Journal of Algebra 423 (2015) 405–421

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Generic extensions and generic polynomials for multiplicative groups

Jorge Morales[a], Anthony Sanchez[b,1]

[a] Department of Mathematics, Louisiana State University, Baton Rouge, LA 70803, USA
[b] Department of Mathematics, Arizona State University, Tempe, AZ 85281, USA

ARTICLE INFO

Article history:
Received 23 June 2013
Available online 31 October 2014
Communicated by Eva Bayer-Fluckiger

MSC:
12F12
13B05

Keywords:
Constructive Galois theory
Frobenius modules
Generic polynomials
Multiplicative group
Field extensions

ABSTRACT

Let $\mathcal{A}$ be a finite-dimensional algebra over a finite field $\mathbb{F}_q$ and let $G = \mathcal{A}^\times$ be the multiplicative group of $\mathcal{A}$. In this paper, we construct explicitly a generic Galois G-extension S/R, where R is a localized polynomial ring over $\mathbb{F}_q$, and an explicit generic polynomial for G in $\dim_{\mathbb{F}_q}(\mathcal{A})$ parameters.

Contents

E-mail addresses: morales@math.lsu.edu (J. Morales), anthony.sanchez.1@asu.edu (A. Sanchez).

[1] Research conducted at the 2012 Louisiana State University Research Experience for Undergraduates (REU) site supported by the National Science Foundation REU Grant DMS-0648064.

http://dx.doi.org/10.1016/j.jalgebra.2014.06.034
0021-8693/© 2014 Published by Elsevier Inc.

1. Introduction

An important and classical problem in Galois theory is to describe for a field k and a finite group G all Galois extensions M/L with Galois group G, where L is a field containing k. This can be done by means of a *generic polynomial*, that is a polynomial $f(Y; t_1, \dots, t_m)$ with coefficients in the function field $k(t_1, \dots, t_m)$ and Galois group G such that every Galois G-extension M/L, with $L \supset k$, is the splitting field of $f(Y; \xi_1, \dots, \xi_m)$ for a suitable $(\xi_1, \dots, \xi_m) \in L^m$.

A related construction is that of *generic extensions* introduced by Saltman [10]. These are Galois G-extensions of commutative rings S/R, where $R = k[t_1, \dots, t_m, 1/d]$ and d is a nonzero polynomial in $k[t_1, \dots, t_m]$, such that every Galois G-algebra M/L, where L is a field containing k, is of the form $M \simeq S \otimes_\varphi L$ for a suitable homomorphism of k-algebras $\varphi : R \to L$.

Over an infinite ground field k, the existence of generic polynomials is equivalent to the existence of generic extensions as shown by Ledet [8], but the dictionary, at least in the direction {polynomials} $\to$ {extensions}, is not straightforward.

In this paper, we construct explicitly both a generic extension and a generic polynomial for groups of the form $G = \mathcal{A}^\times$, where $\mathcal{A}$ is a finite-dimensional $\mathbb{F}_q$-algebra and k is an infinite field containing $\mathbb{F}_q$. Both constructions are based on the theory of Frobenius modules as developed by Matzat [9]. An important ingredient is Matzat's "lower bound" theorem as formulated in [2, Theorem 3.4] that we use to show that the extensions (respectively, polynomials) we construct have the required Galois group.

The number of parameters in our construction is not optimal. For example, if $\mathcal{A} = M_n(\mathbb{F}_q)$, then our method produces a polynomial in n^2 parameters, as opposed to the standard generic polynomial for $\mathbf{GL}_n(\mathbb{F}_q)$ that needs only n parameters [1], [4, Section 1.1]. However, our method has the advantage of being general for all groups of the form $\mathcal{A}^\times$, where $\mathcal{A}$ is any finite-dimensional algebra over $\mathbb{F}_q$.

We are indebted to the referee for her/his pertinent and useful comments.

2. Frobenius modules

In this section we recall the basic theory and definitions relating to Frobenius modules for convenience of the reader. Most of the material in Sections 2.1–2.3 can be found in [9, Part I], [2]. We include it here for the convenience of the reader.

2.1. Preliminaries

Let K be a field containing the finite field $\mathbb{F}_q$ and let $\overline{K}$ denote an algebraic closure of K.

Definition 1. A *Frobenius module* over K is a pair (M, φ) consisting of a finite-dimensional vector space M over K and an $\mathbb{F}_q$-linear map $\varphi : M \to M$ satisfying

1. $\varphi(ax) = a^q \varphi(x)$ for $a \in K$ and $x \in M$.
2. The natural extension of φ to $M \otimes_K \overline{K} \to M \otimes_K \overline{K}$ is injective.[2]

The *solution space* $\mathrm{Sol}^{\varphi}(M)$ of (M, φ) is the set of fixed points of φ, i.e.

$$\mathrm{Sol}^{\varphi}(M) = \{x \in M \mid \varphi(x) = x\},$$

which is clearly an $\mathbb{F}_q$-subspace of M.

Let $e_1, e_2, \ldots, e_n$ be a K-basis of M. Clearly φ is completely determined by its values on this basis. Write

$$\varphi(e_j) = \sum_{i=1}^{n} a_{ij} e_i,$$

where $a_{ij} \in K$ and let $A = (a_{ij}) \in M_n(K)$. Identifying M with K^n via the choice of this basis, we have

$$\varphi(X) = AX^{(q)},$$

where $X = (x_1, \ldots, x_n)^T$ and $X^{(q)} = (x_1^q, \ldots, x_n^q)^T$. Condition (2) of Definition 1 ensures that A is nonsingular. We shall denote by (K^n, φ_A) the Frobenius module determined by a matrix $A \in \mathbf{GL}_n(K)$.

With the above notation, the solution space $\mathrm{Sol}^{\varphi}(M)$ is identified with the set of solutions in K of the system of polynomial equations

$$AX^{(q)} = X. \tag{1}$$

By the Lang–Steinberg theorem (Theorem 2.5), there is a matrix $U = (u_{ij}) \in \mathbf{GL}_n(\overline{K})$ such that

$$A = U\left(U^{(q)}\right)^{-1}, \tag{2}$$

[2] Note that if K is not perfect, the injectivity of $\varphi : M \to M$ does not imply condition (2) above. For example, if $a \in K \setminus K^q$, the map $\varphi : K^2 \to K^2$ given by $\varphi(x, y) = (x^q - ay^q, 0)$ is injective over K but not over $\overline{K}$.

where $U^{(q)} = (u_{ij}^q)$. Thus, the change of variables $Y = U^{-1}X$ over $\overline{K}$ yields the "trivial" system

$$Y^{(q)} = Y, \tag{3}$$

whose solutions are exactly the vectors in $\mathbb{F}_q^n \subset \overline{K}^n$. We have proved:

Proposition 2.1. *The columns of U form a basis of $\mathrm{Sol}^\varphi(M \otimes_K \overline{K})$ over $\mathbb{F}_q$. In particular*

$$\dim_{\mathbb{F}_q} \mathrm{Sol}^\varphi(M \otimes_K \overline{K}) = n.$$

2.2. Separability

We shall now show that the solutions of (1) are in K_{sep}^n. See [9, Theorem 1.1c] for a different argument.

