Math. Res. Lett. **14** (2007), *no.* 3, 443–452 © International Press 2007

GENERIC GALOIS EXTENSIONS FOR $\mathrm{SL}_2(\mathbb{F}_5)$ OVER $\mathbb{Q}$

Bernat Plans

Abstract. Let G_n be a double cover of either the alternating group A_n or the symmetric group S_n, and let G_{n-1} be the corresponding double cover of A_{n-1} or S_{n-1}. For every odd $n \geq 3$ and every field k of characteristic 0, we prove that the following are equivalent: **(i)** there exists a generic extension for G_{n-1} over k, **(ii)** there exists a generic extension for G_n over k. As a consequence, there exists a generic extension over $\mathbb{Q}$ for the group $\widetilde{A_5} \cong \mathrm{SL}_2(\mathbb{F}_5)$.

1. Introduction

The problem originating the present paper concerns generic Galois extensions, as introduced by D. Saltman [14], for the non-trivial double cover $\widetilde{A_n}$ of the alternating group A_n ($n \geq 4$). More concretely, one may ask whether such extensions do exist over $\mathbb{Q}$.

In [13], Y. Rikuna obtains a positive answer to this question in the case $n = 4$. In [10], J-F. Mestre gives a different proof of this same result.

On the other hand, J-P. Serre [17, Thm. 33.26] proved that the answer is 'no' for $n = 6$ and $n = 7$.

Our initial purpose was to fill the gap corresponding to $n = 5$. It may be worth mentioning that, in the context of Noether's problem, this case is positively solved over a field k (instead of $\mathbb{Q}$) provided $\widetilde{A_5}$ can be embedded into $\mathrm{GL}_2(k)$ (cf. [11] and, e.g., [15]); actually, this is possible for $k := \mathbb{Q}[e^{2\pi i/5}]$, but *not* for $k := \mathbb{Q}$.

Serre's result fits well our Thm. 3.1: there exists a generic extension for $\widetilde{A_{2m}}$ over $\mathbb{Q}$ if and only if so happens for $\widetilde{A_{2m+1}}$.

This, together with Rikuna's result, solves in the affirmative the case $n = 5$. That is, the binary icosahedral group $\widetilde{A_5} \cong \mathrm{SL}_2(\mathbb{F}_5)$ does admit a generic Galois extension over $\mathbb{Q}$.

Section 3 contains the proof of Thm. 3.1, as well as a generalization to other central extensions of A_n. In addition, almost the same proofs produce analogous results for the symmetric group S_n.

Previously, in Section 2, it is convenient to introduce the concept of "generic" Galois extension (resp. polynomial) for a finite group extension $\widetilde{G} \to G$. As a consequence of the main result of Section 2 (Prop. 2.5), such an extension exists for a double cover $\widetilde{G} \to G$ if and only if there exists a generic extension for $\widetilde{G}$.

All of the above is relative to a fixed base field k. In Section 2, it can be an arbitrary *infinite* field. In Section 3 we add the extra hypothesis, which comes from [9], that the characteristic of k is 0.

Received by the editors July 10, 2006.
2000 *Mathematics Subject Classification.* 12F10, 12F12, 13A50.

2. Generic embeddable extensions

In what follows G denotes a finite group.

By a *G-extension* S/R we mean a Galois extension of commutative rings $R \subset S$ with group G as defined, for example, in [4]. In particular, this implicitly assumes that a faithful action of G on S (by R-algebra automorphisms) has been fixed. Let us mention that, in this paper, S and R will always be k-algebras for some field k.

Usually, we deal with G-extensions *up to Galois isomorphism*. Recall that a *Galois isomorphism* between two G-extensions S_1/R and S_2/R is an R-algebra isomorphism $S_1 \to S_2$ which commutes with the action of G.

Let $\widetilde{G} \xrightarrow{\pi} G$ denote a fixed epimorphism of finite groups and let C denote its kernel.

The embedding problem given by π and a G-extension S/R will be denoted by $(S/R, \pi)$. A *solution to* $(S/R, \pi)$ is a $\widetilde{G}$-extension $\widetilde{S}/R$ such that S/R is Galois isomorphic to the (quotient) G-extension $\widetilde{S}^C/R$ obtained from $\widetilde{S}/R$ and π.

A G-extension S/R such that the embedding problem $(S/R, \pi)$ is solvable will be called a *$(\widetilde{G} \xrightarrow{\pi} G)$-extension*.

Let k be a field.

Definition 2.1. A $(\widetilde{G} \xrightarrow{\pi} G)$-extension S/R is called a **generic extension for $\widetilde{G} \xrightarrow{\pi} G$ over k** if

(i) R is a *localised polynomial ring over k*, i.e., $R = k[\underline{U}][1/u]$ for some set of indeterminates $\underline{U} = (U_1, \dots, U_m)$ and some $u \in k[\underline{U}] \setminus \{0\}$.

