INSTITUT DE FRANCE
Académie des sciences

Comptes Rendus

Mathématique

Gil Alon, François Legrand and Elad Paran

Galois groups over rational function fields over skew fields

Volume 358, issue 7 (2020), p. 785-790.

<https://doi.org/10.5802/crmath.20>

Comptes Rendus
Mathématique
2020, 358, nº 7, p. 785-790
https://doi.org/10.5802/crmath.20

Number Theory / *Théorie des nombres*

Galois groups over rational function fields over skew fields

Gil Alon [a], **François Legrand** [b] **and Elad Paran** [*, a]

[a] Department of Mathematics and Computer Science, the Open University of Israel, Ra'anana 4353701, Israel

[b] Institut für Algebra, Fachrichtung Mathematik, TU Dresden, 01062 Dresden, Germany

E-mails: gilal@openu.ac.il, francois.legrand@tu-dresden.de, paran@openu.ac.il

Abstract. Let H be a skew field of finite dimension over its center k. We solve the Inverse Galois Problem over the field of fractions $H(X)$ of the ring of polynomial functions over H in the variable X, if k contains an ample field.

Résumé. Soit H un corps gauche de dimension finie sur son centre k. Nous résolvons le Problème Inverse de Galois sur le corps des fractions $H(X)$ de l'anneau des fonctions polynomiales en la variable X et à coefficients dans H, si k contient un corps ample.

Manuscript received 17th December 2019, accepted 28th May 2020.

1. Introduction

The Inverse Galois Problem over a field k asks whether every finite group occurs as the Galois group of a Galois field extension of k. Hilbert showed in 1892, via his celebrated irreducibility theorem, that this problem over the field $\mathbb{Q}$ of rational numbers is equivalent to the same problem over the field $\mathbb{Q}(t)$ of rational functions over $\mathbb{Q}$. While the problem is wide open over $\mathbb{Q}(t)$, it is known to have an affirmative answer over many other function fields, e.g., over the field $\mathbb{C}(t)$ of complex rational functions, as a consequence of Riemann's Existence Theorem.

The aim of this note is to contribute to inverse Galois theory over skew fields, following a first work on this topic by Deschamps and Legrand (see [4]). In this more general context, given skew fields (equivalently, division rings) $H \subseteq M$, the extension M/H is said to be *Galois* if every element of M which is fixed under any automorphism of M fixing H pointwise lies in H. See [3, Section 3.3] for more on Galois theory over skew fields.

Let H be a skew field, and let $H[X]$ denote the ring of all polynomial functions over H in the variable X. That is, $H[X]$ is the ring of all functions from H to H that can be expressed by sums

[*] Corresponding author.

and products of the variable X and elements of H. We observe that, if H is of finite dimension over its center k and if k is infinite, then $H[X]$ has a classical (right) field of fractions, denoted by $H(X)$. See Section 2 for more details.

In the sequel, we solve the Inverse Galois Problem over the skew field $H(X)$, if the center of H contains an ample field:

Theorem 1. *Let H be a skew field of finite dimension over its center k. If k contains an ample field, then every finite group is the Galois group of a Galois extension of $H(X)$.*

Recall that a field k is *ample* (or *large*) if every smooth geometrically irreducible k-curve has either zero or infinitely many k-rational points. Ample fields, which were introduced by Pop in [9] (and which are necessarily infinite), include algebraically closed fields, some complete valued fields (e.g., $\mathbb{Q}_p, \mathbb{R}, \kappa((T))$), the field $\mathbb{Q}^{\mathrm{tr}}$ of all totally real algebraic numbers, etc. See [7], [2], and [10] for more details. Consequently, a special (but fundamental) case of Theorem 1 is that the Inverse Galois Problem has an affirmative answer over $\mathbb{H}(X)$, where $\mathbb{H}$ denotes the skew field of Hamilton's quaternions.

Given a skew field H of finite dimension over its center k, with k infinite, the ring $H[X]$ is one possible natural generalization of the usual polynomial ring in one variable over an infinite field. Another one is the polynomial ring $H_c[t]$, where t is a central indeterminate, commuting with the coefficients[1] [2]. While these rings are isomorphic in the special case $H = k$, it is not clear that such an isomorphism exists if H is non-commutative. This suggests that the Inverse Galois Problem over the field of fractions $H_c(t)$ of $H_c[t]$, which is studied by Deschamps and Legrand, and the same problem over $H(X)$ are a priori independent. In particular, although the Inverse Galois Problem over $H_c(t)$ has a positive answer if k contains an ample field (see [4, Théorème B]), Theorem 1 has its own merits and, as [4, Théorème B], extends the deep result of Pop solving the Inverse Galois Problem over the field $k(t)$, if k contains an ample field.