Proposition 2.2. *Let $A \in \mathbf{GL}_n(K)$ and let $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ be indeterminates. Then the K-algebra*

$$\mathcal{F} = K[\mathbf{X}]/\big\langle A\mathbf{X}^{(q)} - \mathbf{X}\big\rangle,$$

where $\mathbf{X} = [\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n]^T$ and $\langle A\mathbf{X}^{(q)} - \mathbf{X}\rangle$ is the ideal generated by the coordinates of $A\mathbf{X}^{(q)} - \mathbf{X}$, is étale over K.

Proof. Consider the change of variables $\mathbf{Y} = U\mathbf{X}$ over $\overline{K}$, where U is as in (2). Then

$$\begin{aligned} \mathcal{F} \otimes_K \overline{K} &= \overline{K}[\mathbf{Y}]/\big\langle \mathbf{Y}^{(q)} - \mathbf{Y}\big\rangle \\ &\simeq \prod_{\mathbb{F}_q^n} \overline{K}. \qquad \square \end{aligned}$$

Corollary 2.3. *The solutions of the system of polynomial equations $AX^{(q)} = X$ in $\overline{K}^n$ lie in K_{sep}^n. In particular, the matrix U of (2) is in $\mathbf{GL}_n(K_{\mathrm{sep}})$.*

Proof. The solutions of $AX^{(q)} = X$ are exactly the images of $\mathbf{X}$ under K-algebra homomorphisms $\mathcal{F} \to \overline{K}$. Since $\mathcal{F}/K$ is étale, so are all its quotients. This implies that the images of such homomorphisms are contained in K_{sep}. $\square$

Definition 2. The *splitting field* E of (M, φ) is the subfield of K_{sep} generated over K by all the solutions of $AX^{(q)} = X$.

Remark 1. The above definition does not depend on the choice of a basis of M over K.

Corollary 2.4. *The splitting field E of (M, φ) is a finite Galois extension of K generated by the coefficients u_{ij} of the matrix U of (2).*

Proof. The extension E/K is finite, separable by Proposition 2.2. It is normal since a Galois conjugate of a solution X of $AX^{(q)} = X$ is also a solution. Every solution X of $AX^{(q)} = X$ is an $\mathbb{F}_q$-linear combination of the columns of U by Proposition 2.1, thus the coefficients u_{ij} of U generate E over K. □

2.3. The Galois group of a Frobenius module

The Lang–Steinberg theorem (see [6, Theorem 1] and [14, Theorem 10.1]) plays an important role in the theory of Frobenius modules.

Theorem 2.5 *(Lang–Steinberg). Let $\Gamma \subset \mathbf{GL}_n$ be a closed connected algebraic subgroup defined over $\mathbb{F}_q$ and let $A \in \Gamma(K)$. Then there exists $U \in \Gamma(\overline{K})$ such that $U(U^{(q)})^{-1} = A$.*

Remark 2. In fact, the element U given in Theorem 2.5 lies in $\Gamma(K_{\mathrm{sep}})$ as discussed in Corollary 2.3.

Next we state two theorems due to Matzat [9] that play an important role in the determination of the Galois group of a Frobenius module.

Theorem 2.6 *("Upper Bound" Theorem). (See [9, Theorem 4.3].) Let $\Gamma \subset \mathbf{GL}_n$ be a closed connected algebraic subgroup defined over $\mathbb{F}_q$ and let $A \in \Gamma(K)$. Let E/K be the splitting field of the Frobenius module (K^n, φ_A) defined by A and let $U \in \Gamma(E)$ be an element given by the Lang–Steinberg theorem. Then the map*

$$\begin{aligned} \mathrm{Gal}(E/K) &\xrightarrow{\rho} \Gamma(\mathbb{F}_q) \\ \sigma &\longmapsto U^{-1}\sigma(U) \end{aligned}$$

is an injective group homomorphism.

We state next Matzat's "lower bound" theorem in the particular case that we will use. See [2, Theorem 3.4] and ensuing paragraph.

Theorem 2.7 *("Lower Bound" Theorem). Let $K = \mathbb{F}_q(\mathbf{t})$ where $\mathbf{t} = (t_1, \dots, t_m)$ are indeterminates. Let $\Gamma \subset \mathbf{GL}_n$ be a closed connected algebraic subgroup defined over $\mathbb{F}_q$ and let $A \in \Gamma(K)$. Let $\rho : \mathrm{Gal}(E/K) \to \Gamma(\mathbb{F}_q)$ be the homomorphism of Theorem 2.6. Then every specialization of A in $\mathbb{F}_q$ is conjugate in $\Gamma(\overline{\mathbb{F}}_q)$ to an element of $\mathrm{im}(\rho)$.*

2.4. Integrality

In this subsection we discuss integrality properties of the solutions of the system $AX^{(q)} = X$.

Proposition 2.8. *Let R be a Noetherian domain containing $\mathbb{F}_q$ with field of fractions K and let $A \in \mathbf{GL}_n(R)$. Then the solutions of the system $AX^{(q)} = X$ have coordinates that are integral over R.*

Proof. Define recursively $B_0 = I$, $B_k = (A^{-1})^{(q^{k-1})} B_{k-1}$ for $k \geq 1$. Let N_k be the R-submodule of $M_n(R)$ generated by $B_0, B_1, \dots, B_k$. Since R is Noetherian, the ascending chain of submodules $\{N_k\}$ stabilizes, that is $N_{k-1} = N_k$ for k large enough. For such a k we have

$$B_k = \sum_{j=0}^{k-1} c_j B_j,$$

where $c_j \in R$. Let $X \in K_{\mathrm{sep}}^n$ be such that $AX^{(q)} = X$. It follows from the definition of the B_j's that $X^{(q^j)} = B_j X$, thus

$$X^{(q^k)} = \sum_{j=0}^{k-1} c_j X^{(q^j)},$$

which shows that the coordinates of X are roots of the monic additive polynomial with coefficients in R

$$T^{q^k} - \sum_{j=0}^{k-1} c_j T^{q^j}. \qquad \square$$

Proposition 2.9. *Let R be a Noetherian integrally closed domain containing $\mathbb{F}_q$ with field of fractions K and let $A \in \mathbf{GL}_n(R)$. Let $U \in \mathbf{GL}_n(K_{\mathrm{sep}})$ be such that $A = U(U^{(q)})^{-1}$ and let $S = R[U]$ be the ring generated by the coefficients of U over R. Then the ring extension S/R is Galois with Galois group $G = \mathrm{Gal}(E/K)$, where $E = K[U]$.*