(ii) If K is a field containing k and L/K is a $(\widetilde{G} \xrightarrow{\pi} G)$-extension, then there exists a homomorphism $\varphi : R \to K$ of k-algebras (called a *specialization*) such that L/K is Galois isomorphic to the natural G-extension $S \otimes_\varphi K/K$ obtained from S/R.

Definition 2.2. A monic polynomial $F(\underline{U}; X) \in k(\underline{U})[X]$, where $\underline{U} = (U_1, \dots, U_m)$ is a set of indeterminates, is called a **generic polynomial for $\widetilde{G} \xrightarrow{\pi} G$ over k** if

(i) $F(\underline{U}; X)$ is a separable polynomial and its splitting field over $k(\underline{U})$ is a $(\widetilde{G} \xrightarrow{\pi} G)$-extension of $k(\underline{U})$.

(ii) If L/K is a $(\widetilde{G} \xrightarrow{\pi} G)$-extension of *fields* containing k, then there exists $\underline{v} \in K^m$ such that the polynomial $F(\underline{v}; X) \in K[X]$ is separable and its splitting field over K is L.

Definition 2.3. We say that the **lifting property for $\widetilde{G} \xrightarrow{\pi} G$ over k holds** if, for every local k-algebra $(A, \mathfrak{m})$ with residue field $K := A/\mathfrak{m}$ and every $(\widetilde{G} \xrightarrow{\pi} G)$-extension of *fields* L/K, there exists a $(\widetilde{G} \xrightarrow{\pi} G)$-extension B/A such that the G-extensions L/K and $B \otimes_A K/K$ are Galois isomorphic.

Remark 2.4. If we take $\widetilde{G} = G$ and $\pi = id$, then the above definitions correspond to the usual concepts of *generic extension* (resp. *generic polynomial*) for G over k as defined, for example, in [4]. This is also true for the *lifting property* if k is an *infinite* field, although the usual definition (as in [4]) does not require that L is a field.

Proposition 2.5. *Let k be an infinite field. Let $\widetilde{G} \xrightarrow{\pi} G$ be an epimorphism of finite groups with kernel $C := Ker(\pi)$ contained in the center of $\widetilde{G}$. Assume that there exists a generic extension for C over k. Then, the following properties are equivalent:*

(i) *There exists a generic extension for* $\widetilde{G}$ *over* k.
(ii) *There exists a generic polynomial for* $\widetilde{G}$ *over* k.
(iii) *The lifting property for* $\widetilde{G}$ *over* k *holds.*
$(i)'$ *There exists a generic extension for* $\widetilde{G} \xrightarrow{\pi} G$ *over* k.
$(ii)'$ *There exists a generic polynomial for* $\widetilde{G} \xrightarrow{\pi} G$ *over* k.
$(iii)'$ *The lifting property for* $\widetilde{G} \xrightarrow{\pi} G$ *over* k *holds.*

Proof. The equivalences $(i) \Leftrightarrow (ii) \Leftrightarrow (iii)$ are well-known. See, for example, [4, Sec. 5.2] or [1]. Moreover, the proofs of $(i) \Rightarrow (iii)$ and $(ii) \Rightarrow (iii)$ given in [1, Thm. 1] are easily adapted in order to obtain $(i)' \Rightarrow (iii)'$ and $(ii)' \Rightarrow (iii)'$.

It is also clear that $(i) \Rightarrow (i)'$. Indeed, if $\widetilde{S}/R$ is a generic extension for $\widetilde{G}$ over k, then the G-extension $\widetilde{S}^C/R$ is generic for $\widetilde{G} \xrightarrow{\pi} G$ over k.

A stronger form of $(i) \Rightarrow (ii)'$ will be proved later in Lemma 2.8.

We are now going to prove $(iii)' \Rightarrow (iii)$, thus establishing Proposition 2.5.

Let $(A, \mathfrak{m})$ be a local k-algebra with residue field $K := A/\mathfrak{m}$ and let be given a $\widetilde{G}$-extension of fields $\widetilde{L}/K$.

Let us define $L := (\widetilde{L})^C$. Then, L/K is a G-extension (via π) and $\widetilde{L}/K$ is a solution to the embedding problem $(L/K, \pi)$. Now, hypothesis $(iii)'$ ensures the existence of a $(\widetilde{G} \xrightarrow{\pi} G)$-extension B/A such that the G-extensions L/K and $B \otimes_A K/K$ are Galois isomorphic.

