Descent for differential modules and skew fields

Mark van Hoeij* and Marius van der Put**

*Department of Mathematics, Florida State University
Tallahassee, FL 32306, USA.
email: hoeij@math.fsu.edu

**Department of Mathematics, University of Groningen
P.O.Box 800, 9700 AV Groningen, The Netherlands
email: mvdput@math.rug.nl

Abstract. In this paper we study rationality questions for differential modules and differential operators. If a differential operator L is equivalent to its conjugates over k, is it then equivalent to an operator defined over k? We will show how counter examples to this question correspond to skew fields, and will make this correspondence explicit in both directions. Similar questions are studied for projective equivalence of differential operators. The main tool is the study of differential modules over skew fields.

1 Introduction

Let K/k be a Galois extension of differential fields of characteristic 0. The skew ring of differential operators over K is denoted by $\mathcal{D} := K[\partial]$. An element σ in the Galois group $\mathrm{Gal}(K/k)$ acts on $\mathcal{D}$ by $\sigma(\sum a_i\partial^i) = \sum \sigma(a_i)\partial^i$. The *conjugates* of an element $L \in \mathcal{D}$ are the operators $\sigma(L)$. The *order* of L is the degree in ∂. If $L \in k[\partial]$ then L is called *rational*. Two operators

*Supported by NSF grant 0098034.

L_1, L_2 are called *equivalent* (or of the *same type*) if the two differential modules $\mathcal{D}/\mathcal{D}L_i,\ i = 1,2$ are isomorphic. The operators are called *projectively equivalent* if there exists a $\mathcal{D}$-module E of dimension 1 over K such that $\mathcal{D}/\mathcal{D}L_1 \cong E \otimes \mathcal{D}/\mathcal{D}L_2$.

Abbreviations:

R	Rational, i.e. element of $k[\partial]$.
$\mathrm{E_R}$	Equivalent to an element of $k[\partial]$.
$\mathrm{E_C}$	Equivalent to all its conjugates over k.
$\mathrm{E_R^p}$	Projectively equivalent to an element of $k[\partial]$.
$\mathrm{E_C^p}$	Projectively equivalent all its conjugates over k.

The following implications are obvious:

$$\mathrm{R} \Longrightarrow \mathrm{E_R} \Longrightarrow (\mathrm{E_C} \wedge \mathrm{E_R^p}), \qquad (\mathrm{E_C} \vee \mathrm{E_R^p}) \Longrightarrow \mathrm{E_C^p}.$$

These implications leave seven possible combinations for the truth-values of R,$\mathrm{E_R}$,$\mathrm{E_C}$,$\mathrm{E_R^p}$,$\mathrm{E_C^p}$. In case $k = \mathbf{Q}(x)$ and $K = \overline{\mathbf{Q}}(x)$, all seven cases occur. The examples, given in the table below, are irreducible in $\mathcal{D}$.

Case	R	$\mathrm{E_R}$	$\mathrm{E_C}$	$\mathrm{E_R^p}$	$\mathrm{E_C^p}$	Example
1	Y	Y	Y	Y	Y	∂
2	N	Y	Y	Y	Y	$\partial - 1/(x-i)$
3	N	N	Y	Y	Y	$(x^2+1)\partial^2 + (2x+i)\partial + 1$
4	N	N	Y	N	Y	$\partial^2 + x^2 + 1 + i$
5	N	N	N	Y	Y	$\partial + i$
6	N	N	N	N	Y	$4x\partial^2 - 2\partial + x^2 + x + i$
7	N	N	N	N	N	$\partial^2 + i$

Cases 1, 5, and 7 are not of interest. Further, [H] p. 101/102 contains already an example of a second order operator $R_{s,t}$ for which computer computations show that $R_{s,t}$ is $\mathrm{E_C}$ but not $\mathrm{E_R}$. The table can be verified by computer computations, however, this would not explain the underlying mathematics nor where these examples come from. That is the main theme of this paper.

Denote C_K resp. C_k as the field constants of K resp. k. Suppose that $K = C_K(x)$ and $k = C_k(x)$ with differentiation $\frac{d}{dx}$. Then $\mathrm{E_C}$ without $\mathrm{E_R}$ (case 3 or 4) is related to skew fields F^o of finite dimension over their center C_k. Any such skew field yields examples for $\mathrm{E_C}$ without $\mathrm{E_R}$. Case 6 also corresponds to a skew field F, this time of finite dimension over its center k. For second order equations this skew field is a quaternion field and corresponds to a conic over k. All skew fields of this type (all non-degenerate conics) are shown to produce examples for case 6. For most of our constructions it will be more convenient to use modules instead of operators.

In section 2, one considers a differential module M over K which is isomorphic to all its conjugates ${}^{\sigma}M$ under the Galois group of K/k. The question is whether M descends to k, i.e., $M \cong K \otimes_k N$ for some differential module N over k. The answer is positive for a formal Laurent series field K, see theorem 2.4. For function fields K in one variable, e.g., $K = C_K(x)$ and $k = C_k(x)$, the obstruction to descent is a 2-cocycle, which is related to a skew field F^o of finite dimension over its center C_k. The introduction of skew differential fields, and differential modules over these, produces the examples for cases 3 and 4. For completeness, Amitsur's totally different construction is illustrated as well.

The main problem treated in section 3 is whether a differential module M over K of dimension 3 is the second symmetric power of a differential module of dimension 2 over K. Again rationality problems, 2-cocycles, quaternion fields over k with a differentiation and conics enter the picture. The constructions in section 3 are explained in section 4, where the notion of projective equivalence is studied in detail.

We would like to thank J.-A. Weil and E. Compoint for sharing their ideas in [C-W].

2 The Descent problem

2.1 Twists and descent data

Let $K \supset k$ denote two fields and let M be some object over K. The *descent problem* asks for an object N over k such that $K \otimes_k N$ is isomorphic to M. We are interested in the case where M and N are differential modules. We start with definitions and notations.

Definitions 2.1 *The twist ${}^{\sigma}V$ of a vector space V.*
Let K be a field and σ an automorphism of K. For any vector space V over K one associates a vector space ${}^{\sigma}V$ which is equal to V as additive group and has a new scalar multiplication defined by $\lambda * v := \sigma(\lambda)v$ for all $\lambda \in K$ and $v \in V$. For any K-linear map $f : V \to W$ between K-vector spaces one denotes by ${}^{\sigma}f : {}^{\sigma}V \to {}^{\sigma}W$ the same map f, which is K-linear for the

new structures. In this way, one has defined a functor from the category of the K-vector spaces to itself. This functor commutes with tensor products, exterior powers, symmetric powers, et cetera.

Let V, W be K-vector spaces and let σ be an automorphism of K. The map $f : V \to W$ is called *σ-linear* if f is additive and $f(\lambda v) = \sigma(\lambda)f(v)$ for all $\lambda \in K$, $v \in V$. To a linear map $f : V \to {}^{\sigma}W$ we associate a σ-linear map $F : V \to W$ by composing f with the set-theoretic identity ${}^{\sigma}W \to W$.

Observation: Let $K \supset k$ be a finite Galois extension with Galois group G. *Let V be a vector space over K. Then the K-vector space $K \otimes_k V$ is naturally isomorphic to $\oplus_{\sigma \in G}\, {}^{\sigma}V$.*

Indeed, consider $K \otimes_k K$ with the right structure of K-algebra given by the morphism $f \mapsto 1 \otimes f$ from K to $K \otimes_k K$. Then $K \otimes_k V \cong (K \otimes_k K) \otimes_K V$. Consider the isomorphism $\phi : K \otimes_k K \to \oplus_{\sigma \in G} K_\sigma$, where each K_σ is a copy of K, and ϕ is given by $\phi(a \otimes b) = (\sigma(a)b)_{\sigma \in G}$. Then ϕ is a K-algebra homomorphism. The left K-algebra structure on $K \otimes_k K$ is given by $f \in K \mapsto f \otimes 1 \in K \otimes_k K$. For this left structure one has that $K \otimes_k K$ is isomorphic to $\oplus_{\sigma \in G}\, {}^{\sigma}K$. Finally ${}^{\sigma}K \otimes_K V$ is isomorphic to ${}^{\sigma}V$.

2.2 The descent problem. *The basic situation and descent data.*

(1) k is a differential field of characteristic zero. Its algebraic closure will be denoted by $\overline{k}$. Let $K \subset \overline{k}$ be a Galois extension (finite or infinite) of k. Then K is also a differential field. The action of the Galois group G of K/k commutes with differentiation on K. Let $\mathcal{D} := K[\partial]$ denote the skew ring of the differential operators over the field K. A *differential module* over K is a left $\mathcal{D}$-module, of finite dimension as vector space over K. Let M be a differential module over K. For $\sigma \in G$ one defines the twist ${}^{\sigma}M$ of M as follows: The $K[\partial]$-module ${}^{\sigma}M$ is M as additive group, has a new scalar multiplication as defined in 2.1 and has the same operator ∂.

The action of G on K is extended to an action on $\mathcal{D}$ by imposing $\sigma(\partial) = \partial$ for all $\sigma \in G$. As usual, one associates to a monic differential operator $L \in \mathcal{D}$ the differential module $M = \mathcal{D}/\mathcal{D}L$. For $\sigma \in G$ one has that ${}^{\sigma}M$ is the differential module associated to $\sigma^{-1}(L)$.

(2) *Descent data* for M are given by:

(i) for every $\sigma \in G$ an isomorphism $\phi(\sigma) : M \to {}^{\sigma}M$ of differential modules,
(ii) satisfying $\Phi(\sigma)\Phi(\tau) = \Phi(\sigma\tau)$ for all $\sigma, \tau \in G$.

Here $\Phi(\sigma) : M \to M$ is the σ-linear map associated to $\phi(\sigma)$. See (3) below for a translation in terms of matrices.

Observation: Suppose that $K \supset k$ is a finite Galois extension. By the observation of 2.1 one has that $K \otimes_k M = (K \otimes_k K) \otimes_K M \cong \oplus_{\sigma \in G} {}^{\sigma}M$ (using the right K-algebra structure of $K \otimes_k K$ in the tensor product and the left K-algebra structure for the final object). This leads to an equivalent formulation of (i), namely:
Let $N_l := (K \otimes_k K) \otimes_K M$ and $N_r := (K \otimes_k K) \otimes_K M$ denote the two tensor products w.r.t. the left and the right structure (thus N_r is equal to the $K \otimes_k M$ above). Then there exists a $K \otimes_k K$-linear isomorphism $\phi : N_l \to N_r$ which commutes with ∂.
Condition (ii) has a translation involving $K \otimes_k K \otimes_k K$.