Proof. Let $\rho : G \to \mathbf{GL}_n(\mathbb{F}_q)$ be the homomorphism $\rho(\sigma) = U^{-1}\sigma(U)$ of Theorem 2.6. Then $\sigma(U) = U\rho(\sigma)$, so $S = R[U]$ is preserved by G. By Proposition 2.8, the ring S is integral over R and, since R is assumed to be integrally closed, we must have $S^G = R$. It remains to show that S/R is unramified at maximal ideals.

Let $\mathfrak{m} \subset S$ be a maximal ideal and let $\mathfrak{m}_0 = R \cap \mathfrak{m}$. Let $\ell = S/\mathfrak{m}$ and $k = R/\mathfrak{m}_0$. Notice that since S/R is integral, the ideal $\mathfrak{m}_0$ is also maximal [3, Corollary 5.8]. Clearly $\ell = k[\overline{U}]$ is the splitting field of the system $\overline{A}\mathbf{X}^{(q)} = \mathbf{X}$ over k, where $\overline{A}$ is the class of A modulo $\mathfrak{m}_0$. Hence ℓ/k is Galois. Let $G_\mathfrak{m} \subset G$ be the stabilizer of $\mathfrak{m}$. Each $\sigma \in G_\mathfrak{m}$ induces an automorphism $\overline{\sigma}$ of ℓ/k; we have a canonical homomorphism

$$\begin{aligned} G_\mathfrak{m} &\xrightarrow{\pi} \mathrm{Gal}(\ell/k) \\ \sigma &\longmapsto \overline{\sigma}. \end{aligned}$$

We need to verify that the map π above is injective. Indeed, let $\bar{\rho} : \mathrm{Gal}(\ell/k) \to \mathbf{GL}_n(\mathbb{F}_q)$ be the map given by $\bar{\rho}(\tau) = \overline{U}^{-1}\tau(\overline{U})$. We verify immediately that the following diagram is commutative

$$\begin{tikzcd} G_{\mathfrak{m}} \arrow[r, "\rho"] \arrow[d, "\pi"'] & \mathbf{GL}_n(\mathbb{F}_q) \\ \mathrm{Gal}(\ell/k) \arrow[ur, "\bar{\rho}"'] & \end{tikzcd}$$

Since ρ is injective by Theorem 2.6, we conclude that so is π. $\square$

2.5. Description of the splitting field

Let K be a field containing $\mathbb{F}_q$ and let $A \in \mathbf{GL}_n(K)$.

Let $\mathbf{U} = (\mathbf{u_{ij}})$, where the $\mathbf{u_{ij}}$'s $(i, j = 1, \ldots, n)$ are indeterminates. Let $d = \det(A)$ and let $J \subset K[\mathbf{U}]$ be the ideal

$$J = \langle A\mathbf{U}^{(q)} - \mathbf{U}, \det(\mathbf{U})^{(q-1)}d - 1\rangle.$$

Proposition 2.10. *The K-algebra*

$$\mathcal{E} = K[\mathbf{U}]/J$$

is a Galois $\mathbf{GL}_n(\mathbb{F}_q)$-algebra over K. Its indecomposable factors are isomorphic to the splitting field E of the Frobenius module (K^n, Φ_A).

Proof. Let $U \in \mathbf{GL}_n(K_{\mathrm{sep}})$ be such that $A = UU^{(q)^{-1}}$ and let $\mathbf{W} = U^{-1}\mathbf{U}$. Then, as in Proposition 2.2, we have

$$\begin{aligned} \mathcal{E} \otimes_K K_{\mathrm{sep}} &= K_{\mathrm{sep}}[\mathbf{W}]/\langle \mathbf{W}^{(q)} - \mathbf{W}, \det(\mathbf{W})^{q-1} - 1\rangle \\ &\simeq \prod_{\mathbf{GL}_n(\mathbb{F}_q)} K_{\mathrm{sep}}. \end{aligned}$$

Thus $\mathcal{E}$ is étale. The action of $\mathbf{GL}_n(\mathbb{F}_q)$ on $\mathcal{E}$ is given by $\mathbf{U} \mapsto \mathbf{U}a$ for $a \in \mathbf{GL}_n(\mathbb{F}_q)$. The primitive idempotents of $\mathcal{E} \otimes_K K_{\mathrm{sep}}$ are represented by $e_b(\mathbf{U}) = f_b(U^{-1}\mathbf{U})$, where $b \in \mathbf{GL}_n(\mathbb{F}_q)$ and $f_b(\mathbf{W}) \in \mathbb{F}_q[W]$ is the Lagrange interpolation polynomial such that $f_b(w) = \delta_{b,w}$ for $w \in \mathbf{GL}_n(\mathbb{F}_q)$. We see easily that $ae_b = e_{ba^{-1}}$, so $\mathbf{GL}_n(\mathbb{F}_q)$ acts simply transitively on the set of primitive idempotents of $\mathcal{E} \otimes_K K_{\mathrm{sep}}$. Thus $\mathcal{E}$ is a Galois $\mathbf{GL}_n(\mathbb{F}_q)$-algebra.

The indecomposable factors of $\mathcal{E}$ are precisely the images of K-algebra homomorphisms $\mathcal{E} \to K_{\mathrm{sep}}$. If $\varphi : \mathcal{E} \to K_{\mathrm{sep}}$ is such a homomorphism, then the columns of $U = \varphi(\mathbf{U})$ form an $\mathbb{F}_q$-basis of the space of solutions of the system $AX^{(q)} = X$. Thus $E = \varphi(\mathcal{E})$. $\square$

Let $\{\epsilon_1, \epsilon_2, \dots, \epsilon_h\}$ be the set of primitive idempotents of $\mathcal{E}$. The group $\mathbf{GL}_n(\mathbb{F}_q)$ acts on this set transitively and each subalgebra $\mathcal{E}\epsilon_i$ (with identity ϵ_i) is isomorphic to E by Proposition 2.10.