We prove Theorem 1 in Section 3, by reducing it to the case settled by Deschamps and Legrand. The main observation needed is that the ring $H[X]$ is isomorphic to the ring $H_c[t_1,\dots,t_n]$ of polynomials over H in n central variables, where n denotes the dimension of H over its center (see Proposition 4). This follows from a theorem of Wilczynski [12, Theorem 4.1]. We also make use of the general observation that the Inverse Galois Problem over skew fields is "algebraic"; see Proposition 6.

2. Polynomial rings and fields of fractions

2.1. *Polynomial rings*

For this subsection, let H be a skew field.

The *polynomial ring* $H_c[t]$ in the *central* variable t is the set of all sequences $(a_n)_{n\in\mathbb{N}}$ of elements of H such that $a_n = 0$ for all but finitely many n. As in the commutative setting, the addition is defined componentwise and the multiplication is defined by $(a_n)_n \cdot (b_n)_n = (c_n)_n$, where $c_n = \sum_{l+m=n} a_l b_m$ for every $n \in \mathbb{N}$. Setting $(a_n)_n = \sum_n a_n t^n$, one has $at = ta$ for every $a \in H$, thus justifying the terminology "central". If H is a field, then $H_c[t]$ is nothing but the usual polynomial ring in the variable t over H. In the sense of Ore [8], $H_c[t]$ is the skew polynomial ring

[1] We adopt a different notation from that of [4], where this ring is denoted by $H[t]$, in order to distinguish between the cases of central variables and non-central ones. We note that there are alternative notations for this ring in the literature, such as $H[x,\mathrm{id},0]$ in [8], or $H_L[t]$ in [6].

[2] Throughout this note, we use upper-case letters to denote non-central variables and lower case-letter to denote central ones, to add a visual distinction between the two.

$H[t,\alpha,\delta]$ in the variable t, where the automorphism α is the identity of H and the derivation δ is 0. One can iteratively construct rings of polynomials in several central variables over H, by putting $H_c[t_1,t_2] = (H_c[t_1])_c[t_2]$, $H_c[t_1,t_2,t_3] = (H_c[t_1,t_2])_c[t_3]$, and so on. Since the variables are all central, the order in which they are added does not change the ring obtained, up to isomorphism.

On the other hand, let $H\langle X\rangle$ be the free algebra in one symbol X over H. That is, $H\langle X\rangle$ is the algebra spanned by all words whose letters are elements of H or X. For an element $a \in H$ and $f(X) \in H\langle X\rangle$, the substitution $f(a) \in H$ is defined in the obvious way, by replacing each occurrence of X in $f(X)$ by a, and computing the resulting value in H. For a fixed $a \in H$, the map $f(X) \mapsto f(a)$ is a homomorphism from $H\langle X\rangle$ to H. We say that f *vanishes* at a if $f(a) = 0$. Let I be the (two-sided) ideal of $H\langle X\rangle$ which consists of all $f(X) \in H\langle X\rangle$ that vanish at all $a \in H$. Then the ring $H[X]$ is defined as the quotient $H\langle X\rangle/I$, and it is isomorphic to the ring of polynomial functions over H. Note that, if H is an infinite field, then this definition coincides with the usual definition of the polynomial ring in the variable X over H.

2.2. *Classical fields of fractions*

For this subsection, let R be a non-zero ring, not necessarily commutative. Recall that R is an *integral domain* if, for all $r \in R\setminus\{0\}$ and $s \in R\setminus\{0\}$, one has $sr \neq 0$ and $rs \neq 0$. From now on, suppose R is an integral domain.

A *classical right quotient ring for R* is an overring $S \supseteq R$ such that every non-zero element of R is invertible in S, and such that every element of S can be written as ab^{-1} for some $a \in R$ and some $b \in R\setminus\{0\}$. We say that R is a *right Ore domain* if, for all non-zero elements x and y of R, there exist r and s in R such that $xr = ys \neq 0$. By [5, Theorem 6.8], if R is a right Ore domain, then R has a classical right quotient ring H which is a skew field and, by [3, Proposition 1.3.4], H is unique up to isomorphism. We then say that H is the *classical right field of fractions* of R.