(3) One says that M *descends to* k if there exists a differential module N over k such that M is isomorphic to $K \otimes_k N$. If M descends to k, then M has obviously descent data.
On the other hand, let descent data for M be given. Choose a basis $m_1, \ldots, m_n$ of M over K. This also provides a basis for ${}^{\sigma}M$ using the set-theoretic identity. Let $b(\sigma)$ denote the matrix of $\phi(\sigma)$ w.r.t. this basis. Then condition (ii) translates into:

(ii) $\quad b(\sigma\tau) = b(\sigma)\ \sigma(b(\tau))$

in other words $\sigma \mapsto b(\sigma)$ is a 1-cocycle for G and $\mathrm{GL}_n(K)$. It is well known that $H^1(G, \mathrm{GL}_n(K))$ is trivial (see [S]) and that this implies that there exists a K-basis $\tilde{m}_1, \ldots, \tilde{m}_n$ of M such that the matrices $\tilde{b}(\sigma)$ of $\phi(\sigma)$ w.r.t. this new basis are 1. Let $N = k\tilde{m}_1 \oplus \cdots \oplus k\tilde{m}_n$. Then N is a differential module over k (since the $\phi(\sigma)$ commute with ∂) and the natural map $K \otimes_k N \to M$ is an isomorphism of differential modules. In other words, M descends to k.

(4) In the sequel we will study the situation where only the first part of the descent data is given, i.e., for a differential module M over K a collection of isomorphisms $\{\phi(\sigma) : M \to {}^{\sigma}M\}$ is given. The *descent problem* is to decide whether M descends to k or, more generally, to find the differential fields ℓ (say with $K \supset \ell \supset k$) such that M descends to ℓ. This problem can be stated for differential operators as follows:
Assume that L is $\mathrm{E_C}$ (see abbreviations in section 1), is L also $\mathrm{E_R}$?

(5) For any algebraic extension of differential fields $K \supset k$ one can also define descent data and a weak form of descent data, as in (4), for a differential module over K. Let K_c denote the normal closure of K. Then these data translate into data for $N := K_c \otimes_K M$ w.r.t. the Galois extension K_c/k and

with the additional information that N descends to K. Therefore we will restrict ourselves to Galois extensions. $\square$

We start with a useful lemma. Consider an algebraic extension of differential fields $k \subset K$, obtained by *extension of constants*, and a differential module M over K which descends to k. Then, by part (a) of the lemma, the module N over k with $K \otimes_k N \cong M$ is unique up to isomorphism.

Lemma 2.3 *Consider an algebraic extension of differential fields $k \subset K$, with fields of constants C_k, C_K. Suppose that $K = C_K \cdot k$.*
(a) *Let M_1, M_2 be differential modules over K, which descend to modules N_1, N_2 over k. Then*

$$\mathrm{Hom}_{K[\partial]}(M_1, M_2) = C_K \otimes_{C_k} \mathrm{Hom}_{k[\partial]}(N_1, N_2).$$

Furthermore, if $M_1 \cong M_2$, then $N_1 \cong N_2$ (uniqueness of descent).
(b) *Let N be a differential module over k and put $M = K \otimes_k N$. If the group of differential automorphisms of N is C_k^*, then $\mathrm{Hom}_{k[\partial]}(N, N) = C_k$, and $\mathrm{Hom}_{K[\partial]}(M, M) = C_K$. Moreover the group of the differential automorphisms of M is C_K^*.*

Proof. (a) Let $W := \mathrm{Hom}_{k[\partial]}(N_1, N_2)$ denote the C_k-vector space of the differential homomorphisms between the two differential modules over k. The natural C_K-linear map $C_K \otimes W \to \mathrm{Hom}_{K[\partial]}(M_1, M_2)$ is a bijection. Indeed, let $\mathbf{1}$ denote the trivial differential module of dimension one over k. Then $\mathrm{Hom}_{k[\partial]}(N_1, N_2) \cong \mathrm{Hom}_{k[\partial]}(\mathbf{1}, N_1^* \otimes N_2)$ and the latter is the space $\{a \in N_1^* \otimes N_2 |\ \partial a = 0\}$ of the "rational solutions" of the differential module $N_1^* \otimes N_2$. Similarly, $\mathrm{Hom}_{K[\partial]}(M_1, M_2)$ is the space of the rational solutions of $M_1^* \otimes M_2 = K \otimes_k (N_1^* \otimes N_2)$. The bijectivity follows now from [P-S], chapter 4, proposition 4.3. Consider a basis $w_1, \ldots, w_d$ of W. There is a polynomial $h \in K[X_1, \ldots, X_d]$ (the determinant of $\sum X_i w_i$ w.r.t. any bases for N_1, N_2) such that the set $\{(\lambda_1, \ldots, \lambda_d) \in C_K^d |\ \sum_i \lambda_i w_i$ is an isomorphism$\}$ is given by $h(\lambda_1, \ldots, \lambda_d) \neq 0$. This implies that some $w \in W$ induces an isomorphism between M_1 and M_2. Then w is an isomorphism between N_1 and N_2.
(b) Put $E := \mathrm{Hom}_{k[\partial]}(N, N)$. This is a finite dimensional algebra over C_k with basis $e_1, \ldots, e_d$. For any $e = \sum \lambda_i e_i$ one writes $\det(e)$ for the determinant of the matrix of left multiplication by e on N. This is a polynomial in $\lambda_1, \ldots, \lambda_d$. The automorphisms of N are the elements $e \in E$ with $\det(e) \neq 0$. The assumption that this group is C_k^* implies that $E = C_k$. Then, as in (a), $\mathrm{Hom}_{K[\partial]}(M, M) = C_K$ and the group of the automorphisms of M is C_K^*. $\square$

Theorem 2.4 *Let C_K/C_k be a finite Galois extension with group G. Consider the differential fields $k = C_k((x))$ and $K = C_K((x))$ with differentiation $x\frac{d}{dx}$. Suppose that the differential module M over K has the properties:*
(a) *M is irreducible and* (b) *${}^{\sigma}M$ is isomorphic to M for all $\sigma \in G$.*
Then M descends to k.

Proof. The proof is based on the classification of irreducible differential modules over K as given in the thesis [So] of R. Sommeling. The relevant information is the following:
(1) One associates to $Q \in \cup_{m\geq 1}\overline{C_K}[x^{-1/m}]$ the one dimensional differential module $K(Q)e$ over the finite field extension $K(Q)$ of K, given by $\partial e = Qe$ (recall that ∂ now refers to $x\frac{d}{dx}$ instead of $\frac{d}{dx}$). Then $K(Q)e$, viewed as a differential module over K, will be denoted as $E(Q)$. It is irreducible and has dimension $[K(Q) : K]$.
(2) Every irreducible differential module over K is obtained in this way.
(3) $E(Q_1) \cong E(Q_2)$ if and only if there exists a τ in the Galois group of $\overline{K}/K$ such that $\tau(Q_1) - Q_2 \in \frac{1}{r}\mathbf{Z}$, where r is the ramification index of $K(Q_1)/K$ (or equivalently the ramification index of $K(Q_2)/K$).

One associates to Q (as above) its monic minimal polynomial $f_Q \in K[T]$ over K. Then (3) translates into ([So], Proposition 3.3.6):
(3') $E(Q_1) \cong E(Q_2)$ if and only if there is a $\lambda \in \frac{1}{r}\mathbf{Z}$, where r is the ramification index of $K(Q_1)/K$, such that $f_{Q_1}(T) = f_{Q_2}(T + \lambda)$.

Now suppose that M satisfies (a) and (b). Choose a $Q \in \overline{C_K}[x^{-1/r}]$ with $r \geq 1$ minimal, such that $M \cong K(Q)e$. Let $f_M = f_Q \in K[T]$ be the minimal monic polynomial of Q over K. Take $\sigma \in \mathrm{Gal}(C_K/C_k) = \mathrm{Gal}(K/k)$ and extend σ to an automorphism $\tilde{\sigma}$ of $\overline{K}/k$. Then ${}^{\tilde{\sigma}}M$ is seen to be associated to $\tilde{\sigma}Q$. Therefore $f_{{}^{\sigma}M} = \sigma(f_M)$. Thus ${}^{\sigma}M \cong M$ translates into $\sigma(f_M)(T) = f_M(T + \lambda)$ for some $\lambda \in \frac{1}{r}\mathbf{Z}$. Since σ has finite order, one has $\lambda = 0$. Hence $f_M = f_Q \in k[T]$. Now Q defines also an irreducible differential module $N := k(Q)e$ with $\partial e = Qe$ over k of dimension $[k(Q) : k]$. Clearly $K \otimes_k N$ is isomorphic to M. □

Remarks 2.5
(1) Condition (a) in theorem 2.4 is superfluous. Any differential module M can be written as a finite direct sum $\oplus_i E(Q_i) \otimes R_i$, where $E(Q_i) \not\cong E(Q_j)$ for $i \neq j$ and where each R_i has the property that the matrix of ∂ w.r.t. a basis is nilpotent. This decomposition is unique (see [L]) and the Q_i are unique

up to the equivalence stated in the proof of 2.4. One observes that each R_i descends to k. This information suffices to prove the theorem without the assumption that M is irreducible.

(2) Let K be any finite (Galois) extension of $C_k((x))$. Such K has the form $C_K((t))$ where t has the property $t^m = cx$ with $c \in C_K^*$. The above theorem and its proof remain valid for this Galois extension and any differential module M over K. However, in case $m > 1$, the differential module N over k with $K \otimes_k N \cong M$ is no longer unique up to isomorphism.

(3) Theorem 2.4 and (1), (2) above, answer the descent problem for the local case, i.e., for formal Laurent series fields. In the sequel of this paper we will study the descent problem for the global case, i.e., for differential fields which are function fields in one variable over the field of constants. The situation $k = C_k(x) \subset K = C_K(x)$, where $C_k \subset C_K$ is an algebraic extension, is easier to deal with (see Theorem 2.8) than the general case. The following example illustrates this.

(4) Consider the differential fields $k = \mathbf{Q}(x)$ and $K = \mathbf{Q}(t)$ with $x = t - \frac{1}{t}$ and with differentiation $'$ given by $x' = 1$. Let σ denote the non-trivial automorphism of K/k. We note that $\sigma t = -\frac{1}{t}$. Define the 1-dimensional differential module $M = Ke$ with $\partial e = \frac{t'}{2t}e$. Then ${}^{\sigma}M \cong Ke$ with $\partial e = -\frac{t'}{2t}e$ and thus M is isomorphic to ${}^{\sigma}M$. We will prove that there does not exist $h \in K^*$ such that $a := \frac{t'}{2t} + \frac{h'}{h} \in k$. This implies that M does not descend to k. Suppose that h exists. Then $\sigma a = a$ and consequently $\frac{t'}{t} = \frac{\sigma h'}{\sigma h} - \frac{h'}{h}$. Then $t = \alpha \frac{\sigma h}{h}$ for some $\alpha \in \mathbf{Q}$. This yields the contradiction $-1 = \sigma(t)t = \alpha^2$.

2.2 Semi-simple modules and semi-simple algebras

In this subsection some known facts are collected, which are useful for the descent problem. It seems that proposition 2.7 is not available is the literature. For the first standard result we omit the proof.