Proposition 2.11. *Let R be an integrally closed Noetherian domain with field of fractions K and let $\mathcal{S} = R[\mathbf{U}]/J_0$, where $J_0 = J \cap R[\mathbf{U}]$. Assume $A \in \mathbf{GL}_n(R)$. Then each primitive idempotent ϵ_i of $\mathcal{E}$ lies in $\mathcal{S}$. In particular, we have a decomposition*

$$\mathcal{S} = \sum_{i=1}^{h} \mathcal{S}\epsilon_i. \tag{4}$$

Proof. It is enough to prove that $\epsilon_1 \in \mathcal{S}$. Let G be the stabilizer of ϵ_1 in $\mathbf{GL}_n(\mathbb{F}_q)$. Then

$$\epsilon_1 = \sum_{a \in G} e_a,$$

where the $e_a \in \mathcal{E} \otimes K_{\mathrm{sep}}$ are absolutely primitive idempotents. As we have seen in the proof of Proposition 3, we have $e_a(\mathbf{U}) = f_b(U^{-1}\mathbf{U})$, where $f_a(\mathbf{W}) \in \mathbb{F}_q[\mathbf{W}]$ is the Lagrange interpolation polynomial such that $f_a(w) = \delta_{a,w}$ for $w \in \mathbf{GL}_n(\mathbb{F}_q)$, where δ is the Dirichlet symbol. Since the entries of U (and U^{-1}) are integral over R by Proposition 2.8, we conclude that the coefficients of $e_a(\mathbf{U})$, as polynomial in the variables $\mathbf{u}_{ij}$, are integral over R. It follows that $\epsilon_1 \in K[\mathbf{U}]$ has coefficients integral over R. Since R is integrally closed by hypothesis, we have $\epsilon_1 \in R[\mathbf{U}]$. $\square$

Corollary 2.12. *The ring extension $\mathcal{S}/R$ is Galois with group $\mathbf{GL}_n(\mathbb{F}_q)$.*

Proof. Let $\epsilon \in \mathcal{S}$ be a primitive idempotent and let G be the stabilizer of ϵ in $\mathbf{GL}_n(\mathbb{F}_q)$ and let $S = \mathcal{S}\epsilon$. From the decomposition (4) we have

$$\mathcal{S} \simeq \mathrm{Map}_G\big(\mathbf{GL}_n(\mathbb{F}_q), S\big),$$

where $\mathrm{Map}_G(\mathbf{GL}_n(\mathbb{F}_q), S)$ is the set of G-equivariant maps $\mathbf{GL}_n(\mathbb{F}_q) \to S$ and $(a\alpha)(x) = \alpha(xa)$ for $a \in \mathbf{GL}_n(\mathbb{F}_q)$ and $\alpha \in \mathrm{Map}_G(\mathbf{GL}_n(\mathbb{F}_q))$. Since S/R is G-Galois by Proposition 2.9, we conclude that $\mathcal{S}/R$ is $\mathbf{GL}_n(\mathbb{F}_q)$-Galois. $\square$

3. Generic extensions for multiplicative groups

Let k be a field and let G be a finite group. Let $R = k[\mathbf{t}, 1/d]$, where $\mathbf{t} = (t_1, \dots, t_m)$ are indeterminates and d is a nonzero polynomial in $k[\mathbf{t}]$. The following definition is due to Saltman [10].

Definition 3. A Galois G-extension S/R of commutative rings is called *G-generic over k* if for every Galois G-algebra M/L, where L is a field containing k, there exists a homomorphism of k-algebras $\varphi : R \to L$ such that $S \otimes_\varphi L \simeq M$ as G-algebras over L.

In this section $\mathcal{A} \subset M_n(\mathbb{F}_q)$ denotes a fixed $\mathbb{F}_q$-subalgebra and m denotes its dimension over $\mathbb{F}_q$. The goal of this section is to construct explicitly a Galois $\mathcal{A}^\times$-extension S/R that is $\mathcal{A}^\times$-generic in the above sense.

We denote henceforth by $\mathbf{G}$ the multiplicative group $\mathbf{G}_m(\mathcal{A})$ as an algebraic group defined over $\mathbb{F}_q$. Let $a_1, a_2, \dots, a_m$ be a basis of $\mathcal{A}$ over $\mathbb{F}_q$ and define

$$A(\mathbf{t}) = \sum_{i=1}^{m} t_i a_i, \tag{5}$$

where $\mathbf{t} = (t_1, \dots, t_m)$ are indeterminates.

Let $d = \det(A)$ and let $R = \mathbb{F}_q[\mathbf{t}, 1/d]$. By the construction of R we clearly have $A \in \mathbf{G}(R)$. Let E be the splitting field of the Frobenius module given by A over $K = \mathbb{F}_q(\mathbf{t})$. By Theorem 2.5, there exists $U \in \mathbf{G}(K_{\mathrm{sep}})$ such that $A = U(U^{(q)})^{-1}$. Recall that by Corollary 2.4, the coefficients u_{ij} of U generate E over K. We write, by abuse of notation, $E = K(U)$. We define similarly $S = R[U]$, the subring of E generated by the u_{ij}'s over R. Note that by Proposition 2.8 the u_{ij}'s are integral over R, so S is finitely generated as an R-module.

Here is the main theorem in this section.

Theorem 3.1. *With the notation above, we have*

1. $\mathrm{Gal}(E/K) \simeq \mathbf{G}(\mathbb{F}_q)$.
2. *The ring extension S/R is $\mathbf{G}(\mathbb{F}_q)$-generic.*

The following two lemmas will be needed in the proof of Theorem 3.1.