Let $\widetilde{B_1}/A$ be (a $\widetilde{G}$-extension which is) a solution to $(B/A, \pi)$ and let us define $\widetilde{L_1} := \widetilde{B_1} \otimes_A K$. Clearly, the (specialized) $\widetilde{G}$-extension $\widetilde{L_1}/K$ is a solution to $(L/K, \pi)$.

Since $\widetilde{L}/K$ and $\widetilde{L_1}/K$ are solutions to the same embedding problem $(L/K, \pi)$, it follows from [3, Thm. 3.15.4] (and our centrality assumption) that $\widetilde{L}/K$ must be Galois isomorphic to the *composition* of $\widetilde{L_1}/K$ and a solution to the trivial (central) embedding problem $(L/K, C \times G \to G)$.

Here, the term *composition* refers to composition of solutions to embedding problems as defined, for example, in [3, 1.15], and "corresponds" to the Baer sum of group extensions. Explicitly, the last paragraph says that there exists a C-extension L_2/K such that $\widetilde{L}/K$ is Galois isomorphic to the $\widetilde{G}$-extension obtained as follows.

First, consider $L_2 \otimes_K \widetilde{L_1}/K$, which we view as a $(C \times \widetilde{G})$-extension via the action $(c, g)(l_1 \otimes l_2) := {l_1}^c \otimes {l_2}^g$ (cf. [4, Thm. 4.2.9]).

Now, if C_1 denotes the kernel of the epimorphism

$$C \times \widetilde{G} \longrightarrow \widetilde{G}, \qquad (c, g) \longmapsto cg,$$

then $(L_2 \otimes_K \widetilde{L_1})^{C_1}/K$ is a $\widetilde{G}$-extension (solution to $(L/K, \pi)$) via the corresponding isomorphism $\widetilde{G} \cong (C \times \widetilde{G})/C_1$. This $\widetilde{G}$-extension is the one which must be Galois isomorphic to $\widetilde{L}/K$.

On the other hand, since we are assuming that the lifting property holds for C over k, there exists a C-extension B_2/A such that the C-extensions L_2/K and $B_2 \otimes_A K/K$ are Galois isomorphic.

Thus, $B_2 \otimes_A \widetilde{B_1}/A$ is a $(C \times \widetilde{G})$-extension and $L_2 \otimes_K \widetilde{L_1}/K$ is Galois isomorphic to $(B_2 \otimes_A \widetilde{B_1}) \otimes_A K/K$.

As above, $(B_2 \otimes_A \widetilde{B_1})^{C_1}/A$ is a $\widetilde{G}$-extension and, certainly, $\widetilde{L}/K$ is Galois isomorphic to $(B_2 \otimes_A \widetilde{B_1})^{C_1} \otimes_A K/K$.

□

Remark 2.6. It is well-known that, over $\mathbb{Q}$, there exists a generic extension for C if and only if the (finite abelian) group C has no elements of order 8 (cf. [14, Thm. 2.1, Thm. 5.11]).

Remark 2.7. Proposition 2.5 also holds for an epimorphism $\widetilde{G} \xrightarrow{\pi} G$ with abelian kernel C not necessarily contained in the center of $\widetilde{G}$, under the assumption that there exists a generic extension over k for the semidirect product of C and G with respect to the G-action given by π. Note that this hypothesis implies the existence of a generic extension for G over k (cf. [14, Thm. 3.1]).

The following fact will also be used in the next section.

Lemma 2.8. *In Proposition 2.5, we can replace $(ii)'$ by $(ii)''$:*

Given a transitive embedding $G \hookrightarrow S_n$, there exists a generic polynomial $F(\underline{U}; X)$ for $\widetilde{G} \xrightarrow{\pi} G$ over k with the following additional properties:

- *(a)* $\deg_X(F(\underline{U}; X)) = n$ *and* $\mathrm{Gal}_{k(\underline{U})}(F)$ *is conjugate to G in S_n.*
- *(b) For every subgroup $H \subseteq G$ and every $(\pi^{-1}(H) \xrightarrow{\pi} H)$-extension L/K of fields containing k, there exists $\underline{v} \in K^m$ such that the polynomial $F(\underline{v}; X) \in K[X]$ is separable, its splitting field over K is L and, on the (suitably ordered) set of roots of $F(\underline{v}; X)$, the permutation action of H (from the fixed embedding $H \hookrightarrow S_n$) coincides with the Galois action of H (from the given H-extension L/K).*

Proof. It suffices to show that $(i) \Rightarrow (ii)''$.

Recall that we are assuming that k is an infinite field.