Lemma 2.6 *Let M be a differential module over K. The following are equivalent.*
(1) *M is a sum of irreducible submodules.*
(2) *M is a direct sum of irreducible submodules.*
(3) *Every submodule $N \subset M$ is a direct summand, i.e., there exists a submodule N' with $M = N \oplus N'$.*

A differential module M, having the equivalent properties of 2.6, is called *semi-simple* or *completely reducible.*

Proposition 2.7 *Let $K \supset k$ be an algebraic extension of differential fields.*
(1) *Let N be a differential module over k. Then N is semi-simple $\Leftrightarrow$ the differential module $K \otimes_k N$ over K is semi-simple.*
(2) *Suppose that $[K : k] < \infty$ and that M is a semi-simple differential module over K. Then M considered as a differential module over k is semi-simple.*
(3) *Let A, B be semi-simple differential modules over k. Then $A \otimes_k B$ is semi-simple.*
(4) *The collection of semi-simple differential modules is stable under all "operations of linear algebra", i.e., submodules, quotients, direct sums, tensor products, symmetric powers,...*

Proof. (1'). We suppose first that $K \supset k$ is a finite Galois extension with Galois group G.
(1')$\Rightarrow$. We may suppose that N is irreducible. Take an irreducible K-submodule D of $K \otimes_k N$. Every $\sigma \in G$ acts on $K \otimes_k N$ in the obvious way and this action commutes with ∂. Then each $\sigma(D)$ is also an irreducible K-submodule of $K \otimes_k N$. Therefore $E = \sum_{\sigma \in G} \sigma(D)$ is a semi-simple K-submodule. Moreover, $\sigma(E) = E$ for all $\sigma \in G$. Hence $E = K \otimes_k F$ for some submodule of N. Since N is irreducible, one has that $F = N$ and $E = K \otimes_k N$.
(1')$\Leftarrow$. Let $F \subset N$ be a submodule. Then $K \otimes_k F$ is a K-submodule of $K \otimes_k N$. There exists a K-linear $P : K \otimes_k N \to K \otimes_k N$ with the properties im $P = K \otimes_k F$, $P^2 = P$ and $P\partial = \partial P$. Define $Q = \frac{1}{|G|} \sum_{\sigma \in G} \sigma P \sigma^{-1}$. Then $Q\partial = \partial Q$, $Qm = m$ for $m \in K \otimes_k F$, im $Q = K \otimes_k F$ and $\tau Q = Q\tau$ for all $\tau \in G$. Then $Q^2 = Q$. Let us identify any $n \in N$ with $1 \otimes n \in K \otimes_k N$. For any $n \in N$ one has that $Q(n)$ is invariant under G and therefore belongs to N. The restriction $\tilde{Q}$ of Q to N has the properties im $\tilde{Q} = F$, $\tilde{Q}\partial = \partial\tilde{Q}$ and $\tilde{Q}^2 = \tilde{Q}$. Then $N = F \oplus \ker \tilde{Q}$. Thus N is semi-simple.

(1"). Consider any finite extension of differential fields $k \subset K$. Let K_c denote its normal closure. By (1'), N is semi-simple over k if and only if $K_c \otimes_k N$ is semi-simple over K_c. But, again by (1'), $K_c \otimes_k N = K_c \otimes_K (K \otimes_k N)$ is semi-simple over K_c if and only if $K \otimes_k N$ is semi-simple over K.

(1). Let $K \supset k$ be an arbitrary algebraic extension. Suppose that N is semi-simple. Any K-submodule D of $K \otimes_k N$ comes (by tensoring) from a

$\tilde{K}$-submodule $\tilde{D}$ of $\tilde{K} \otimes_k N$ for some field $\tilde{K} \subset K$ which is finite over k. Since $\tilde{D}$ is a direct summand, D is a direct summand, too.
Suppose that $K \otimes_k N$ is semi-simple. Let $F \subset N$ be a submodule. Then $K \otimes_k F$ is a direct summand of $K \otimes_k N$. For a suitable finite extension K_1 of k, contained in K, also $K_1 \otimes_k F$ is a direct summand of $K_1 \otimes_k N$. One replaces K_1 by its normal closure $K_2 \supset K_1$. Then $K_2 \otimes_k F$ is a direct summand of $K_2 \otimes_k N$. As in the proof of (1')$\Leftarrow$, it follows that F is a direct summand.

(2). Let K_c be the normal closure of K. Then $K_c \otimes_K M$ is semi-simple over K_c. Further M is a k-submodule of $K_c \otimes_K M$. Therefore it suffices to consider the case where K is a Galois extension of k with Galois group G. By 2.1, one has $K \otimes_k M \cong \oplus {}^\sigma M$. Each ${}^\sigma M$ is semi-simple and thus $K \otimes_k M$ is a semi-simple differential module over K. By (1), M is semi-simple as k-differential module.

(3) We use the notations: C_k is the field of constants of k, $\overline{C}_k$ is an algebraic closure of C_k and $\underline{k} = \overline{C}_k \cdot k$. By (1), $\underline{A} := \underline{k} \otimes_k A$ and $\underline{B} := \underline{k} \otimes_k B$ are semi-simple. Using differential Galois theory, see [P-S], Exercise 2.38 (4), one has that $\underline{A} \otimes_{\underline{k}} \underline{B}$ is semi-simple. By (1), $A \otimes_k B$ is semi-simple.

(4) follows from (3). □

Let M be a semi-simple differential module over k. The *isotypical decomposition* $M = M_1 \oplus \cdots \oplus M_s$ is defined by: each M_i is a direct sum of, say, n_i copies of an irreducible differential module D_i. Moreover the $D_i \not\cong D_j$ for $i \neq j$. Put $F_i = \mathrm{End}_{k[\partial]}(D_i)$. Then one has the following obvious results:
(a) The isotypical decomposition of M is unique.
(b) F_i is a (skew) field of finite dimension over the field of constants C_k of k.
(c) $\mathrm{End}_{k[\partial]}(M)$ is isomorphic to the product of the algebras $\mathrm{Matr}(n_i, F_i)$.

Let C be any field. The algebras A that we consider here are supposed to have a neutral element, further C lies in the center of A, and A as vector space over C has finite dimension. A is called *semi-simple* if for every two-sided ideal I, there is a two-sided ideal J with $A = I \oplus J$. The semi-simple algebras are the algebras of the form $\prod_i \mathrm{Matr}(n_i, F_i)$ where the F_i are (skew) fields of finite dimension over C, with C in the center of F_i. The algebra A is called *simple* if A has no two-sided ideals other than 0 and A. Equivalently, $A \cong \mathrm{Matr}(n, F)$ for some n and some (skew) field F of finite dimension over C, with C in the center of F.

We recall some facts on skew fields and the Brauer group. For more information we refer to [Bl,Bo,Rei,S]. Let C be any field. Consider a skew field F of finite dimension over its center C. Then the dimension of F over C is a square, say n^2. A field extension $C' \supset C$ is called a *splitting field for* F if $C' \otimes F$ is isomorphic to the matrix algebra $\mathrm{Matr}(n, C')$. Any maximal commutative subfield C' of F satisfies $[C' : C] = n$ and is moreover a splitting field for F of minimal degree over C. This is illustrated by the example of Hamilton's quaternion field over $\mathbf{Q}$, namely $\mathbf{H} = \mathbf{Q} + \mathbf{Q}i + \mathbf{Q}j + \mathbf{Q}k$. The minimal splitting fields are $\mathbf{Q}(\sqrt{-m})$ for every squarefree positive integer m that can be written as the sum of three squares in $\mathbf{Q}$.

One way to construct examples of skew fields with center k is the following (Dickson's construction). Take a Galois extension $\ell \supset k$ of degree n with cyclic Galois group $< \sigma >$. Then take an $a \in k$ which is not the norm of any $b \in \ell'$ over ℓ'/k for any subfield $\ell' \neq k$ of ℓ. Then define $F = \oplus_{i=0}^{n-1} \ell u^i$ with the rules: $u\lambda = \sigma(\lambda)u$ for $\lambda \in \ell$ and $u^n = a$. Skew fields F that can be obtained this way are called *cyclic* (in the terminology of [Rei], p 259 and p 280). If k is a number field then every skew field F of finite dimension n^2 over its center k is cyclic.

For a general field k of characteristic 0, the classification of skew fields F of finite dimension over their center k is not very explicit. It is possible that no maximal commutative subfield of F is a Galois extension of k.

A *central simple* algebra A over the field C is an algebra whose only two-sided ideals are A and $\{0\}$ and which has finite dimension over its center C. Every central simple algebra over C has the form $\mathrm{Matr}(d, F)$, where F is a (skew) field with center C. The Brauer group $\mathrm{Br}(C)$ of a field C consists of the equivalence classes of the central simple algebras over C. Two such algebras $\mathrm{Matr}(d_i, F_i)$ are called equivalent if the (skew) fields F_1, F_2 are isomorphic. The group structure on $\mathrm{Br}(C)$ is induced by the tensor product. There is a natural isomorphism $\mathrm{Br}(C) \to H^2(\mathrm{Gal}(\overline{C}/C), \overline{C}^*)$, where $\overline{C}$ is the separable algebraic closure of C.

2.3 The associated two-cocycle and skew fields

Theorem 2.8 The associated 2-cocyle for a special case.
Consider the differential fields $k = C_k(x)$ and $K = C_K(x)$ where C_K/C_k is a finite Galois extension with group G. Assume that the differential module M of dimension n over K has the properties:
(i) *The group of the differential automorphism of M is C_K^*.*

(ii) *For every* $\sigma \in G$ *one has* ${}^{\sigma}M \cong M$.
These assumptions define a 2-cocycle class $\overline{c} \in H^2(G, C_K^*)$ *which has the following properties:*
(a) $\overline{c} = 1 \Leftrightarrow M$ *descends to* k.
(b) *The order* d *of* $\overline{c}$ *divides* n *and* $[K : k]$.
(c) *The inflation homomorphism* $H^2(G, C_K^*) \to H^2(\mathrm{Gal}(\overline{C_K}/C_k), \overline{C_k}^*) = \mathrm{Br}(C_k)$ *is injective and the image of* $\overline{c}$ *in the Brauer group* $\mathrm{Br}(C_k)$ *determines a (skew) field* F^o *with center* C_k.
(d) $E := \mathrm{End}_{k[\partial]}(M)$ *is a simple algebra, of dimension* $[C_K : C_k]^2$ *over its center* C_k, *having image* $\overline{c} \in \mathrm{Br}(C_k)$. *In particular,* E *is isomorphic to* $\mathrm{Matr}(m, F^o)$ *for some* $m \geq 1$. *Moreover,* C_K *is a maximal commutative subfield of* E.
(e) *A finite field extension* $\ell \supset C_k$ *is a splitting field for* F^o *if and only if* M *descends to* $\ell(x)$.

Proof. Choose an isomorphism $\phi(\sigma) : M \to {}^{\sigma}M$ for each $\sigma \in G$. By assumption (i), $\phi(\sigma)$ is unique up to an element in C_K^*. Let $\Phi(\sigma) : M \to M$ denote the associated σ-linear map. For $\sigma, \tau \in G$ one defines $c(\sigma, \tau) := \Phi(\sigma)\Phi(\tau)\Phi(\sigma\tau)^{-1}$. This is a K-linear bijection on M and commutes with ∂. By assumption (i), $c(\sigma, \tau) \in C_K^*$. Further $c(\sigma, \tau)$ satisfies the usual 2-cocycle relation. The image $\overline{c} \in H^2(G, C_K^*)$ is independent of the choices for the $\{\phi(\sigma)\}$. Part (a) follows at once from definition 2.2 part (3).

