Math. **4** (1970), 374–383.

6. Antonio Engler and Alexander Prestel, *Valued fields*, Springer, Berlin, 2005.

7. Israel Nathan Herstein, *Topics in algebra*, Blaisdell Publishing Company, New York, 1964.

8. Dan Haran and Helmut Völklein, *Galois groups over complete valued fields*, Israel J. Math. **93** (1996), 9–27.

9. B. Heinrich Matzat, *Frobenius modules and Galois groups*, in *Galois theory and modular forms*, Ki-ichiro Hashimoto, ed., Dordrecht: Kluwer, 2004.

10. Gunter Malle and B. Heinrich Matzat, *Inverse Galois theory*, Springer, New York, 1999.

11. Gunter Malle, Jan Saxl and Thomas Weigel, *Generation of classical groups*, Geom. Dedic. **49** (1994), 85–116.

12. Jean Pierre Serre, *Groupes algébriques et corps de classes*, Hermann, Paris, 1959.

13. ———, *Galois cohomology*, Springer, New York, 1997.

14. Robert Steinberg, *Regular elements of semi-simple algebraic groups*, Inst. Haut. Scient. **25** (1965), 49–80.

15. Damian Stichel, *Realization of classical groups as Galois groups over* $\mathbb{F}_p(t)$, Diplom thesis, Heidelberg, 2011.

16. Tonny A. Springer, *Linear algebraic groups*, Birkhäuser, Boston, 1998.

Interdisciplinary Center of Scientific Computing, Im Neuenheimer Feld 368, 69120 Heidelberg, Germany
Email address: **damian.stichel@bioquant.uni-heidelberg.de**