Let $R := k[\underline{U}][1/u]$ be a localised polynomial ring over k, and let $\widetilde{S}/R$ be a generic extension for $\widetilde{G}$ over k. It is known that we can assume that $\widetilde{S}/R$ has a normal basis $\underline{\alpha} = \{\alpha_{\widetilde{g}}\}_{\widetilde{g} \in \widetilde{G}}$, as shown in [8, Rem. 2.1]. Moreover, given a set of indeterminates $\underline{Y} = \{Y_{\widetilde{g}}\}_{\widetilde{g} \in \widetilde{G}}$ and a non-zero polynomial $d(\underline{Y}) \in k[\underline{Y}]$, we can assume too that $d(\underline{\alpha})$ is a unit in S. This also follows from the argument given in [8, Rem. 2.1], as a consequence of a result of Kuyk [7] (or [2, Lemma 3]).

For every $g \in G$, let us define

$$\beta_g := \sum_{\widetilde{g} \in \pi^{-1}(g)} \alpha_{\widetilde{g}}.$$

Obviously, $\{\beta_g\}_{g \in G}$ is a normal basis for the G-extension $\widetilde{S}^C/R$, which is generic for $\widetilde{G} \xrightarrow{\pi} G$ over k.

Let $G_1 \subset G$ be the stabilizer of 1 with respect to the fixed (faithful and transitive) action of G on $\{1, \ldots, n\}$. Given a set $\{g_1, \ldots, g_n\}$ of representatives of the left cosets of G_1 in G, we define:

$$\gamma_i := \sum_{g \in g_i G_1} \beta_g, \quad i \in \{1, \ldots, n\}.$$

We are going to show that $(ii)''$ holds with the polynomial

$$F(\underline{U}; X) := \prod_{1 \leq i \leq n} (X - \gamma_i) \quad \in \; k[\{\beta_g\}_{g \in G}]^G[X] \subset R[X],$$

whose discriminant can (and will) be assumed to being a unit in R.

Only property (b) deserves some explanation.

Given a subgroup $H \subseteq G$, let us define $\widetilde{H} := \pi^{-1}(H)$ and let $\pi_H : \widetilde{H} \to H$ denote the restriction of π to $\widetilde{H}$.

Let be given a $(\widetilde{H} \xrightarrow{\pi} H)$-extension L/K of fields containing k.

Let $\mathrm{Ind}_H^G(L)/K$ be the G-extension *induced* from the H-extension L/K and the inclusion $H \subseteq G$. Recall (e.g., [4, p.89]) that, up to Galois isomorphism, $\mathrm{Ind}_H^G(L)/K$ is the direct product of $r := (G : H)$ copies of L with the following G-action. Let $\{\sigma_1, \ldots, \sigma_r\}$ be a set of representatives of the left cosets of H in G. If $g \in G$ satisfies $g\sigma_i = \sigma_j h \in \sigma_j H$, then the j-th component of $g((l_1, \ldots, l_r))$ is $h(l_i)$.

Since we are assuming that the embedding problem $(L/K, \pi_H)$ is solvable, so must be $(\mathrm{Ind}_H^G(L)/K, \pi)$. More precisely, if $\widetilde{L}/K$ is a solution to $(L/K, \pi_H)$, then one easily checks that $\mathrm{Ind}_{\widetilde{H}}^{\widetilde{G}}(\widetilde{L})/K$ is a solution to $(\mathrm{Ind}_H^G(L)/K, \pi)$.

Then, because the G-extension $\widetilde{S}^C/R$ is generic for $\widetilde{G} \xrightarrow{\pi} G$ over k, there exists a specialization $\varphi : R \to K$ such that the G-extensions $\mathrm{Ind}_H^G(L)/K$ and $\widetilde{S}^C \otimes_\varphi K/K$ are Galois isomorphic.

Let us take $\underline{v} := \varphi(\underline{U}) \in K^m$.

Note that the (specialised) polynomial $F(\underline{v}; X) \in K[X]$ must be separable, since its discriminant belongs to $\varphi(R^*)$.

One can show that L is the splitting field of $F(\underline{v}; X)$ over K as follows (see also the proof of [1, Thm. 2]).

The elements $\{\gamma_i \otimes 1\}_{1 \le i \le n}$ generate the K-algebra $\widetilde{S}^C \otimes_\varphi K$ and they satisfy $F(\underline{v}; X) = \prod_i (X - (\gamma_i \otimes 1))$. Thus, if

$$f : \widetilde{S}^C \otimes_\varphi K \xrightarrow{\cong} \mathrm{Ind}_H^G(L) = L \times \overset{r}{\cdots} \times L$$

defines a Galois isomorphism between G-extensions of K, and $\theta_i \in L$ denotes the (say) first component of $f(\gamma_i \otimes 1) \in L \times \cdots \times L$, then $L = K[\theta_1, \ldots, \theta_n]$ and $F(\underline{v}; X) = \prod_i (X - \theta_i)$.