Consider the case where M has dimension 1. Write $M = Ke$ and write $\partial e = ae$. For any σ one normalizes $\Phi(\sigma) : M \to M$ by $\Phi(\sigma)e = b(\sigma)e$ such that $b(\sigma) \in C_K(x)$ has the form $b_1(\sigma)/b_2(\sigma)$ with $b_i(\sigma)$ monic elements of $C_K[x]$. Then $c(\sigma, \tau) \in C_K^*$ has this form too, which implies $c(\sigma, \tau) = 1$.

Let M of dimension n induce the 2-cocycle class $\overline{c}$. Then the 2-cocycle class of the 1-dimensional differential modules $\Lambda^n M$ is easily seen to be $\overline{c}^n$. Since the latter is trivial, the order d of $\overline{c}$ is a divisor of n. Moreover, every element in $H^2(G, C_K^*)$ is annihilated by the order of G, which is $[K : k]$. This proves (b). For (c) we refer to [S], p.126.
(d) According to 2.3 (a), $\mathrm{End}_{K[\partial]}(K \otimes_k M) \cong C_K \otimes_{C_k} \mathrm{End}_{k[\partial]}(M)$. By 2.1, $K \otimes_k M \cong \oplus_{\sigma \in G}\, {}^{\sigma}M$, which by assumption (ii) is isomorphic to the direct sum of $[C_K : C_k]$ copies M. Now $\mathrm{End}_{K[\partial]}(M) = C_K$, so $\mathrm{End}_{K[\partial]}(K \otimes_k M)$ is isomorphic to the matrix algebra $\mathrm{Matr}([C_K : C_k], C_K)$. It follows that the dimension of E over C_k is $[C_K : C_k]^2$.

Consider the algebra A consisting of the $L \in E$ of the form $L = \sum_{\sigma \in G} c_\sigma \Phi(\sigma)$ with $c_\sigma \in C_K$. It is easily verified that $L = 0$ if and only all c_σ are 0.

By [Bl], Proposition IV-1, one has that A is a simple algebra of dimension $[C_K : C_k]^2$ over its center C_k. Hence $A = E$. By construction the 2-cocycle class corresponding to E is $\overline{c}$. One concludes that $E \cong \mathrm{Matr}(m, F^o)$ for some m where F^o is the (skew) field associated to $\overline{c}$. Further $C_K = \mathrm{End}_{K[\partial]}(M)$ consists of the elements of E which commute with C_K. Hence C_K is a maximal commutative subfield of E.
If $C_k \subset \ell \subset C_K$ then part (e) follows from the statement that $\ell \supset C_k$ is a splitting field for F^o if and only if the image of $\overline{c}$ in $H^2(\mathrm{Gal}(C_K/\ell), C_K^*)$, under the restriction map, is 1. If ℓ is not a subfield of C_K, then replace C_K by the normal closure of $\ell \cdot C_K$. Then the same proof applies; assumption (i) still holds by lemma 2.3 (b), assumption (ii) is clear. □

Corollary 2.9 *We keep the notations and assumptions of theorem 2.8.*
(1) *Suppose that M is irreducible as K-differential module. Then M viewed as k-differential module is the direct sum of m copies of an irreducible differential module N over k with $\mathrm{End}_{k[\partial]}(N) = F^o$.*
(2) *Let be given:*
* *a skew field F^o of finite dimension over its center C_k,*
* *$m \geq 1$ and a maximal commutative subfield C_K of $\mathrm{Matr}(m, F^o)$, which is Galois over C_k,*
* *an irreducible k-differential module N with $\mathrm{End}_{k[\partial]}(N) = F^o$.*

Then M, the direct sum of m copies of N, has a natural structure of an irreducible $K = C_K(x)$-differential module that satisfies the assumptions of theorem 2.8.

Proof. (1) Let $P_i \in \mathrm{Matr}(m, F^o) = E = \mathrm{End}_{k[\partial]}(M)$ denote the matrix with all entries 0 with the exception of an entry 1 at the position (i, i). Put $N_i = P_i M$. Then N_i is a k-submodule of M and $M = \oplus_i N_i$. An element $L \in \mathrm{End}_{k[\partial]}(N_i)$ can be extended to an element $\tilde{L} \in E$ by prescribing $\tilde{L} = 0$ on each N_j with $j \neq i$. The structure of E implies that $\tilde{L}$ is a diagonal matrix with zeros on the diagonal, except for the position (i, i). Hence $L \in F^o$. Since the matrices P_i are conjugated in $\mathrm{Matr}(m, C_k)$, the k-differential modules N_i are all isomorphic. Moreover, since N_i is semi-simple and $\mathrm{End}_{k[\partial]}(N_i) = F^o$ one has that N_i is irreducible.
(2) $M = N \oplus \cdots \oplus N$ has $\mathrm{End}_{k[\partial]}(M) = \mathrm{Matr}(m, F^o)$. The embedding of C_K in $\mathrm{Matr}(m, F^o)$ makes M into a K-differential module. $\mathrm{End}_{K[\partial]}(M)$ consists of the elements in $\mathrm{Matr}(m, F^o)$ commuting with C_K. Thus $\mathrm{End}_{K[\partial]}(M) = C_K$. Further M is a semi-simple K-differential module since it is a semi-

simple k-differential module. Thus M is an irreducible K-differential module. Finally, by the Skolem-Noether theorem ([Bl], Théorème III-4, or [Rei], (7.21)) for every σ in the Galois group of C_K/C_k, there is an invertible element $\Phi(\sigma) \in \mathrm{Matr}(m, F^o)$ with $\sigma(\lambda) = \Phi(\sigma)\lambda\Phi(\sigma)^{-1}$ for all $\lambda \in C_K$. Then $\Phi(\sigma) : M \to M$ is a σ-linear map which commutes with ∂. $\square$

For a general finite Galois extension of differential fields $k \subset K$ with group G, the situation is more complicated; e.g. one-dimensional modules need not descend, and lemma 2.3 no longer applies (instead, apply proposition 1 in [C-W] to the Galois group of K over $C_K \cdot k$). Parts (a) and (b) of the following proposition can be proven along the lines of the proof of theorem 2.8. Part (c) follows from 2.11 (a) below.

Proposition 2.10 The associated 2-cocycle in the general case.
Let K/k be a finite Galois extension of differential fields with Galois group G. Let C_K denote field of constants of K. Let a differential module M over K of dimension n satisfy:
(i) *the group of the differential automorphisms of M is C_K^*, and*
(ii) *for every $\sigma \in G$ one has ${}^\sigma M \cong M$.*
(a) *These data determine a 2-cocycle class $\overline{c} \in H^2(G, C_K^*)$ of an order d, dividing $[K : k]$. Moreover M descends to k if and only if $\overline{c} = 1$.*
(b) *The tensor product $M \otimes \cdots \otimes M$ of d copies of M has associated 2-cocycle $\overline{c}^d$ and therefore this tensor product descends to k. The same holds for $\mathrm{sym}^d M$, the symmetric tensor product of d copies of M.*
(c) *The image of $\overline{c}$ under the map $H^2(G, C_K^*) \to H^2(G, K^*)$ defines a (skew) field F with center k. Let $k \subset \ell \subset K$. Then ℓ is a splitting field for F if and only if there exists a module L of dimension 1 over K such that ${}^\sigma L \cong L$ for all $\sigma \in G$ and $L \otimes M$ descends to ℓ.*

The condition ${}^\sigma L \cong L$ can be omitted if one assumes that M is not cyclic-imprimitive (see section 4, theorem 4.4).

In general the map $H^2(G, C_K^*) \to H^2(G, K^*)$ is not one to one. If $\overline{c}$ is a non-trivial element of the kernel, then $F = k$, so k is a splitting field, but M does not descend to k.

Consider differential modules M of dimension 1 over K such that ${}^\sigma M \cong M$ for all $\sigma \in G$. The isomorphism classes of these modules form an abelian group I with the tensor product as multiplication. Let I_0 denote the subgroup of the classes of differential modules which descend to k.

Proposition 2.11 *Let C_K denote the constant field of K. Then*
(a) *I/I_0 is naturally isomorphic to the kernel of $H^2(G, C_K^*) \to H^2(G, K^*)$.*
(b) *Let $M = Ke$ represent an element of I and let $E = \mathrm{End}_{k[\partial]}(M)$ which is a semi-simple algebra over C_k.*
If $K = C_K \cdot k$, then E is a central simple algebra over C_k. Moreover, M descends to ℓ with $k \subset \ell \subset K$ if and only if the field of constants C_ℓ is a splitting field for E.
If $K \neq C_K \cdot k$, then, in general, the 2-cocycle in $H^2(G, C_K^*)$ attached to M, does not describe a central simple algebra over C_k or k. Moreover, E is (in general) not a central simple algebra over C_k.

Proof. (a) Let $M = Ke$ represent an element of I. For any $\sigma \in G$ there is a σ-linear bijection $\Phi(\sigma) : M \to M$, commuting with ∂. Then $\Phi(\sigma)\Phi(\tau) = c(\sigma, \tau)\Phi(\sigma\tau)$ with $c(\sigma, \tau) \in C_K$. As before, $\{c(\sigma, \tau)\}$ is a 2-cocycle and defines a unique element $\overline{c}$ of $H^2(G, C_K^*)$. Further $\overline{c} = 1$ if and only if M descends to k. Write $\Phi(\sigma)e = f(\sigma)e$ with $f(\sigma) \in K^*$. Then $f(\sigma)\ \sigma(f(\tau)) = c(\sigma, \tau)f(\sigma\tau)$ and thus the image of $\overline{c}$ in $H^2(G, K^*)$ is 1. Thus we have obtained an injective homomorphism from I/I_0 to the kernel of $H^2(G, C_K^*) \to H^2(G, K^*)$.
On the other hand, let a 2-cocycle c for the action of G on C_K^* be given which has trivial image in $H^2(G, K^*)$. Then there are elements $f(\sigma) \in K^*$ such that $f(\sigma)\ \sigma(f(\tau)) = c(\sigma, \tau)f(\sigma\tau)$. From this one obtains $\frac{f(\sigma)'}{f(\sigma)} + \sigma(\frac{f(\tau)'}{f(\tau)}) = \frac{f(\sigma\tau)'}{f(\sigma\tau)}$. Since $H^2(G, K) = 0$, there is an element $A \in K$ with $\frac{f(\sigma)'}{f(\sigma)} = \sigma A - A$ for all σ. Define now the differential module $M = Ke$ by $\partial e = Ae$. Then the σ-linear maps $\Phi(\sigma) : M \to M$, defined by $\Phi(\sigma)e = f(\sigma)e$, commute with ∂. Thus M yields the given 2-cocycle c. This proves that the map from I/I_0 to the kernel of $H^2(G, C_K^*) \to H^2(G, K^*)$ is surjective.
(b) The algebra $\{\sum_{\sigma \in G} m_\sigma \Phi(\sigma) |\ m_\sigma \in K\}$ is equal to the algebra of all k-linear endomorphisms of M. This follows from the K-linear independence of the maps $\{\sigma : K \to K |\ \sigma \in G\}$. One derives from this that $E = \{\sum_{\sigma \in G} c_\sigma \Phi(\sigma) |\ c_\sigma \in C_K\}$.
If $K = C_K \cdot k$, then G is the Galois group of C_K/C_k. Again, by [Bl], Proposition IV-1, one has that E is a central simple algebra over C_k of dimension $[C_K : C_k]^2$. Consider an intermediate field ℓ. Then $K = C_K \cdot \ell$ and K/ℓ and C_K/C_ℓ have the same Galois group H. Now M descends to ℓ if and only if the restriction of the 2-cocycle $\overline{c}$ to H is trivial, if and only if C_ℓ is a splitting field for E.
Suppose that $K \neq C_K \cdot k$. Then C_K/C_k is still a Galois extension but its Galois group is different from G. The 2-cocycle in $H^2(G, C_K^*)$, attached to M,

need not describe a central simple algebra. Consider the example (4) of 2.5. The algebra E for this example is isomorphic to $\mathbf{Q}(i)$. It is also interesting to make part (a) explicit for this example. One has that I/I_0 is isomorphic to the kernel of $H^2(\{1,\sigma\},\mathbf{Q}^*) \to H^2(\{1,\sigma\},\mathbf{Q}(t)^*)$. One can verify that this kernel is the group of two elements. The example describes the non trivial element in this kernel. $\square$