Lemma 3.2. *Let $a, b \in \mathbf{G}(\mathbb{F}_q)$. If a and b are conjugate in $\mathbf{G}(\overline{\mathbb{F}}_q)$, then they are conjugate in $\mathbf{G}(\mathbb{F}_q)$.*

Proof. Suppose $a = ubu^{-1}$ with $u \in \mathbf{G}(\overline{\mathbb{F}}_q)$. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. Then $z_\sigma := u^{-1}\sigma(u)$ is in $(\mathcal{Z} \otimes \overline{\mathbb{F}}_q)^\times$, where $\mathcal{Z}$ is the centralizer of b in $\mathcal{A}$. The map $\sigma \mapsto z_\sigma$ is a 1-cocycle with values in $(\mathcal{Z} \otimes \overline{\mathbb{F}}_q)^\times$. By the generalized Hilbert Theorem 90 (see e.g. [12, Chap. X]), this 1-cocycle is trivial, that is, there exists $w \in (\mathcal{Z} \otimes \overline{\mathbb{F}}_q)^\times$ such that $z_\sigma := w^{-1}\sigma(w)$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. Then $v := uw^{-1}$ satisfies $a = vbv^{-1}$ and is fixed under $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, that is, v is in $\mathbf{G}(\mathbb{F}_q) = \mathcal{A}^\times$. □

Lemma 3.3. *Let G be a finite group and let $C_1, C_2, \dots, C_h$ be the conjugacy classes of G. Let $g_i \in C_i$ for $i = 1, \dots, h$. Then the set $\{g_1, g_2, \dots, g_h\}$ generates G.*

Proof. See [13, Theorem 4′]. □

Proof of Theorem 3.1. (1) By Theorem 2.5, there exists $U \in \mathbf{G}(K_{\mathrm{sep}})$ such that $A = UU^{(q)^{-1}}$. Let $\rho : \mathrm{Gal}(E/K) \to \mathbf{G}(\mathbb{F}_q)$ be the map defined by $\rho(\sigma) = U^{-1}\sigma(U)$. By Theorem 2.6, the map ρ is an injective group homomorphism.

We have on the one hand by Theorem 2.7 and Lemma 3.2 that every specialization $A(\boldsymbol{\xi}) \in \mathbf{G}(\mathbb{F}_q)$ (where $\boldsymbol{\xi} \in \mathbb{F}_q^m$) is conjugate in $\mathbf{G}(\mathbb{F}_q)$ to an element of $\mathrm{im}(\rho)$. On the other hand, every element of $\mathbf{G}(\mathbb{F}_q)$ is of the form $A(\boldsymbol{\xi})$ for some $\boldsymbol{\xi} \in \mathbb{F}_q^m$, thus every conjugacy class of $\mathbf{G}(\mathbb{F}_q)$ intersects nontrivially $\mathrm{im}(\rho)$. We conclude by Lemma 3.3 that $\mathrm{im}(\rho) = \mathbf{G}(\mathbb{F}_q)$.

(2) Let L be a field containing $\mathbb{F}_q$ and let M/L be a Galois G-algebra with group $G = \mathbf{G}(\mathbb{F}_q)$ and let $\delta \in M$ be a primitive idempotent. Then $N = M\delta$ is a field that is Galois with group $H = G_\delta$ over K. Moreover, there is an isomorphism of G-algebras over L

$$M \simeq \mathrm{Map}_H(G, N),$$

where $\mathrm{Map}_H(G, N)$ is the algebra of H-equivariant maps $G \to N$ [5, Proposition 18.18]. The action of G is given by $(g\alpha)(x) = \alpha(xg)$ for $\alpha \in \mathrm{Map}_H(G, N)$ and $g \in G$. Under the above isomorphism, the primitive idempotents of M correspond to the characteristic functions of the right cosets of H in G. In particular, δ corresponds to the characteristic function of H.

Let $\rho : \mathrm{Gal}(N/L) \to H$ be an isomorphism. Composing with the inclusion $H \subset G = \mathbf{G}(\mathbb{F}_q) \subset \mathbf{G}(N)$, we can view ρ as a 1-cocycle with values in $\mathbf{G}(N) = (\mathcal{A} \otimes N)^\times$. By the generalized Hilbert Theorem 90 (see e.g. [12, Chap. X]), ρ is a trivial 1-cocycle, i.e. there exists $W \in \mathbf{G}(N)$ such that $\rho(\sigma) = W^{-1}\sigma(W)$ for all $\sigma \in \mathrm{Gal}(N/L)$.

We first observe that N is generated over L by the coefficients w_{ij} of W. Indeed, if $\sigma \in G$ is such that $\sigma(w_{ij}) = w_{ij}$ for $i, j = 1, \ldots, n$, then $\rho(\sigma) = 1$ and consequently $\sigma = 1$ since ρ is injective.

Let $B = WW^{(q)^{-1}}$. It is readily verified that B is fixed by $\mathrm{Gal}(N/L)$ and hence lies in $\mathbf{G}(L)$. Thus we can write $B = A(\boldsymbol{\xi})$ for some $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_n) \in L^n$. Define an $\mathbb{F}_q$-algebra homomorphism $f : R \to L$ by $\mathbf{t} \mapsto \boldsymbol{\xi}$. Since S is integral over R, we can extend f to a ring homomorphism [7, Ch. VII, Proposition 3.1]

$$\hat{f} : S \to \overline{L}.$$

Let U be the class of $\mathbf{U}$ in S. Then $U(U^{(q)})^{-1} = A$ and $W_1 := \hat{f}(U) \in \mathbf{GL}_n(\overline{L})$ satisfies $W_1(W_1^{(q)})^{-1} = B$ so $W_1 = Wg$ for some $g \in \mathbf{GL}_n(\mathbb{F}_q)$. Replacing U by Ug^{-1}, we can assume $\hat{f}(U) = W$. Since the coefficients u_{ij} of U generate S over R and the coefficients w_{ij} of W generate N over L, we have

$$\hat{f}(S)L = N. \tag{6}$$

Since $\hat{f}$ is $\mathbb{F}_q$-linear, we have

$$\hat{f}(Uh) = Wh$$

for $h \in H$. Identifying $\mathrm{Gal}(S/R)$ with G via the isomorphism $\sigma \mapsto U^{-1}\sigma(U)$ and $\mathrm{Gal}(N/L)$ with H via the isomorphism $\tau \mapsto W^{-1}\tau(W)$, we have from the above that

$$\hat{f}\bigl(h(U)\bigr) = h(W)$$

for $h \in H$, which implies that $\hat{f}$ is an H-homomorphism. Then we can consider the induced G-homomorphism

$$F : S \longrightarrow M = \mathrm{Map}_H(G, N)$$

defined by $F(s)(g) = \hat{f}(g(s))$ for $s \in S$ and $g \in G$.

Since S/R is G-Galois by Proposition 2.9, so is $S \otimes_f L/L$ and the map

$$\begin{aligned} S \otimes_f L &\longrightarrow M \\ s \otimes x &\longmapsto F(s)x \end{aligned} \tag{7}$$

is a morphism of Galois G-extensions of L, which is automatically an isomorphism (see e.g. [4, Proposition 5.1.1]). □

4. Generic polynomials

We recall here the definition of generic polynomial. We refer to [4] for details and a wealth of examples.