Moreover, the (given) Galois action of H on $\{\theta_i\}_i$ is conjugate in S_n to the fixed H-action on $\{1, \ldots, n\}$. In fact, if we choose $\sigma_1 = id$, then the H-actions on $\{\theta_i\}_i$ and on $\{\gamma_i\}_i$ coincide.

□

Remark 2.9. In accordance with the usual terminology in the case of G-extensions (see [5]), a generic polynomial for $\widetilde{G} \xrightarrow{\pi} G$ over k with property (b) may be called *descent-generic for* $\widetilde{G} \xrightarrow{\pi} G$ *over* k.

3. The cases $G = A_n$ and $G = S_n$

We first consider, for $n \ge 4$, the central extension

$$1 \to \{\pm 1\} \to \widetilde{A_n} \xrightarrow{\pi} A_n \to 1,$$

which is the unique non-split extension of the alternating group A_n by $\{\pm 1\}$. As above, if H is a subgroup of A_n, then we define $\widetilde{H} := \pi^{-1}(H)$ and $\pi_H : \widetilde{H} \to H$ denotes the restriction of π to $\widetilde{H}$.

Theorem 3.1. *Let k be a field of characteristic 0. For every odd integer $n \geq 5$, the following properties are equivalent:*

(*i*) *There exists a generic extension for $\widetilde{A_{n-1}}$ over k.*
(*ii*) *There exists a generic extension for $\widetilde{A_n}$ over k.*

Proof. In this proof we use the following terminology. Given a characteristic 0 field K, we say that a separable monic polynomial $f(X) \in K[X]$ of degree n is a *$*$-polynomial over K* if:

(1) The discriminant of $f(X)$ is a square in K. Equivalently, the Galois group of $f(X)$ over K is a subgroup H of A_n.
(2) If K_f/K denotes the (H-extension defined by the) splitting field of $f(X)$ over K, then the embedding problem $(K_f/K, \pi_H)$ is solvable.

This is equivalent to the vanishing of the two first Stiefel-Whitney invariants of the (quadratic) *trace form* $\mathrm{Tr}(X^2)$ of $K[X]/(f(X))$ over K (see [17, 33.18]).

In addition, we are going to view monic polynomials as points in affine space. Namely, a monic polynomial $f(X) := X^n + a_1X^{n-1} + \cdots + a_n \in K[X]$ of degree n over K will be identified with the point $(a_1, \ldots, a_n) \in \mathbb{A}^n(K)$.

From Proposition 2.5, it suffices to prove the equivalence between:

(*i*) There exists a generic polynomial for $\widetilde{A_{n-1}} \xrightarrow{\pi} A_{n-1}$ over k.
(*ii*) There exists a generic polynomial for $\widetilde{A_n} \xrightarrow{\pi} A_n$ over k.

(i) $\Rightarrow$ (ii).

Let $F(\underline{U}; X)$ be a generic polynomial for $\widetilde{A_{n-1}} \xrightarrow{\pi} A_{n-1}$ over k. We can (and will) assume that $F(\underline{U}; X)$ satisfies properties (a) and (b) of Lemma 2.8 with respect to $A_{n-1} \subset S_{n-1}$. In particular, its degree is $n-1$.

Recall that, given a monic polynomial $\prod_{1\leq i\leq m}(X-\theta_i)$ of degree m, its *Tschirnhaus transformation* with respect to a polynomial $\varphi(X)$ of degree $< m$ is the polynomial $\prod_{1\leq i\leq m}(X - \varphi(\theta_i))$ (see, e.g., [4, p.141]).

Let $\underline{S} := (S_1, \ldots, S_{n-1})$ be a set of indeterminates and let us define $F_{\underline{S}}(\underline{U}; X)$ as the ("generic") Tschirnhaus transformation of $F(\underline{U}; X)$ with respect to the polynomial $\varphi_S(X) := S_1X^{n-2} + \cdots + S_{n-2}X + S_{n-1}$. That is,

$$F_{\underline{S}}(\underline{U}; X) = \mathrm{Res}_Y\left(F(\underline{U}; Y), X - \varphi_S(Y)\right) \in k(\underline{U}, \underline{S})[X],$$

where $\mathrm{Res}_Y(\cdot, \cdot)$ denotes the resultant with respect to Y.

The polynomials $F_{\underline{S}}(\underline{U}; X)$ and $F(\underline{U}; X)$ have the same splitting field over $k(\underline{U}, \underline{S})$, and they satisfy $F(\underline{U}; X) = F_{\underline{s}}(\underline{U}; X)$ for $\underline{s} := (0, \ldots, 0, 1, 0)$. Hence, the polynomial $F_{\underline{S}}(\underline{U}; X) \in k(\underline{U}, \underline{S})[X]$ is also generic for $\widetilde{A_{n-1}} \xrightarrow{\pi} A_{n-1}$ over k, and satisfies properties (a) and (b) of Lemma 2.8.