2.4 Differential modules over a skew differential field

In the sequel of this section we will produce explicit examples for corollary 2.9. More precisely, for a given finite Galois extension $C_k \subset C_K$ and a skew field F^o of finite dimension over its center C_k such that C_K is a maximal commutative subfield of $\mathrm{Matr}(m,F^o)$, we will produce an irreducible differential module M over $K = C_K(x)$ which satisfies (i) and (ii) of 2.8 and such that $\mathrm{End}_{k[\partial]}(M) = \mathrm{Matr}(m,F^o)$. The basic feature of the construction is the introduction of differential modules over skew differential fields.

Definitions 2.12 Let k be a differential field and F a skew field of finite dimension over its center k. A differentiation $f \mapsto f'$ on F is an additive map from F to itself such that $(fg)' = f'g + fg'$ for all $f,g \in F$ and such that the restriction of $f \mapsto f'$ to $k \subset F$ is the differentiation of k. A differential module M over F is a finite dimensional left vector space over F, equipped with an additive map $\partial : M \to M$ satisfying $\partial(fm) = f'm + f\partial m$ for all $f \in F$ and $m \in M$.

Let $e_1,\dots,e_n$ be a basis of M over F. Then ∂ is determined by the elements $\partial e_1,\dots,\partial e_n$. Moreover, these elements in M can be chosen arbitrarily.

The next proposition together with part (2) of corollary 2.9 provides the required examples.

Proposition 2.13 *Let F^o be a skew field of finite dimension over its center C_k. On the skew field $F = F^o(x) := F^o \otimes_{C_k} C_k(x)$ with center $k = C_k(x)$, a differentiation is given by $(f \otimes a)' = f \otimes a'$ for all $f \in F^o$ and $a \in k$. Let N be a finite dimensional left vector space over F. Then N can be given the structure of differential module over F such that N is irreducible as k-differential module and* $\mathrm{End}_{k[\partial]}(N) = F^o$.

Proof. Choose a maximal commutative subfield C of F^o containing C_k. Then N is also a vector space over $C(x)$. Write $C = C_k(\alpha)$ and let $P \in C_k[x]$

denote the monic minimal polynomial of α. The completion of the local ring $C_k[x]_{(P)}$ is denoted by O_L. The residue field of O_L is C. There is a unique subfield of O_L containing C_k, which maps bijectively to the residue field C. We will identify C with this subfield of O_L. After this identification, the element $t = x - \alpha \in O_L$ is a generator of the maximal ideal. Thus we can identify the P-adic discrete valuation ring O_L with the t-adic discrete valuation ring $C[[t]]$. The embedding $C_k[x] \to O_L$ has dense image (the discrete valuation defines a topology). Let L denote the field of fractions of O_L. Then L is the completion of the field $k = C_k(x)$ w.r.t. the discrete valuation. The discrete valuation defines a topology on vector spaces over k, $C(x)$, and L. Now k is dense in L and $k \subset C(x) \subset L$.

Let $V = \mathrm{End}_F(N)$, $W = \mathrm{End}_{C(x)}(N)$, and $X = \mathrm{End}_L(L \otimes_{C(x)} N)$. Then $V \subset W \subset X$. We will show that V is dense in X. The natural k-algebra homomorphism $\phi : C(x) \otimes_k V \to W$ is bijective. Indeed, the first algebra is simple and the two algebras have the same dimension over k. Now k is dense in $C(x)$, hence V is dense in $C(x) \otimes_k V$ and hence in W, which is dense in X because $C(x)$ is dense in L.

We identify N with F^a and define the standard differentiation on N by $n = (n_1, \ldots, n_a) \mapsto n' = (n'_1, \ldots, n'_a)$. A structure ∂ on N as differential module over F has the form $\partial n = n' + A(n)$ with $A \in V$. A structure ∂ on N as differential module over $C(x) = C(t)$ has the form $\partial n = n' + A(n)$ with $A \in W$. Likewise, an element $A \in X$ defines a differential structure on $C((t)) \otimes_{C(t)} N$. Consider now the set X_r consisting of all $A \in X$ for which the Newton polygon of a cyclic element of $C((t)) \otimes_{C(t)} N$ has slope $\frac{1}{r}$, where r is the dimension of N as $C(x)$-vector space. This set is not empty, and for any $A \in X_r$, the $\overline{C}((t))[\partial]$-module $\widehat{N} := \overline{C}((t)) \otimes_{C(t)} N$ is irreducible.

The Newton polygon of a differential module over $C((t))$ depends on only finitely many coefficients in C. This implies that X_r is an open set, and hence there exists $A \in V \bigcap X_r$. We conclude from the irreducibility of $\widehat{N}$ that:
N can be given the structure of a differential module over F such that N and $\overline{C}(x) \otimes_{C(x)} N$ are irreducible differential modules over $C(x)$ and $\overline{C}(x)$. Moreover $\mathrm{End}_{\overline{C}(x)[\partial]}(\overline{C}(x) \otimes_{C(x)} N) = \overline{C}$.

Let $\tilde{C} \supset C$ be the normal closure of $C \supset C_k$. Put $\tilde{N} = \tilde{C}(x) \otimes_{C(x)} N$. As a k-differential module, $\tilde{N}$ is isomorphic to a direct sum of $[\tilde{C} : C]$ copies of N. Therefore, $\mathrm{End}_{k[\partial]}(\tilde{N})$ equals $\mathrm{Matr}([\tilde{C} : C], \mathrm{End}_{k[\partial]}(N))$ and contains the simple algebra $A := \mathrm{Matr}([\tilde{C} : C], F^o)$ with center C_k. Further $\tilde{C}$ is a maximal commutative subfield of A (since it has the correct dimension).

By the Skolem-Noether theorem, every $\sigma \in \mathrm{Gal}(\tilde{C}/C_k)$ extends to an inner automorphism of A. Thus the $\tilde{C}(x)$-module $\tilde{N}$ satisfies condition (ii) of 2.8. Further $\tilde{N}$ is irreducible and $\mathrm{End}_{\tilde{C}(x)[\partial]}(\tilde{N}) = \tilde{C}$. Condition (i) of 2.8 holds and we can apply the first part of 2.9. One has $\mathrm{End}_{k[\partial]}(\tilde{N}) = \mathrm{Matr}(b, F^o)$ for some $b \geq 1$. Now $\tilde{C}$ is also a maximal commutative subfield of $\mathrm{End}_{k[\partial]}(\tilde{N})$. Therefore the latter algebra coincides with A and $\mathrm{End}_{k[\partial]}(N) = F^o$. Finally, since N is semi-simple as differential module over k, it follows that N is irreducible. $\square$

We give now *a second construction of examples for corollary 2.9 with* $m = 1$, which will produce nicer examples because there will be only one irregular singularity (at $x = \infty$). Given is a skew field F^o of finite dimension over its center C_k and a maximal commutative subfield C_K of F^o which is a Galois extension of C_k. As before $F = F^o(x) = F^o \otimes_{C_k} C_k(x)$ is made into a skew differential field by the formula $(f \otimes a)' = f \otimes a'$ for all $f \in F^o$ and $a \in C_k(x)$. Then $K = C_K(x)$ is a maximal commutative subfield of F and the restriction of the differentiation of F to K is the obvious differentiation of K.

Proposition 2.14 *We use the above notations. Let M be a finite dimensional left vector space over F. Then M can be given a structure of differential module over F such that M is an irreducible K-differential module with the properties:*
(a) $\mathrm{End}_{K[\partial]}(M) = C_K$.
(b) ${}^{\sigma}M \cong M$ *for all* $\sigma \in \mathrm{Gal}(K/k)$.
(c) $\mathrm{End}_{k[\partial]}(M) = F^o$ *and M is irreducible as k-differential module.*
(d) $\underline{M} := \overline{C_K}(x) \otimes_K M$ *is an irreducible differential module over* $\overline{C}_K(x)$.
(e) $\mathrm{End}_{\overline{C}_K(x)[\partial]}(\underline{M}) = \overline{C}_K$.

Proof. As in the proof of proposition 2.13, we identify M with F^a for some $a \geq 1$ and define the operation $'$ on F^a by $(f_1, \ldots, f_a)' = (f_1', \ldots, f_a')$. A structure ∂ of differential module over F on M is given by $\partial m = m' + mD$, with $D \in \mathrm{Matr}(a, F)$.

For D we make the choice $D = \sum_{i=0}^{N} D_i x^i$, with:
(1) D_N is a diagonal matrix with distinct coefficients in C_k on the diagonal,
(2) $\{D_0, \ldots, D_{N-1}\}$ are generators of $\mathrm{Matr}(a, F^o)$ over C_k,
(3) M is irreducible as differential module over F.
For $a = 1$, property (3) is obvious. Moreover in that case we may replace

(1)+(2) by: $D_0,\dots,D_N$ generate F^o over C_k. If $a>1$, then one could apply the method of proposition 2.13 in order to obtain (3) and (a–e), but we will avoid this because it leads to examples more complicated than $\sum_{i=0}^N D_i x^i$, and because (3) is easy to verify for our explicit examples.

(i) $\mathrm{End}_{k[\partial]}(M)=F^o$.
For any algebra B we write B^{opp} for the opposite algebra. For any algebra B we write $\mathrm{Matr}(a,B)$ for the algebra of the $a\times a$-matrices with coordinates in B. Now F and $\mathrm{Matr}(a,F)^{opp}$ are central simple algebras over k. By [Ren], Corollaire 4, p 107, the algebra $F\otimes_k \mathrm{Matr}(a,F)^{opp}$ is again simple. This algebra is mapped to $\mathrm{End}_k(F^a)$, the algebra of the k-linear endomorphisms of F^a, by the following formula $(f\otimes B)(v)=fvB$ for $f\in F$, $v\in F^a$, $B\in\mathrm{Matr}(a,F)^{opp}$. Since the first algebra has only trivial two-sided ideals, this map is injective. By counting dimensions over k, one concludes that the map is bijective. Let $b_1,\dots,b_{d^2}$ denote a basis of F^o over C_k. From the above it follows that every k-linear map $L:M\to M$ can uniquely be written as $L(v)=\sum_{i=1}^{d^2} b_i v A_i$, with all $A_i\in\mathrm{Matr}(a,F)$.