If H denotes an arbitrary skew field, then the polynomial ring $H_c[t]$ in the central variable t over H is an integral domain, since the degree is additive on products. Moreover, $H_c[t]$ is a right Ore domain, by [5, Theorem 2.6 and Corollary 6.7]. By an easy induction, given a positive integer n, the polynomial ring $H_c[t_1,\dots,t_n]$ in n central variables over H has a classical right field of fractions, which we denote by $H_c(t_1,\dots,t_n)$.

Proposition 2. *Let H be a skew field and $n \geq 2$. Then the equality $H_c(t_1,\dots,t_n) = (H_c(t_1,\dots,t_{n-1}))_c(t_n)$ holds.*

Proof. First, it is clear that the inclusion $H_c[t_1,\dots,t_n] \subseteq (H_c(t_1,\dots,t_{n-1}))_c(t_n)$ holds. As every element of $H_c(t_1,\dots,t_n)$ can be written as fg^{-1} with f and g in $H_c[t_1,\dots,t_n]$, we actually have $H_c(t_1,\dots,t_n) \subseteq (H_c(t_1,\dots,t_{n-1}))_c(t_n)$.

For the converse, take a polynomial $f = \sum_{l=0}^{m} a_l t_n^l$ with $a_l \in H_c(t_1,\dots,t_{n-1})$ for every $l \in \{0,\dots,m\}$. As before, we can write $a_l = b_l c_l^{-1}$ with $b_l \in H_c[t_1,\dots,t_{n-1}]$ and $c_l \in H_c[t_1,\dots,t_{n-1}]\setminus\{0\}$, for every $l \in \{0,\dots,m\}$. Since $H_c[t_1,\dots,t_{n-1}] \subseteq H_c[t_1,\dots,t_n] \subseteq H_c(t_1,\dots,t_n)$ and $t_n \in H_c(t_1,\dots,t_n)$, we get that $f = \sum_{l=0}^{m} b_l c_l^{-1} t_n^l$ is in $H_c(t_1,\dots,t_n)$. This shows the desired inclusion $(H_c(t_1,\dots,t_{n-1}))_c(t_n) \subseteq H_c(t_1,\dots,t_n)$, since every element of $(H_c(t_1,\dots,t_{n-1}))_c(t_n)$ can be written as fg^{-1} with f and g in $(H_c(t_1,\dots,t_{n-1}))_c[t_n]$. $\square$

Proposition 3. *Let H be a skew field of center k and let n be a positive integer. The center of $H_c(t_1,\dots,t_n)$ equals $k(t_1,\dots,t_n)$. Moreover, if the dimension of H over k is finite, then the equality $\dim_{k(t_1,\dots,t_n)} H_c(t_1,\dots,t_n) = \dim_k H$ holds.*

Proof. By, e.g., [3, Proposition 2.1.5], if K is an arbitrary skew field of center C, then $C(t)$ is the center of $K_c(t)$. Hence, by iterating Proposition 2, the center of $H_c(t_1,\dots,t_n)$ equals $k(t_1,\dots,t_n)$. Now, suppose $\dim_k H$ is finite. Then, by [4, Proposition 9], we have $H_c(t_1) \cong H \otimes_k k(t_1)$. Consequently, $\dim_{k(t_1)} H_c(t_1)$ is finite and equals $\dim_k H$. As before, it remains to iterate Proposition 2 to conclude the proof. □

Proposition 4. *Let H be a skew field of finite dimension n over its center k. Assume k is infinite. Then the ring $H[X]$ is isomorphic to $H_c[t_1,\dots,t_n]$.*

Proof. The existence of such an isomorphism follows from [12, Theorem 4.1]. See also [1, Theorem 5] for a different, more explicit proof. For the convenience of the reader, we include an elementary proof in the special case $H = \mathbb{H}$, where $\mathbb{H}$ is the skew field of Hamilton's quaternions.