Moreover, $F_{\underline{S}}(\underline{U}; X)$ satisfies the following stronger property:

> Every $*$-polynomial $f(X)$ of degree $n-1$ over a field $K \supseteq k$ arises as $F_{\underline{s}}(\underline{v}; X)$, for some $\underline{v} \in K^m$ and $\underline{s} \in K^{n-1}$.

This is clear since, from property (b) of Lemma 2.8, $f(X)$ must be Tschirnhaus equivalent over K to $F(\underline{v}; X)$ for some $\underline{v} \in K^m$.

Now, [9] produces a "$P(X) - TQ(X)$ polynomial" corresponding to $P(X) = X.F_{\underline{S}}(\underline{U}; X)$. We are going to prove that this polynomial is generic for $\widetilde{A_n} \xrightarrow{\pi} A_n$ over k. For this purpose, we rephrase (some of) the properties of Mestre's construction [9] as follows (see also [12]).

Let us define $H := \{(x_1, \ldots, x_n) \in \mathbb{A}^n \mid x_n = 0\}$ and let T be an indeterminate. Then, one deduces from [9] that there exist a Zariski open set $W \subseteq \mathbb{A}^n$ and a rational map

$$\Theta : \mathbb{A}^n \times \mathbb{A}^1 \longrightarrow \mathbb{A}^n,$$

both defined over $\mathbb{Q}$, with the following properties:

(I) $W(\mathbb{Q}) \cap H(\mathbb{Q}) \neq \emptyset$.

(II) For every field K of characteristic 0 and every $f \in W(K)$, f is a separable polynomial in $K[X]$ and $\Theta(f, T)$ is a (well-defined) separable polynomial in $K(T)[X]$ such that:

(II.1) $\Theta(f, T) \in K[T, X]$ and $\Theta(f, 0) = f$.

(II.2) The trace form of $K(T)[X]/(\Theta(f, T))$ over $K(T)$ is constant, i.e. it is $K(T)$-equivalent to a quadratic form over K.

(II.3) The Galois group of $\Theta(f, T)$ over $K(T)$ contains A_n.

(III) Restriction of Θ to $H \times \mathbb{A}^1$ defines a $\mathbb{Q}$-birational map between $H \times \mathbb{A}^1$ and $\mathbb{A}^n$. Moreover, if we denote its inverse by

$$(\Psi, \lambda) : \mathbb{A}^n \longrightarrow H \times \mathbb{A}^1,$$

then $\Psi_{|H} = id_H$, as rational maps.

It may be convenient to mention here that the map Θ above corresponds, with Mestre's notation, to the assignment $(P(X), T) \mapsto P(X) - TQ(X)$. In particular, Θ is linear in T.

Let us denote $X.F_{\underline{S}}(\underline{U}; X)$ simply by G. We claim that $\Theta(G, T)$, as a polynomial in $k(\underline{U}, \underline{S}, T)[X]$, is generic for $\widetilde{A_n} \xrightarrow{\pi} A_n$ over k.

First, note that G is a $*$-polynomial over $k(\underline{U}, \underline{S})$ which, as a consequence of property (I), must belong to $W(k(\underline{U}, \underline{S}))$. Thus, $\Theta(G, T)$ is a $*$-polynomial over $k(\underline{U}, \underline{S}, T)$ by (II.1) and (II.2), with Galois group A_n by (II.3).

Secondly, let L/K be a $(\widetilde{A_n} \xrightarrow{\pi} A_n)$-extension of fields containing k.

We can view L/K as the splitting field of some $*$-polynomial $f \in K[X]$ of degree n. Moreover, "Kuyk's Lemma" (see, e.g., [2, Lemma 3]) shows that the set of such polynomials is Zariski-dense in $\mathbb{A}^n(K)$.

Hence, we can assume that $(\Theta \circ (\Psi, \lambda))(f)$ is well-defined and equal to f, and that $\Psi(f)$ belongs to $W(K)$.

Then, $\Psi(f)$ is a $*$-polynomial over K of degree n by (II). Since $\Psi(f)$ belongs to $H(K)$, it must be $\Psi(f) = X.F_{\underline{s}}(\underline{v}; X)$, for some $\underline{v} \in K^m$ and $\underline{s} \in K^{n-1}$. This shows that f arises by specialization from $\Theta(G, T)$ at $(\underline{U}, \underline{S}, T) = (\underline{v}, \underline{s}, \lambda(f))$.

(ii) $\Rightarrow$ **(i)**.