Let $\mathbf{t} = (t_1, \dots t_m)$ be indeterminates over the field k and let G be a finite group.

Definition 4. A monic separable polynomial $f(Y; \mathbf{t}) \in k(\mathbf{t})[Y]$ is called *G-generic* over k if the following conditions are satisfied:

1. $\mathrm{Gal}(f(Y; \mathbf{t})/k(\mathbf{t})) \simeq G$.
2. Every Galois G-extension M/L, where L is a field containing k, is the splitting field of a specialization $f(Y; \boldsymbol{\xi})$ for some $\boldsymbol{\xi} \in L^n$.

In this section we give a method to explicitly construct a generic polynomial for the group $G = \mathcal{A}^\times$ over the field $k = \mathbb{F}_q$. The method is based on the cyclicity of Frobenius modules over $k(\mathbf{t})$ (see [9, Section I.2]).

Definition 5. A Frobenius module (M, φ) over a field K is *cyclic* if there exists a nonzero vector $v \in M$ such that $\{v, \varphi(v), \varphi^2(v), \dots, \varphi^{n-1}(v)\}$ forms a basis of M.

Note that the matrix of (M, φ) relative to a cyclic basis

$$\{v, \varphi(v), \varphi^2(v), \dots, \varphi^{n-1}(v)\}$$

has the form

$$\Delta = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & a_{n-1} \end{pmatrix}. \tag{8}$$

In [9, Theorem 2.1], Matzat proves in particular that if the ground field K is infinite, all Frobenius modules over K are cyclic. The Frobenius modules we consider in this section are over the field $K = \mathbb{F}_q(\mathbf{t})$, where $\mathbf{t} = (t_1, \dots, t_m)$, so they are always cyclic.

For $B \in \mathbf{GL}_n(K)$, we denote by B^* the matrix

$$B^* = \left(B^{-1}\right)^T.$$

Notice that the map $B \mapsto B^*$ is a group homomorphism.

Proposition 4.1. *Let $B \in \mathbf{GL}_n(K)$. The systems $BX^{(q)} = X$ and $B^*X^{(q)} = X$ have the same splitting fields.*

Proof. Let $U \in \mathbf{GL}_n(K_{\text{sep}})$ be such that $B = U(U^{(q)})^{-1}$. As we have seen in 2.4, the splitting field of the Frobenius module given by B is found by adjoining the coefficients of U to the base field K. If we apply the matrix operator *, we obtain

$$B^* = U^*\left(U^{*(q)}\right)^{-1},$$

which shows that the splitting field of the Frobenius module given by B^* is generated over K by the coefficients of U^*. Clearly the coefficients of U and those of U^* generate the same field. □

Let $B \in \mathbf{GL}_n(K)$, where K is an infinite field. Then the Frobenius module (K^n, φ_B), where $\varphi_B X = BX^{(q)}$ admits a cyclic basis, that is, there exists $N \in \mathbf{GL}_n(K)$ such that

$$N^{-1}BN^{(q)} = \Delta, \tag{9}$$

where Δ is a matrix of the form (8). An immediate application of Proposition 4.1 is

Corollary 4.2. *The splitting fields of the Frobenius modules given by B and Δ^* are the same.*

Computing the splitting field of the Frobenius module given by Δ^* is straightforward. We solve explicitly the system $\Delta^* X^{(q)} = X$ or, equivalently, the system $X^{(q)} = \Delta^T X$. Letting $X = (x_1, \dots, x_n)^T$, we have

$$\begin{cases} x_1^q = x_2 \\ \quad\vdots \\ x_{n-1}^q = x_n \\ x_n^q = a_0 x_1 + a_1 x_2 + \cdots + a_{n-1} x_n. \end{cases}$$

Setting $x_1 = y$, we have from the above system $x_i = y^{q^{i-1}}$ for $i = 1, \dots, n$, where y satisfies the equation

$$y^{q^n} = a_0 y + a_1 y^q + \cdots + a_{n-1} y^{q^{n-1}}.$$

Corollary 4.3. *The splitting fields of the Frobenius module given by B and the additive polynomial $f(Y) = Y^{q^n} - a_0 y - a_1 Y^q - \cdots - a_{n-1} Y^{q^{n-1}}$ coincide.*

Remark 3. The polynomial $f(Y)$ above is separable since $f'(Y) = a_0 = \det \Delta \neq 0$.

We shall now apply the above observations to obtain an explicit generic polynomial for the group $\mathcal{A}^\times$, where $\mathcal{A} \subset M_n(\mathbb{F}_q)$ is an $\mathbb{F}_q$-subalgebra. Recall that $\mathbf{G}$ denotes the multiplicative group $\mathbf{G}_m(\mathcal{A})$ as an algebraic group defined over $\mathbb{F}_q$. Let $v_1, v_2, \dots, v_m$ be a basis of $\mathcal{A}$ over $\mathbb{F}_q$ and define

$$A(\mathbf{t}) = \sum_{i=1}^{m} t_i v_i,$$

where the t_i's are indeterminates.

Our next goal is to show that for $K = \mathbb{F}_q(\mathbf{t})$ and $B = A(\mathbf{t})$, the polynomial $f \in K[Y]$ given by Corollary 4.3 is $\mathbf{G}(\mathbb{F}_q)$-generic. We will need the following preliminary lemmas.

Lemma 4.4. *Let L be a field and let $B \in \mathbf{G}(L)$. Then the morphism of affine varieties defined over L*

$$\begin{aligned} \psi : \quad & \mathbf{G} \longrightarrow \mathbf{G} \\ & X \longmapsto X^{-1} B X^{(q)} \end{aligned} \tag{10}$$

is an epimorphism, that is, the induced ring homomorphism $\psi^* : L[\mathbf{G}] \to L[\mathbf{G}]$ is injective.

Proof. Over an algebraic closure $\bar{L}$, the map $\psi : \mathbf{G}(\bar{L}) \to \mathbf{G}(\bar{L})$ is surjective as an immediate consequence of the Lang–Steinberg theorem. Indeed, write $B = U {U^{(q)}}^{-1}$

with $U \in \mathbf{G}(\bar{L})$ and let $Y = U^{-1}X$. Then $\psi(X) = Y^{-1}Y^{(q)}$. Theorem 2.5 states that all elements of $\mathbf{G}(\bar{L})$ are of the form $Y^{-1}Y^{(q)}$.