One has the following classical identity for each $a \in \mathbb{H}$:

$$\mathrm{Re}(a) = \frac{1}{4}(a - iai - jaj - kak),$$

where $\mathrm{Re}(a)$ is the real component of a. More generally, putting

$$\begin{aligned} y_1 &= \frac{1}{4}(X - iXi - jXj - kXk), \\ y_2 &= \frac{1}{4}(jXk - Xi - iX - kXj), \\ y_3 &= \frac{1}{4}(kXi - Xj - jX - iXk), \\ y_4 &= \frac{1}{4}(iXj - Xk - kX - jXi), \end{aligned}$$

the functions $y_1, y_2, y_3, y_4 \in \mathbb{H}[X]$ obtain real values only, and one has $X = y_1 + iy_2 + jy_3 + ky_4$. In particular, y_1, y_2, y_3, y_4 belong to the center of $\mathbb{H}[X]$, and we may then define a homomorphism $\phi\colon \mathbb{H}_c[t_1,t_2,t_3,t_4] \to \mathbb{H}[X]$ by $\phi(t_l) = y_l$, $1 \le l \le 4$, and $\phi(a) = a$ for all $a \in \mathbb{H}$. The equality $X = y_1 + iy_2 + jy_3 + ky_4$ implies that ϕ is surjective.

Let $p = p(t_1,t_2,t_3,t_4) \in \mathbb{H}_c[t_1,t_2,t_3,t_4]$. By decomposing the coefficients of p into their real, i, j, and k components, we may present p in the form $p = p_1 + p_2 i + p_3 j + p_4 k$ with $p_1,p_2,p_3,p_4 \in \mathbb{R}[t_1,t_2,t_3,t_4]$. If $p \neq 0$, then $p_l \neq 0$ for some $1 \le l \le 4$. Then there exists a non-zero tuple $a = (a_1,a_2,a_3,a_4) \in \mathbb{R}^4$ such that $p_l(a) \neq 0$. Hence, $\phi(p)$ does not vanish at $X = a_1 + a_2 i + a_3 j + a_4 k$, thus showing that ϕ is also injective. □

Corollary 5. *Let H be a skew field of finite dimension n over its center k. Assume k is infinite. Then the ring $H[X]$ has a classical right field of fractions, denoted by $H(X)$, which is isomorphic to $H_c(t_1,\dots,t_n)$.*

Proof. As recalled, the ring $H_c[t_1,\dots,t_n]$ is a right Ore domain. Since $H[X]$ is isomorphic to $H_c[t_1,\dots,t_n]$ by Proposition 4, $H[X]$ is also a right Ore domain and so has a classical right field of fractions. Finally, [3, Section 1.3] shows that the isomorphism $H[X] \cong H_c[t_1,\dots,t_n]$ from Proposition 4 extends to an isomorphism $H(X) \cong H_c(t_1,\dots,t_n)$. □

3. Proof of Theorem 1

We first make the general observation that the Inverse Galois Problem over skew fields is an "algebraic problem". More precisely:

Proposition 6. *Let H_1 and H_2 be isomorphic skew fields and let G be a finite group. Then there exists a Galois extension of H_1 of group G if and only if there exists a Galois extension of H_2 of group G.*

Proof. Let $\varphi : H_1 \to H_2$ be an isomorphism. Suppose there exists a Galois extension K_1/H_1 of group G.

By the exchange principle[3], there exists a set C such that $C \cap H_2 = \emptyset$ and $|C| = |K_1 \setminus H_1|$. Let $f : K_1 \setminus H_1 \to C$ be a bijection. Then set $K_2 = C \cup H_2$ and consider the well-defined map $\psi : K_1 \to K_2$ given by $\psi(x) = \varphi(x)$ if $x \in H_1$ and $\psi(x) = f(x)$ if $x \in K_1 \setminus H_1$. The map ψ is surjective and, as $C \cap H_2 = \emptyset$, it is also injective. Now, define the ring operations on K_2 as inherited from K_1 via ψ:

$$\forall\, x, y \in K_2,\ x \cdot y = \psi(\psi^{-1}(x) \cdot \psi^{-1}(y)),\ x + y = \psi(\psi^{-1}(x) + \psi^{-1}(y)).$$

Then K_2 is isomorphic to K_1 via ψ and, in particular, K_2 is a skew field containing H_2.