For L as above one calculates that $(\partial L-L\partial)v=\sum_{i=1}^{d^2} b_i v B_i$, where B_i equals the matrix $A_i'+A_iD-DA_i$. Hence L commutes with ∂ if and only if $A_i'+A_iD-DA_i=0$ for every i.

Suppose that $A\in\mathrm{Matr}(a,F)$ is a non-zero solution of $A'=[D,A]$. Let $q\in C_k[x]$ denote the monic polynomial of minimal degree such that $qA\in\mathrm{Matr}(a,F^o[x])$. Write $A=q^{-1}B$, then $-q'q^{-2}B+q^{-1}B'+q^{-1}BD-q^{-1}DB=0$. After multiplying this identity with q one finds that $q'A\in\mathrm{Matr}(a,F^o[x])$. One concludes that $q=1$. Hence $A\in\mathrm{Matr}(a,F^o[x])$.

The set V of all solutions $A\in\mathrm{Matr}(a,F^o[x])$ of $A'=[D,A]$ is an algebra over C_k. Moreover, V is a finite dimensional vector space over C_k since $A'=[D,A]$ can be interpreted as a linear differential equation over the differential field k. Any $A\in V$, $A\neq 0$ can be written in the form $A=\sum_{i=0}^e A_i x^i$ with all $A_i\in\mathrm{Matr}(a,F^o)$ and $A_e\neq 0$. One finds that $[D_N,A_e]=0$ and thus A_e is a diagonal matrix (with coefficients in F^o). The elements $\mathbf{1},A,A^2,A^3,\dots$ all belong to V. In particular, there is a non-trivial relation $\lambda_0\mathbf{1}+\lambda_1A+\cdots+\lambda_sA^s=0$ with all $\lambda_i\in C_k$ and $\lambda_s\neq 0$. If $e>0$, then, since A_e is a non-zero diagonal matrix, the term x^{es} is present in A^s and not in the A^i with $i<s$. This contradiction implies that $e=0$. Further $A=A_0$ lies in the center of $\mathrm{Matr}(a,F^o)$, since A_0 commutes with all D_i. Hence $A=\lambda\mathbf{1}$ for some $\lambda\in C_k$. Hence $\mathrm{End}_{k[\partial]}(M)=F^o$.

(ii) $\mathrm{End}_{K[\partial]}(M)=C_K$ *and* M *is an irreducible differential module over* K.

The first statement holds because C_K is a maximal commutative subfield of F^o. Let $0 \neq N \subset M$ be an irreducible K-differential module. For any $f \in F^o$, $f \neq 0$, also fN is an irreducible K-differential module. The sum $\sum fN$, where f runs in a basis of F^o over C_K, is a semi-simple K-differential module. Since this object is invariant under left multiplication by F, and M is an irreducible F-differential module, one has $\sum fN = M$. So M is semi-simple over K and since $\mathrm{End}_{K[\partial]}(M)$ contains no zero-divisors it follows that M is irreducible over K. The same argument (or 2.7) shows that M is semi-simple and irreducible over k.

(iii) ${}^{\sigma}M \cong M$ *as differential modules over* K.
The Skolem-Noether theorem asserts that for $\sigma \in G$ there exists non-zero $f_\sigma \in F^o$ such that $\sigma(\lambda) = f_\sigma \lambda f_\sigma^{-1}$ for every $\lambda \in C_K$. One defines $\Phi(\sigma)(m) = f_\sigma m$. Clearly $\Phi(\sigma) : M \to M$ is a σ-linear bijection, commuting with ∂. This proves (b). Statements (d) and (e) follow from 2.7 and 2.3. □

Examples 2.15 *Skew fields over* $\mathbf{Q}$.
(1) Let $\mathbf{H} = \mathbf{Q} + \mathbf{Q}i + \mathbf{Q}j + \mathbf{Q}k$ denote *Hamilton's quaternion field over* $\mathbf{Q}$. We consider a maximal commutative subfield $C_K = \mathbf{Q}(i)$ and the fields $K := C_K(x)$, $k = \mathbf{Q}(x)$. One provides the 1-dimensional left vector space $M = \mathbf{H}(x)e$ over $\mathbf{H}(x)$ with ∂ defined by $\partial e = de$ for some $d \in \mathbf{H}(x)$. According to proposition 2.14, the choice $d = i+jx$ makes M into an example for 2.8 and 2.9. Let σ be the non-trivial element in $\mathrm{Gal}(K/k)$. Then $\Phi(\sigma)$, defined by $\Phi(\sigma)he = jhe$ for all $h \in \mathbf{H}(x)$, is a good choice for the σ-linear bijection commuting with ∂. We note that the 2-cocycle c has the form $c(1,1) = c(1,\sigma) = c(\sigma,1) = 1$ and $c(\sigma,\sigma) = -1$.

(i) *Explicit formulas.*
$e \in M$ is cyclic for M as a differential module over $k = \mathbf{Q}(x)$. The minimal monic operator $L_4 \in k[\partial]$ with $L_4 e = 0$ has the form

$$L_4 = \partial^4 + (2+2x^2)\partial^2 + 4x\partial + (4 + 2x^2 + x^4).$$

By 2.14 (c), L_4 is irreducible as element of $\mathbf{Q}(x)[\partial]$. Moreover, $e \in M$ is also cyclic for M as $\mathbf{Q}(i)(x)[\partial]$-module. The minimal monic operator $L_2 \in \mathbf{Q}(i)(x)[\partial]$ has the form

$$L_2 = \partial^2 - x^{-1}\partial + (ix^{-1} + 1 + x^2).$$

L_2 must be a right hand factor of L_4 in $\mathbf{Q}(i)(x)[\partial]$. Indeed,

$$L_4 = (\partial^2 + x^{-1}\partial + (-x^{-2} - ix^{-1} + 1 + x^2)) \cdot L_2.$$

By 2.14 (d), the operator L_2 is irreducible as element of $\overline{\mathbf{Q}}(x)[\partial]$.
As we know L_2 is equivalent to its conjugate $\partial^2 - x^{-1}\partial + (-ix^{-1} + 1 + x^2)$ and L_2 is not equivalent to any second order differential operator in $\mathbf{Q}(x)[\partial]$. Now $\mathbf{Q}(\sqrt{-m})$ is a splitting field of $\mathbf{H}$ when $m > 0$ is the sum of three squares in $\mathbf{Q}$. Hence for every such m, L_2 must be equivalent to an operator in $\mathbf{Q}(\sqrt{-m})(x)[\partial]$, and L_4 can be factored as a product of two irreducible operators in $\mathbf{Q}(\sqrt{-m})(x)[\partial]$.

(ii) *The associated third order operator* $L_3 \in \mathbf{Q}(x)[\partial]$.
According to 2.10 (b), the *symmetric square* $N := sym^2 M$ of M as $\mathbf{Q}(i)(x)[\partial]$-module descends to $\mathbf{Q}(x)$. We want to make this explicit for our example. The σ-linear map $\Psi(\sigma) : sym^2 M \to sym^2 M$ is defined by

$$\Psi(\sigma)(m_1 \otimes m_2) = \Phi(\sigma)m_1 \otimes \Phi(\sigma)m_2 = jm_1 \otimes jm_2.$$

In particular, $\Psi(\sigma)^2$ is the identity. Let N^0 denote the set of the elements of N invariant under $\Psi(\sigma)$. Give M the basis e, je. Then N has $\mathbf{Q}(i)(x)$-basis $e\otimes e,\ je\otimes e,\ je\otimes je$. One finds that N^0 has $\mathbf{Q}(x)$-basis $e\otimes e + je\otimes je,\ ie\otimes e - ije\otimes je,\ ije\otimes e$. Further N^0 is a differential module over $\mathbf{Q}(x)$, since $\Psi(\sigma)$ commutes with ∂. Thus $N = \mathbf{Q}(i)(x) \otimes_{\mathbf{Q}(x)} N^0$. We take $ije\otimes e$ as cyclic element of N^0 and let L_3 be its minimal operator: $L_3(ije\otimes e) = 0$. A calculation shows that

$$L_3 = \partial^3 - 2x^{-1}\partial^2 + (2x^{-2} + 4 + 4x^2)\partial + 4x.$$

L_3 must be equivalent to the symmetric square of the operator L_2 above. The latter does not have coefficients in $\mathbf{Q}(x)$ because it corresponds to the cyclic vector $e\otimes e$, which is not invariant under $\Psi(\sigma)$.

Since N is a symmetric square, we see that N^0 becomes a symmetric square after making a suitable algebraic extension C of $\mathbf{Q}$. The fields C are precisely the splitting fields for $\mathbf{H}$. We will return to this in the next section.

(2) *Example for a general quaternion field over* $\mathbf{Q}$.
If we repeat the computation with i replaced by b_1, j replaced by b_2, with the following rules of multiplication: $b_1^2 = A_1$, $b_2^2 = A_2$, $b_2b_1 = -b_1b_2$, replacing $\mathbf{H}$ by $F^o = \mathbf{Q} + \mathbf{Q}b_1 + \mathbf{Q}b_2 + \mathbf{Q}b_1b_2$, and d by $b_1 + b_2x$ then we find the following L_2

$$L_2 = \partial^2 - x^{-1}\partial + \sqrt{A_1}x^{-1} - A_1 - A_2x^2.$$

Now the splitting fields of F^o are precisely the fields C for which the conic

$$A_1X^2 + A_2Y^2 - 1 = 0$$

has a point $(X, Y) \in C^2$. In particular, F^o is a skew field if and only if this conic has no $\mathbf{Q}$-rational point. For example if $A_1 = 2$ and $A_2 = 3$, then F^o is a skew field with center $\mathbf{Q}$. We note that the following operator

$$L_2' = \partial^2 - A_2x^2 - A_1 + \sqrt{A_2}$$

is equivalent to L_2. Hence it defines the same descent problem, and L_2' descends to $C(x)[\partial]$ if and only if C is a splitting field of F^o. The symmetric square of L_2 is equivalent to

$$L_3 = \partial^3 - 2x^{-1}\partial^2 + (2x^{-2} - 4A_1 - 4A_2x^2)\partial - 4A_2x$$

which is equivalent to

$$\partial^3 - 4(A_1 + A_2x^2)\partial - 12A_2x.$$

L_3 can be found by a cyclic vector computation (as in (1) part (ii)), but can also be found by computing the third-order right-hand factor of the symmetric product of L_2 and its conjugate.