Thus the induced ring homomorphism $\psi^* : \bar{L}[\mathbf{G}] \to \bar{L}[\mathbf{G}]$ is injective. The announced result follows trivially from this. $\square$

Lemma 4.5. *Assume that L is an infinite field. Let $p \in L[\mathbf{t}, 1/d]$ be a nonzero rational function and let B be an element of $\mathbf{G}(L)$. Then there exists $\boldsymbol{\xi} \in L^n$ such that $p(\boldsymbol{\xi}) \neq 0$ and $A(\boldsymbol{\xi})$ is Frobenius-equivalent to B in $\mathbf{G}(L)$.*

Proof. Let $O \subset \mathbb{A}^m$ be the open subset where $d \neq 0$. Then the map $\alpha : O \to \mathbf{G}$ given by $\alpha(\boldsymbol{\xi}) = A(\boldsymbol{\xi})$ is an isomorphism of affine varieties defined over L. Define $\varphi = \alpha^{-1} \circ \psi \circ \alpha$. By Lemma 4.4, $\varphi^*(p) = p \circ \varphi$ is not zero. Since L is infinite, there exists $\boldsymbol{\eta} \in O(L) \subset L^m$ such that $p(\varphi(\boldsymbol{\eta})) \neq 0$. Let $\boldsymbol{\xi} = \varphi(\boldsymbol{\eta})$. Then $A(\boldsymbol{\xi}) = \alpha(\boldsymbol{\xi}) = \alpha(\varphi(\boldsymbol{\eta})) = \psi(\alpha(\boldsymbol{\eta})) = \alpha(\boldsymbol{\eta})^{-1}B\alpha(\boldsymbol{\eta})^{(q)}$. $\square$

Theorem 4.6. *Let $f(Y;\mathbf{t}) \in \mathbb{F}_q(\mathbf{t})[Y]$ be the polynomial obtained from $A(\mathbf{t})$ as in Corollary 4.3. Then $f(Y;\mathbf{t})$ is $\mathbf{G}(\mathbb{F}_q)$-generic over any infinite field k containing $\mathbb{F}_q$.*

Proof. Let $K = \mathbb{F}_q(\mathbf{t})$ and let E/K be the splitting field of the Frobenius module $(K^n, \varphi_{A\mathbf{t}})$. By Corollary 4.3, E is also the splitting field of $f(Y;\mathbf{t})$. We already know by Theorem 3.1 that $\mathrm{Gal}(E/K) \simeq \mathbf{G}(\mathbb{F}_q)$. Thus we need only to show that $f(Y;\mathbf{t})$ is generic.

As in (9), there exists $N \in \mathbf{GL}_n(K)$ such that

$$N^{-1}AN^{(q)} = \Delta. \tag{11}$$

By choosing a cyclic basis $b \in R^n$ (where $R = \mathbb{F}_q[\mathbf{t}, 1/d]$ as in Section 3), we can assume that N has coefficients in R. Let $p(\mathbf{t}) = \det N$.

Let M/L be a $\mathbf{G}(\mathbb{F}_q)$-extension, where L is an infinite field containing $\mathbb{F}_q$. Choose an isomorphism $\rho : \mathrm{Gal}(M/L) \xrightarrow{\simeq} \mathbf{G}(\mathbb{F}_q)$. We view ρ as a 1-cocycle with values in $\mathbf{G}(M)$. By the general Hilbert's Theorem 90 [12, Chap. X], there exists $W \in \mathbf{G}(M)$ such that $\rho(\sigma) = W^{-1}\sigma(W)$ for $\sigma \in \mathrm{Gal}(M/L)$. Define $B = WW^{(q)^{-1}}$. An elementary verification shows that B is fixed under $\mathrm{Gal}(M/L)$ and therefore lies in $\mathbf{G}(L)$. It is also easy to see that M is the splitting field of the system $BX^{(q)} = X$. By Lemma 4.5, there exists $\boldsymbol{\xi} \in L^n$ such that $p(\boldsymbol{\xi}) \neq 0$ and $B' := A(\boldsymbol{\xi})$ is Frobenius-equivalent to B. Since $\boldsymbol{\xi}$ has been chosen so that $N(\boldsymbol{\xi})$ is nonsingular (recall that $p(\mathbf{t}) = \det N$), we can evaluate (11) at $\mathbf{t} = \boldsymbol{\xi}$. We get

$$N(\boldsymbol{\xi})^{-1}B'N(\boldsymbol{\xi})^{(q)} = \Delta(\boldsymbol{\xi}). \tag{12}$$

We conclude by Corollary 4.3 that M is the splitting field of $f(Y;\boldsymbol{\xi})$ over L. $\square$

5. Examples

In this section, we give specific examples of generic polynomials.

Example 1. Let $\mathcal{A} = \mathbb{F}_9$ be seen as finite-dimensional algebra over $\mathbb{F}_3$. Then $G = \mathcal{A}^\times \simeq C_8$.

Taking the basis $\{1, \sqrt{-1}\}$ of $\mathcal{A}$ over $\mathbb{F}_3$, we can embed $\mathcal{A}$ into $M_2(\mathbb{F}_3)$ via the regular representation. Then the matrix A of (5) is given by

$$A(\mathbf{t}) = \begin{pmatrix} t_1 & -t_2 \\ t_2 & t_1 \end{pmatrix}.$$

Let $v = (0,1)^T \in \mathbb{F}_3^2$ serve as the generator for the cyclic module. Then as in the last section,

$$N = \left(v|Av^{(3)}\right) = \begin{pmatrix} 1 & t_1 \\ 0 & t_2 \end{pmatrix}.$$

Clearly N is non-singular. Let

$$\Delta = N^{-1}AN^{(3)} = \begin{pmatrix} 0 & -t_2^2(t_1^2 + t_2^2) \\ 1 & t_1(t_1^2 + t_2^2) \end{pmatrix}.$$

By Theorem 4.6, the additive polynomial f below build with the coefficients of the last column of Δ is generic for the group C_8 over any infinite field of characteristic 3.

$$f(Y; \mathbf{t}) = t_2^2\left(t_1^2 + t_2^2\right)Y - t_1\left(t_1^2 + t_2^2\right)Y^3 + Y^9.$$

This computation generalizes easily for any odd prime p. An additive generic polynomial for C_{p^2-1} in characteristic p is

$$f(Y; \mathbf{t}) = t_2^{p-1}\left(t_1^2 - \varepsilon t_2^2\right)Y - t_1\left(t_1^{p-1} + t_2^{p-1}\right)Y^p + Y^{p^2},$$

where $\varepsilon \in \mathbb{F}_p^\times$ is a nonsquare.