It remains to show that K_2/H_2 is Galois of group G. To that end, note that the isomorphism $\psi : K_1 \to K_2$, whose restriction to H_1 equals φ, induces an isomorphism $\phi : \mathrm{Aut}(K_1/H_1) \to \mathrm{Aut}(K_2/H_2)$ (namely, $\phi(\sigma) = \psi \circ \sigma \circ \psi^{-1}$ for every $\sigma \in \mathrm{Aut}(K_1/H_1)$). Finally, if x is any element of K_2 such that $\sigma(x) = x$ for every $\sigma \in \mathrm{Aut}(K_2/H_2)$, then we have $\tau(\psi^{-1}(x)) = \psi^{-1}(x)$ for every $\tau \in \mathrm{Aut}(K_1/H_1)$. As K_1/H_1 is Galois, we then have $\psi^{-1}(x) \in H_1$, and so $x \in H_2$, thus showing that K_2/H_2 is Galois. This concludes the proof. □

Proof of Theorem 1. By Corollary 5, we have $H(X) \cong H_c(t_1, \ldots, t_n)$, where n denotes the dimension of H over k. Moreover, by Proposition 3, the center of $H_c(t_1, \ldots, t_{n-1})$ equals $k(t_1, \ldots, t_{n-1})$ and the dimension of $H_c(t_1, \ldots, t_{n-1})$ over $k(t_1, \ldots, t_{n-1})$ is finite. Finally, $k(t_1, \ldots, t_{n-1})$ contains an ample field. Hence, by [4, Théorème B], the Inverse Galois Problem has an affirmative answer over the skew field $(H_c(t_1, \ldots, t_{n-1}))_c(t_n)$, that is, over $H_c(t_1, \ldots, t_n)$ by Proposition 2. It then remains to apply Proposition 6 to get that the Inverse Galois Problem also has an affirmative answer over $H(X)$, thus concluding the proof. □

Remark 7. Similarly, we have this result, which follows from [4, Proposition 12] as Theorem 1 follows from [4, Théorème B]:

Let G be a finite group and H a skew field of finite dimension n over its center k. In each of the following cases, G occurs as the Galois group of a Galois extension of $H(X)$:

(1) *G is abelian and k is infinite,*
(2) *$G = S_m$ $(m \geq 3)$ and k is infinite,*
(3) *$G = A_m$ $(m \geq 4)$ and k has characteristic zero,*
(4) *G is solvable, $n \geq 2$, and k has positive characteristic.*

References

[1] G. Alon, E. Paran, "A quaternionic Nullstellensatz", *J. Pure Appl. Algebra* **225** (2020), no. 4, article ID 106572.

[2] L. Bary-Soroker, A. Fehm, "Open problems in the theory of ample fields", in *Geometric and differential Galois theories*, Séminaires et Congrès, vol. 27, Société Mathématique de France, 2013, p. 1-11.

[3] P. M. Cohn, *Skew fields. Theory of general division rings*, Encyclopedia of Mathematics and Its Applications, vol. 57, Cambridge University Press, 1995, xvi+500 pages.

[4] B. Deschamps, F. Legrand, "Le problème inverse de Galois sur les corps des fractions tordus à indéterminée centrale", *J. Pure Appl. Algebra* **224** (2020), no. 5, article ID 106240 (13 pages).

[5] K. R. Goodearl, R. B. Warfield, Jr., *An Introduction to noncommutative Noetherian rings*, 2nd ed., London Mathematical Society Student Texts, vol. 61, Cambridge University Press, 2004, xxiv+344 pages.

[6] B. Gordon, T. S. Motzkin, "On the zeros of polynomials over division rings", *Trans. Am. Math. Soc.* **116** (1965), p. 218-226.

[7] M. Jarden, *Algebraic patching*, Springer Monographs in Mathematics, Springer, 2011, xxiv+290 pages.

[8] O. Ore, "Theory of non-commutative polynomials", *Ann. Math.* **34** (1933), no. 3, p. 480-508.

[9] F. Pop, "Embedding problems over large fields", *Ann. Math.* **144** (1996), no. 1, p. 1-34.

[3] which asserts that, given two sets A and B, there exists a set C such that $A \cap C = \emptyset$ and $|C| = |B|$ (see, e.g., [11, p. 31]).

[10] ———, "Little survey on large fields - old & new", in *Valuation theory in interaction*, EMS Series of Congress Reports, European Mathematical Society, 2014, p. 432-463.
[11] R. L. Vaught, *Set theory. An introduction*, 2nd ed., Birkhäuser, 1995, x+167 pages.
[12] D. M. Wilczynski, "On the fundamental theorem of algebra for polynomial equations over real composition algebras", *J. Pure Appl. Algebra* **218** (2014), no. 7, p. 1195-1205.