Suppose A_1, A_2 are integers, and that the conic has a rational point $(X, Y) \in \mathbf{Q}^2$. Then L_2 descends to $\mathbf{Q}(x)$ and the cocycle class $\overline{c}$ in theorem 2.8 is 1. If both parts (i) and (ii) of the descent data are explicitly known, then one can explicitly calculate descent: The module N in 2.2 part (3) can be found as $\{\sum_{\sigma\in G}\Phi(\sigma)(m) | m \in M\}$. Conversely, if one knows an explicit descent, then descent data can also be explicitly calculated. Now suppose that A_1, A_2 are given, but X, Y are not. It is easy to calculate part (i) of the descent data for the example L_2. However, to calculate part (ii) of the descent data, one must multiply the $\phi(\sigma)$ by suitable rational numbers, and this requires finding a rational point on the conic. Known algorithms for finding rational points on a conic use factorization of integers. So finding a rational point can be computationally hard (but only if $A_1, A_2, -A_1A_2$ are not squares, and at least one A_i is hard to factor in $\mathbf{Z}$, for an example see http://www.math.fsu.edu/~hoeij/files/conic). For such A_1, A_2, finding part (ii) of the descent data for L_2, or equivalently, finding descent, is computationally hard. Finding an irreducible submodule of M, viewed as differential module over $\mathbf{Q}(x)$, is then also computationally hard, which implies that factoring

$$L_4 = \partial^4 - 2(A_2x^2 + A_1)\partial^2 - 4A_2x\partial + A_1^2 - 3A_2 + A_2^2x^4 + 2A_1A_2x^2$$

in $\mathbf{Q}(x)[\partial]$ is hard. Indeed, one can parametrize all monic second order factors

$$\partial^2 - s/(t+sx)\,\partial - A_2x^2 - A_1 - u/(t+sx)$$

of L_4 in terms of points $(s:t:u)$ on the conic $A_1s^2 + A_2t^2 - u^2 = 0$, and hence finding a second order factor is equivalent to finding a point on the conic.

(3) *Example with M of dimension 2 over F.*
Consider the quaternion field $F^o = \mathbf{Q} + \mathbf{Q}b_1 + \mathbf{Q}b_2 + \mathbf{Q}b_1b_2$, with $b_1^2 = 2$, $b_2^2 = 3$, $b_2b_1 = -b_1b_2$. Let $F = F^o(x)$ and $M = F^2$ be the 2-dimensional differential module over F given by the following action of ∂ (recall that we are using row notation $v = (v_1,\ v_2)$)

$$\partial v = v' + v \begin{pmatrix} 0 & 1 \\ b_1 + b_2x & 0 \end{pmatrix}.$$

By 2.14, $\mathrm{End}_{\mathbf{Q}(x)[\partial]}(M) = F^o$ and M is irreducible as $\mathbf{Q}(\sqrt{2})(x)$-differential module. The cyclic vector $(1,\ 0)$ gives the following operator:

$$\partial^4 - 2x^{-1}\partial^3 + 2x^{-2}\partial^2 + 2\sqrt{2}x^{-1}\partial - 2\sqrt{2}x^{-2} - 2 - 3x^2.$$

This operator is irreducible (even over $\overline{\mathbf{Q}}$) and descends to $C(x)[\partial]$ if and only if C is a splitting field for F^o.

(4) *A skew field F^o of dimension 9 over* $\mathbf{Q}$.
Let α be a solution of $\alpha^3 - 3\alpha - 1 = 0$. Then $\mathbf{Q}(\alpha)$ is Galois over $\mathbf{Q}$ with Galois group generated by σ, where σ maps α to $2 - \alpha^2$. Now take b such that $b\alpha = \sigma(\alpha)b$ and $b^3 = 2$. Let F^o be the skew field generated by α and b, take $d = b + \alpha x$, let $M = F^o(x)$, and $\partial v = v' + vd$. Then we find the following operator

$$\partial^3 + (\alpha^2 - 2\alpha - 2 - 3x^2)\partial - x^3 - (1 + \alpha + \alpha^2)x - 2 \in \mathbf{Q}(\alpha)[\partial].$$

It is irreducible, even as element of $\overline{\mathbf{Q}}(x)[\partial]$, and descends to $C(x)[\partial]$ if and only if C is a splitting field for F^0.

2.5 Amitsur's construction

Let K be a differential field of characteristic 0, having C as field of constants. Amitsur considers an irreducible differential module M of dimension n over K with the property that $M^*\otimes M$ is a trivial differential module. In other words, $\mathrm{Hom}(M,M)$ is a trivial differential module and the ring of endomorphisms $E := \mathrm{End}_{K[\partial]}(M)$, which equals $\ker(\partial, \mathrm{Hom}(M,M))$, has dimension n^2 over C. Now $K\otimes_C E$ is the K-algebra of all K-linear maps $M\to M$. It follows that E is a skew field with center C. Further K is a splitting field for this skew field.

One of the main results, Theorem 16 of [A] is:
Any skew field with center C and splitting field K is obtained in this way.

The following example illustrates the proof, as well as the type of choice one has to make for K, C (common differential fields such as $K = C(x)$ will not produce examples, so there is no overlap with the other material presented in this paper).
The differential field K is given by $K = \mathbf{Q}(s,t)$ with $s^2+t^2 = -1$ and $s' = 1,\ t' = -st^{-1}$. The field K is a splitting field for Hamilton's quaternions $\mathbf{H} = \mathbf{Q}+\mathbf{Q}i+\mathbf{Q}j+\mathbf{Q}k$ over $\mathbf{Q}$. By definition there is a homomorphism $a\in\mathbf{H}\mapsto P_a\in\mathrm{End}_K(M)$, where $M = K^2$. One defines $\partial_0 : M\to M$ by $\partial_0(f_1,f_2) = (f_1',f_2')$. For any K-linear map $L : M\to M$ one defines the K-linear map L' by $L' = \partial_0 L - L\partial_0$. The representations $\mathbf{H}\to\mathrm{End}_K(M\oplus M)$, given by $a\mapsto \begin{pmatrix} P_a & 0\\ 0 & P_a\end{pmatrix}$ and $a\mapsto\begin{pmatrix} P_a & P_a'\\ 0 & P_a\end{pmatrix}$, are isomorphic. Indeed, every finitely generated left module over a semi-simple algebra is itself semi-simple. Using this one obtains a $Q\in\mathrm{End}_K(M)$ with the property $P_a' = QP_a - P_aQ$ for all $a\in\mathbf{H}$. Define now $\partial : M\to M$ by $\partial = \partial_0 - Q$. This makes $M = (M,\partial)$ into a differential module over K such that $\mathbf{H}\to\mathrm{End}_{K[\partial]}(M)$. Hence $\mathrm{Hom}(M,M)$ is a trivial differential module and $\mathrm{End}_{K[\partial]}(M) = \mathbf{H}$. This is Amitsur's construction.

We calculated an example: $M\cong K[\partial]/K[\partial]L$ with

$$L = (s^2+1)^2\partial^2 + s\partial - \frac{1}{4}.$$

$\mathrm{End}_{K[\partial]}(M) = \mathbf{H}$ implies: L is irreducible in $K[\partial]$ but factors in $K(\sqrt{-m})[\partial]$ for every $m>0$ which is a sum of three squares in $\mathbf{Q}$, and $K(\sqrt{-m})\otimes_K M$ is isomorphic to the direct sum of two copies of a 1-dimensional differential module over $K(\sqrt{-m})$ for such m.

3 Differential modules of dimension 3

In this section we consider a differential operator $L_3 \in K[\partial]$ of order 3 over a differential field K. The first question is whether L_3 is equivalent to the second symmetric power of a differential operator of order 2. Singer (see [Si]) answered this, he showed that it reduces to finding a point on a conic. This raises a second question: Which conics can occur, and given a conic, how to construct an example? We will use skew differential fields to answer this.

The first question translates in terms of differential modules as follows. A differential module B of dimension 3 over K is given. Is B isomorphic to the second symmetric power $sym_K^2 A$ of a differential module A of dimension 2 over K? We recall that $sym_K^2 A$ is defined as the K-vector space $A \overset{s}{\otimes}_K A$ with ∂ given by the formula $\partial(a_1 \otimes a_2) = (\partial a_1) \otimes a_2 + a_1 \otimes (\partial a_2)$. Our interest in this question lies in the fact that a differential module B may not be a second symmetric power, but could become a second symmetric power after enlarging the field of constants of K. Example 2.15, (1), (ii) has this feature. There is again a 2-cocycle responsible for this phenomenon (see section 4) and we will construct examples using quaternion fields. First we investigate some properties of the second symmetric power.

3.1 Properties of the second symmetric power

Lemma 3.1 *Let B be a differential module of dimension 3 over a differential field K. The following are equivalent:*
(1) $B \cong sym_K^2 A$ for some differential module A of dimension 2 over K.
(2) $sym_K^2 B$ has a 1-dimensional submodule L with the following property. Let b_1, b_2, b_3 be any basis of B over K. Then L is generated by an element of the form $\sum_{1\leq i\leq j\leq 3} c_{i,j} b_i \otimes b_j$ with $c_{i,j} \in K$ and the quadric $\sum_{1\leq i\leq j\leq 3} c_{i,j} X_i X_j = 0$ in $\mathbf{P}_K^2$ is non-degenerate and has a K-rational point.

Proof. (1)$\Rightarrow$(2). Let a_1, a_2 be a basis of A over K. Put $b_1 = a_1 \otimes a_1,\ b_2 = a_2 \otimes a_2,\ b_3 = a_1 \otimes a_2$. Then the 1-dimensional subspace L of $sym_K^2 B$ with generator $b_1 \otimes b_2 - b_3 \otimes b_3$ is easily seen to be a differential submodule. Moreover $X_1 X_2 - X_3^2 = 0$ has a non-trivial solution in K^3.
The reasoning above is based on the observation that the canonical morphism of differential modules $\phi : sym_K^2 B \to sym_K^4 A$ is surjective. Comparing the dimensions, one finds that the kernel of ϕ is a 1-dimensional submodule of $sym_K^2 B$.