This implication can be proved in a similar (but simpler) manner to the above one, and the details are left to the reader. We only mention that the equality $\Psi_{|H} = id_H$ in (III) can be used to show that, for a suitable generic polynomial F for $\widetilde{A_n} \xrightarrow{\pi} A_n$ over k, the polynomial $\frac{1}{X}\Psi(F)$ must be generic for $\widetilde{A_{n-1}} \xrightarrow{\pi} A_{n-1}$ over k.

□

In [13], Y. Rikuna gives a generic polynomial for $\mathrm{SL}_2(\mathbb{F}_3) \cong \widetilde{A_4}$ over $\mathbb{Q}$. We thus have

Theorem 3.2. *There exists a generic extension for* $\mathrm{SL}_2(\mathbb{F}_5) \cong \widetilde{A_5}$ *over* $\mathbb{Q}$.

Remark 3.3. In [12] we established the analogue of Thm. 3.1 for A_n (resp. A_{n-1}) instead of $\widetilde{A_n}$ (resp. $\widetilde{A_{n-1}}$). In fact, from [12], the following stronger result holds: for every faithful finite-dimensional linear representation V_n of A_n (n odd) over a field k of characteristic 0, the invariant fields $k(V_n)^{A_n}$ and $k(V_n)^{A_{n-1}}$ are *k-stably isomorphic*. We don't know, however, whether this remains valid when replacing A_n (resp. A_{n-1}) by $\widetilde{A_n}$ (resp. $\widetilde{A_{n-1}}$). If it were, then $\mathbb{Q}(\widetilde{V_5})^{\widetilde{A_5}}$ would be $\mathbb{Q}$-*stably rational* for every faithful finite-dimensional linear representation $\widetilde{V_5}$ of $\widetilde{A_5}$ over $\mathbb{Q}$. This is because $\mathbb{Q}(\widetilde{V_5})^{\widetilde{A_4}}$ is known to be $\mathbb{Q}$-stably rational by [13, Thm. 5.2]. What we have proved (Thm. 3.2) is that $\mathbb{Q}(\widetilde{V_5})^{\widetilde{A_5}}$ is $\mathbb{Q}$-*retract rational*. See, e.g., [15].

Let us finally note that Theorem 3.1 can be generalized as follows.

Theorem 3.4. *Let k be a field of characteristic 0. Let $n \geq 3$ be an odd positive integer and let G denote either the alternating group A_n or the symmetric group S_n. Let*

$$1 \to C \to \widetilde{G} \xrightarrow{\pi} G \to 1$$

be a finite central extension. Assume that there exists a generic extension for C over k. In the case $G = A_7$ assume, moreover, that 3 does not divide the order of C. Then, the following properties are equivalent:

(*i*) *There exists a generic extension for $\widetilde{G}$ over k.*
(*ii*) *There exists a generic extension for $\pi^{-1}(G \cap S_{n-1})$ over k.*

Proof. We first note that the result is immediate in the case $G = A_3$, $\widetilde{G}$ being abelian. So, from now on we assume $G \neq A_3$.

Note also that, if the given central extension splits, then the result is a direct consequence of [12] and the following fact: given finite groups G_1 and G_2, there exists a generic extension for $G_1 \times G_2$ over k if and only if so happens for both G_1 and G_2 (cf. [14, Thm. 1.5, Thm. 3.1]).

Now, we claim that Thm. 3.4 can be reduced to the case:

(*) C is a 2-group.

This reduction step, which is similar to [6, Thm. 6], can be proved as follows.

Let $\widetilde{G}'$ (resp. G') denote the derived subgroup of $\widetilde{G}$ (resp. G). Note that, since we excluded the case $G = A_3$, we have $G' = A_n$.

Let C_2 be the 2-Sylow subgroup of C, which we view as a subgroup of $\widetilde{G}$. One easily checks that it is possible to find an element $\tau \in \widetilde{G}$ such that $\tau^2 \in C_2$ and $< \pi(\tau) > \cdot G' = G$.

It is well-known that $C \cap \widetilde{G}'$ must be isomorphic to a subgroup of the Schur multiplier of G. Because of our extra hypothesis in the case $G = A_7$, it must be $C \cap \widetilde{G}' \subseteq C_2$. It follows that, if we define $\overline{G} := C_2 \cdot < \tau > \cdot \widetilde{G}'$, then $C \cap \overline{G} = C_2$. From this, a

complement C_0 of C_2 in C must be a (central) complement of $\overline{G}$ in $\widetilde{G}$. Hence, $\widetilde{G}$ is isomorphic to the direct product $C_0 \times \overline{G}$, and the claim is proved.