Example 2. Consider the following matrices $\mathbf{GL}_3(\mathbb{F}_2)$:

$$a = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad b = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad c = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

It is easily verified that they generate a subgroup isomorphic to A_4, the alternating group on four elements.

Let $\mathcal{A}$ be the subalgebra generated by a, b and c in $M_3(\mathbb{F}_2)$. We verify readily that $\dim_{\mathbb{F}_2}(\mathcal{A}) = 5$ and $|\mathcal{A}^\times| = 12$. Thus $\mathcal{A}^\times \simeq A_4$. After choosing a basis of $\mathcal{A}$, we obtain a matrix in 5 parameters

$$A(\mathbf{t}) = \begin{pmatrix} t_1 + t_2 + t_3 + t_4 + t_5 & t_2 & t_3 + t_4 \\ 0 & t_1 + t_2 + t_4 + t_5 & t_2 + t_3 + t_5 \\ 0 & t_2 + t_3 + t_5 & t_1 + t_3 + t_4 \end{pmatrix}.$$

As in the last section, we choose a generator for the associated Frobenius module. Let $v = (1, 0, 1)^T \in \mathbb{F}_2^3$. The matrix

$$N = \left(v | Av^{(2)} | AA^{(2)}v^{(4)}\right)$$

is nonsingular, so v is indeed a generator.

As before, we compute $\Delta = N^{-1}AN^{(2)}$. Recall that the entries in the last column of Δ are the coefficients of an additive generic polynomial $f(Y; \mathbf{t})$ of degree 8 for $\mathcal{A}^\times \simeq A_4$ by Theorem 4.6. We exhibit below an irreducible factor g of $f(Y; \mathbf{t})$ of degree 4. Since no proper quotient of A_4 can act transitively on 4 elements, the Galois group of g over $\mathbb{F}_2(\mathbf{t})$ is A_4. Obviously g is also generic.

$$\begin{aligned} g = Y^4 &+ \left(t_1^2 + t_1t_2 + t_2^2 + t_1t_3 + t_2t_3 + t_3^2 + t_2t_4 + t_3t_4 + t_4^2 + t_1t_5 + t_3t_5\right. \\ &\left.+ t_4t_5 + t_5^2\right)Y^2 + \left(t_1^2t_2 + t_1t_2^2 + t_2^3 + t_1^2t_3 + t_1t_3^2 + t_3^3 + t_2^2t_4 + t_3^2t_4\right. \\ &\left.+ t_2t_4^2 + t_3t_4^2 + t_1^2t_5 + t_2^2t_5 + t_4^2t_5 + t_1t_5^2 + t_2t_5^2 + t_4t_5^2 + t_5^3\right)Y \\ &+ \left(t_1^2t_2t_4 + t_2^3t_4 + t_1^2t_3t_4 + t_1t_2t_3t_4 + t_1t_3^2t_4 + t_2t_3^2t_4 + t_1^2t_4^2\right. \\ &+ t_2^2t_4^2 + t_2t_3t_4^2 + t_2t_4^3 + t_3t_4^3 + t_4^4 + t_1t_2^2t_5 + t_2^3t_5 + t_2^2t_3t_5 \\ &+ t_1t_3^2t_5 + t_2t_3^2t_5 + t_3^3t_5 + t_1^2t_4t_5 + t_1t_3t_4t_5 + t_3t_4^2t_5 + t_4^3t_5 \\ &\left.+ t_2^2t_5^2 + t_3^2t_5^2 + t_2t_4t_5^2 + t_4^2t_5^2 + t_1t_5^3 + t_2t_5^3 + t_3t_5^3 + t_5^4\right). \end{aligned}$$

While this method always produces $\mathcal{A}^*$-generic polynomials, the number of parameters is not optimal. A generic polynomial with two parameters was obtained in [11] for A_4, compared to the five parameters that this method needed.

The function field in one variable $\mathbb{F}_2(s)$ is Hilbertian, so "most" specializations of g in $\mathbb{F}_2(s)$ are irreducible and have Galois group A_4. Here are some examples.

$$g_1 = s + Y + Y^2 + Y^4;$$
$$g_2 = s^2 + s^3Y + s^2Y^2 + Y^4.$$

References

[1] Shreeram S. Abhyankar, Galois embeddings for linear groups, Trans. Amer. Math. Soc. 352 (8) (2000) 3881–3912.

[2] Maximilian Albert, Annette Maier, Additive polynomials for finite groups of Lie type, Israel J. Math. 186 (2011) 125–195.
[3] M.F. Atiyah, I.G. Macdonald, Introduction to Commutative Algebra, Addison–Wesley Publishing Co., Reading, MA, London, Don Mills, ON, 1969.
[4] Christian U. Jensen, Arne Ledet, Noriko Yui, Constructive aspects of the inverse Galois problem, in: Generic Polynomials, in: Math. Sci. Res. Inst. Publ., vol. 45, Cambridge University Press, Cambridge, 2002.
[5] Max-Albert Knus, Alexander Merkurjev, Markus Rost, Jean-Pierre Tignol, The Book of Involutions, American Mathematical Society, Providence, RI, 1998. With a preface in French by J. Tits.
[6] Serge Lang, Algebraic groups over finite fields, Amer. J. Math. 78 (1956) 555–563.
[7] Serge Lang, Algebra, third edition, Grad. Texts in Math., vol. 211, Springer-Verlag, New York, 2002.
[8] Arne Ledet, Generic extensions and generic polynomials, J. Symbolic Comput. 30 (6) (2000) 867–872.
[9] B. Heinrich Matzat, Frobenius modules and Galois groups, in: Galois Theory and Modular Forms, in: Dev. Math., vol. 11, Kluwer Acad. Publ., Boston, MA, 2004, pp. 233–267.
[10] David J. Saltman, Generic Galois extensions and problems in field theory, Adv. Math. 43 (3) (1982) 250–283.
[11] A.È. Sergeev, A.V. Yakolev, Generic polynomials over fields of characteristic two for transitive subgroups of the group S_4, in: Problems in the Theory of Representations of Algebras and Groups. Part 13, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) 330 (2006) 247–258, 274–275.
[12] Jean-Pierre Serre, Corps locaux, deuxième édition, Hermann, Paris, 1968. Publications de l'Université de Nancago, No. VIII.
[13] Jean-Pierre Serre, On a theorem of Jordan, Bull. Amer. Math. Soc. (N.S.) 40 (4) (2003) 429–440 (electronic).
[14] Robert Steinberg, Endomorphisms of Linear Algebraic Groups, Mem. Amer. Math. Soc., vol. 80, American Mathematical Society, Providence, RI, 1968.