Finally, under assumption (*), Theorem 3.4 can be proved analogously to Theorem 3.1. The main point here is that, from [9] and [16, II.Annexe], it follows that in the proof of Theorem 3.1 one can replace property (II.2) by (II.2)+(II.2)', where

(II.2)' Let G be the Galois group of $\Theta(f,T)$ over $K(T)$ and let $L_T/K(T)$ denote the corresponding G-extension. Let $1 \to C \to \widetilde{G} \stackrel{\pi}{\to} G \to 1$ be a finite central extension. If 3 does not divide the order of C, then the embedding problem $(L_T/K(T), \pi)$ has constant obstruction.

□

Remark 3.5. It is obvious from the given proof that the extra hypothesis in the case $G = A_7$ can be replaced by the weaker assumption that 3 does not divide the order of $C \cap \widetilde{G}'$.

Remark 3.6. If $\widetilde{G}$ is a finite central extension of S_3, then $\pi^{-1}(S_2)$ is an abelian group which contains a 2-Sylow subgroup of $\widetilde{G}$. Hence, as a direct consequence of Thm. 3.4, there exists a generic extension for $\widetilde{G}$ over $\mathbb{Q}$ if and only if $\widetilde{G}$ does not contain an element of order 8.

Acknowledgements

Research partially supported by MCYT grant BFM2003-01898.

References

[1] F. DeMeyer and T. McKenzie, *On generic polynomials*, J. Algebra **261** (2003), no. 2, 327–333.
[2] F. R. DeMeyer, *Generic polynomials*, J. Algebra **84** (1983), no. 2, 441–448.
[3] V. V. Ishkhanov, B. B. Lur′e, and D. K. Faddeev, The embedding problem in Galois theory, Vol. 165 of *Translations of Mathematical Monographs*, American Mathematical Society, Providence, RI (1997), ISBN 0-8218-4592-6. Translated from the 1990 Russian original by N. B. Lebedinskaya.
[4] C. U. Jensen, A. Ledet, and N. Yui, Generic polynomials, Vol. 45 of *Mathematical Sciences Research Institute Publications*, Cambridge University Press, Cambridge (2002), ISBN 0-521-81998-9. Constructive aspects of the inverse Galois problem.
[5] G. Kemper, *Generic polynomials are descent-generic*, Manuscripta Math. **105** (2001), no. 1, 139–141.
[6] D. Kotlar, M. Schacher, and J. Sonn, *Central extensions of symmetric groups as Galois groups*, J. Algebra **124** (1989), no. 1, 183–198.
[7] W. Kuyk, *On a theorem of E. Noether*, Nederl. Akad. Wetensch. Proc. Ser. A 67 = Indag. Math. **26** (1964) 32–39.
[8] A. Ledet, *Generic extensions and generic polynomials*, J. Symbolic Comput. **30** (2000), no. 6, 867–872. Algorithmic methods in Galois theory.
[9] J.-F. Mestre, *Extensions régulières de* $\mathbf{Q}(T)$ *de groupe de Galois* $\widetilde{A}_n$, J. Algebra **131** (1990), no. 2, 483–495.
[10] ———, *Extensions génériques de groupe de Galois* $SL_2(\mathbb{F}_3)$ (2006). Preprint available at `arXiv:math.GR/0602320`.
[11] T. Miyata, *Invariants of certain groups. I*, Nagoya Math. J. **41** (1971) 69–73.
[12] B. Plans, *On the* $\mathbf{Q}$*-rationality of* $\mathbf{Q}(X_1, ..., X_5)^{A_5}$ (2005). Preprint.
[13] Y. Rikuna, *The existence of a generic polynomial for* $\mathrm{SL}(2,3)$ *over* $\mathbf{Q}$. Preprint.
[14] D. J. Saltman, *Generic Galois extensions and problems in field theory*, Adv. in Math. **43** (1982), no. 3, 250–283.

[15] ———, *Groups acting on fields: Noether's problem*, in Group actions on rings (Brunswick, Maine, 1984), Vol. 43 of *Contemp. Math.*, 267–277, Amer. Math. Soc., Providence, RI (1985).
[16] J.-P. Serre, Cohomologie galoisienne, Vol. 5 of *Lecture Notes in Mathematics*, Springer-Verlag, Berlin, fifth edition (1994), ISBN 3-540-58002-6.
[17] ———, *Cohomological invariants, Witt invariants, and trace forms*, in Cohomological invariants in Galois cohomology, Vol. 28 of *Univ. Lecture Ser.*, 1–100, Amer. Math. Soc., Providence, RI (2003). Notes by Skip Garibaldi.

Dept. de Matemàtica Aplicada I, Universitat Politècnica de Catalunya, Av. Diagonal, 647, 08028 Barcelona, Spain
E-mail address: bernat.plans@upc.edu