(2)⇒(1). The assumption on the equation $\sum_{1\leq i\leq j\leq 3} c_{i,j}X_iX_j = 0$ has a non-trivial solution in K^3 implies that there exists a linear change of the variables X_1, X_2, X_3 which transforms the quadratic form into a multiple of $X_1X_2 - X_3^2$. Thus B has a basis b_1, b_2, b_3 such that the 1-dimensional K-vector space generated by $b_1 \otimes b_2 - b_3 \otimes b_3$ of $sym_K^2 B$ is a differential submodule. One considers a 2-dimensional vector space A over K with basis a_1, a_2 and one defines the K-linear bijection $\phi : sym_K^2 A \to B$ by $\phi(a_1 \otimes a_1) = b_1$, $\phi(a_2 \otimes a_2) = b_2$ and $\phi(a_1 \otimes a_2) = b_3$. Let the ∂ on B be given by the formula $\partial b_i = \sum_j e_{j,i} b_j$ for $i = 1, 2, 3$. The K-vector space A is made into a differential module by putting $\partial a_i = \sum_j d_{j,i} a_j$ with $d_{1,1} = e_{1,1}/2,\ d_{2,1} = e_{3,1}/2,\ d_{1,2} = e_{3,2}/2,\ d_{2,2} = e_{2,2}/2$. Using that $\partial(b_1 \otimes b_2 - b_3 \otimes b_3)$ is equal to $f(b_1 \otimes b_2 - b_3 \otimes b_3)$ for some $f \in K$, one can verify that ϕ is an isomorphism of differential modules. □

Lemma 3.2 *Let B be a differential module of dimension 3 over K. If $sym_K^2 B$ has a 1-dimensional submodule such that the corresponding quadratic form is degenerate, then B is reducible.*

Proof. Suppose that the quadratic form associated to the 1-dimensional submodule L is degenerate. This degenerate quadratic form has rank 1 or 2. There exists $c_1, c_2 \in C_K$ and a basis b_1, b_2, b_3 of B such that L is generated by $b_1 \otimes b_1$ (for rank 1) or by $c_1 b_1 \otimes b_1 + c_2 b_2 \otimes b_2$ (for rank 2). Then Kb_1 or $Kb_1 + Kb_2$ is a differential submodule of B. □

Lemma 3.3 *Let A be an irreducible differential module of dimension 2. Put $B = sym_K^2 A$. Then B is reducible if and only if there is a field extension $\tilde{K} \supset K$ of degree two such that $\tilde{K} \otimes_K A$ is reducible.*

Proof. Because of 2.7 (4), if B is reducible then B has a one-dimensional submodule L. One can choose a basis a_1, a_2 of A such that a generator of L has one of the following forms: $a_1 \otimes a_1$, $a_1 \otimes a_2$ or $a_1 \otimes a_1 - f a_2 \otimes a_2$ where $f \in K$ is not a square. The first two cases are excluded since A is irreducible. In the last case one puts $\tilde{K} = K(\sqrt{f})$ and $\tilde{K} \otimes_K A = \tilde{K}(a_1 + a_2\sqrt{f}) \oplus \tilde{K}(a_1 - a_2\sqrt{f})$ and thus $\tilde{K} \otimes A$ is reducible.

Conversely, let $\tilde{K} = K(t)$ with $t^2 = f \in K$ and write σ for the non-trivial element of $\mathrm{Gal}(\tilde{K}/K)$. Let $\tilde{K}e$ be a submodule of $\tilde{K} \otimes A$. If $\tilde{K}\sigma e = \tilde{K}e$, then $\sigma e = ge$ for some $g \in \tilde{K}^*$ and $g\sigma(g) = 1$. Then $g = \frac{h}{\sigma h}$ for some $h \in \tilde{K}^*$ and so $\sigma(he) = he$. It follows that $he \in A$ and Khe is a submodule of A.

This is a contradiction since A is irreducible. Thus $\tilde{K} \otimes A$ is the direct sum of the submodules $\tilde{K}e$ and $\tilde{K}\sigma e$. Then $a_1 = e + \sigma e,\ a_2 = te - t\sigma e$ is a basis of A. Finally $a_1 \otimes a_1 - f^{-1} a_2 \otimes a_2$ generates a submodule of B. $\square$

Remarks. An irreducible differential module A of dimension 2 will be called *imprimitive* if there exists a quadratic extension $\tilde{K}$ of K such that $\tilde{K} \otimes_K A$ is reducible. Otherwise A will be called *primitive.* A differential module A can be imprimitive for two different reasons. It is possible that A becomes reducible after a quadratic extension of the field of constants of K. In the second case, A remains irreducible after replacing K by $\overline{C_K}K$. The differential Galois group G is defined for the differential module $\overline{C_K}K \otimes A$. Imprimitive is now equivalent to: the action of G on the two-dimensional solution space V is irreducible and there are lines $L_1, L_2 \subset V$ such that $V = L_1 \oplus L_2$ and any $g \in G$ permutes the lines L_1, L_2. In other words, G is contained in the infinite dihedral group $\{g \in \mathrm{GL}_2 |\ \{gL_1, gL_2\} = \{L_1, L_2\}\}$.

Lemma 3.4 *Suppose that the two-dimensional differential module A is irreducible and primitive. Put $B = sym_K^2 A$. There are two possibilities:*
(1) *$sym_K^2 B$ has three distinct submodules of dimension 1. Each one of them determines a non-degenerate quadric having a K-rational point.*
(2) *$sym_K^2 B$ has a unique submodule of dimension 1.*

Proof. After replacing A by $L \otimes A$ for a suitable 1-dimensional differential module, we may suppose that the differential Galois group G of A is an irreducible, primitive subgroup of $\mathrm{SL}_2(\overline{C_K})$. We note that the differential Galois group is only well defined over the differential field $\underline{K} := \overline{C_K}K$. Let $\underline{A}$ and $\underline{B}$ denote $\underline{K} \otimes A$ and $\underline{K} \otimes B$. If G is not the group $A_4^{\mathrm{SL}_2}$, then the symmetric power $sym_{\underline{K}}^4 \underline{A}$ has no 1-dimensional submodule and so the same holds for $sym_K^4 A$. It follows that the only 1-dimensional submodule of $sym_K^2 B$ is the kernel of the canonical morphism $sym_K^2 B \to sym_K^4 A$.
Suppose that G is $A_4^{\mathrm{SL}_2}$. Then by differential Galois theory:
(a) The differential Galois group of $\underline{B}$ is A_4.
(b) $sym_{\underline{K}}^2 \underline{B} \cong M_0 \oplus M_1 \oplus M_2 \oplus \underline{B}$, where M_0, M_1, M_2 are 1-dimensional submodules. The differential Galois group of M_0 is trivial and $M_0 = \underline{L}_0$, where L_0 is the kernel of $sym_K^2 B \to sym_K^4 A$.
(c) $M_i \otimes \underline{B} \cong \underline{B}$ for all i.
(d) The differential Galois group of $M_i,\ i = 1, 2$ is the quotient C_3 of A_4. Thus $sym_{\underline{K}}^3 M_i$ is a trivial module. Moreover $sym_{\underline{K}}^2 M_1 \cong M_2$.

We assume that $sym^2_K B$ has a 1-dimensional submodule $L_1 \neq L_0$. Then $\underline{L}_1$ is either M_1 or M_2. We may suppose that $\underline{L}_1 = M_1$. From the above one concludes that $sym^2_{\underline{K}}(\underline{L}_1 \otimes \underline{A})$ is isomorphic to $\underline{B}$ and that the kernel of $sym^2_{\underline{K}}\underline{B} \to sym^4_{\underline{K}}(\underline{L}_1 \otimes \underline{A})$ is equal to M_2. From 2.3 (a) one concludes that all isomorphisms are defined over the field K. As a consequence $M_2 = \underline{K} \otimes L_2$, where $L_2 := sym^2_K L_1$. In the same way, L_1 is the kernel of the morphism $sym^2_K B \cong sym^2_K(L_2 \otimes B) \to sym^4(L_2 \otimes A)$. An application of lemma 3.1 ends the proof. □

3.2 Examples obtained from quaternion fields

Notations and assumptions.
F is a quaternion algebra over $k = C_k(x)$ with basis $b_0, \ldots, b_3$. The multiplication is given by $b_0 = 1$, $b_i^2 = A_i \in k = C_k(x)$ for $i = 1, 2, 3$, $b_1 b_2 = -b_2 b_1 = b_3$, $A_3 = -A_1 A_2$. Then F is a skew field if and only if the equation $A_1 X^2 + A_2 Y^2 - Z^2 = 0$ has only the trivial solution $(0, 0, 0)$ in the field k (see [Bl], Théorème I-5). We will assume that this is the case. Put $F_i = k(b_i)$ for $i = 1, 2, 3$. These are maximal commutative subfields of F. As before, a differentiation $'$ on F will be a map $f \mapsto f'$ such that $(fg)' = f'g + fg'$ for all $f, g \in F$ and $f' = \frac{df}{dx}$ for any $f \in C_k(x) \subset F$. We note that in general for $f \in F$, the elements f and f' need not commute, in which case $k(f)$ is not a differential subfield of F.

Lemma 3.5 *There is a unique differentiation $'$ on F such that the fields F_1, F_2 are stable under differentiation. The field F_3 is also stable under this differentiation.*

Proof. The condition prescribes $b_0' = 0$ and $b_i' = \frac{A_i'}{2A_i} b_i$ for $i = 1, 2$. From $b_3 = b_1 b_2$ one deduces that $b_3' = \frac{A_3'}{2A_3} b_3$. Thus $(\sum_{i=0}^3 a_i b_i)' = \sum_{i=0}^3 (a_i' + a_i \frac{A_i'}{2A_i}) b_i$, where $A_0 := 1$. On the other hand one can easily verify that this formula defines a differentiation on F. The last statement holds because $b_3' \in F_3$. □

A 1-dimensional module $M = Fe$ over F is described by $\partial e = de$, where $d \in F$ is an arbitrarily chosen element. One can see M as a two-dimensional differential module over the differential field F_1. Let σ denote the non-trivial element of the Galois group of F_1/k. One considers the σ-linear bijection $A(\sigma) : M \to M$, defined by $A(\sigma)m = b_2 m$. One has:
$\partial A(\sigma) = A(\sigma)(\partial + \frac{A_2'}{2A_2})$, or in a shorter notation $\partial b_2 = b_2(\partial + \frac{A_2'}{2A_2})$.

Intermezzo.
One has ${}^{\sigma}M \cong L \otimes_{F_1} M$ for the one-dimensional differential module $L = F_1 b$ over F_1 with $\partial b = \frac{A_2'}{2A_2} b$. Further $L \otimes L$ is isomorphic to the trivial one-dimensional module. As a consequence the 3-dimensional differential module $N := sym^2_{F_1} M$ descends to k. We will make this explicit by a calculation.

On the differential module $N =: sym^2_{F_1} M$ of dimension 3 over F_1 we define an additive operator $B(\sigma) : N \to N$ by the formula $B(\sigma)(m_1 \otimes m_2) = \frac{1}{A_2} b_2 m_1 \otimes b_2 m_2$. The following properties are easily verified: $B(\sigma)$ is σ-linear, commutes with ∂, and $B(\sigma)^2$ is the identity.
Let N^0 denote the subset of N consisting of the elements invariant under $B(\sigma)$. An explicit calculation shows that N^0 is a vector space of dimension 3 over k with basis $n_1^0 = e \otimes e + \frac{1}{A_2} b_2 e \otimes b_2 e, n_2^0 = b_1 e \otimes e - \frac{b_1}{A_2} b_2 e \otimes b_2 e, n_3^0 = b_2 e \otimes e$. Since $B(\sigma)$ and ∂ commute, N^0 is a differential module over k and moreover $N = F_1 \otimes_k N^0$. In other words N descends to k.

M, as differential module over F_1, has basis $e, b_2 e$. The differential module N has basis $n_1 = e \otimes e,\ n_2 = b_2 e \otimes b_2 e,\ n_3 = e \otimes b_2 e$. By lemma 3.1, $sym^2_{F_1} N$ has a 1-dimensional submodule, generated by $n_1 \otimes n_2 - n_3 \otimes n_3$. This expression can be rewritten in the basis n_1^0, n_2^0, n_3^0 and reads

$$\frac{A_2}{4} n_1^0 \otimes n_1^0 - \frac{A_2}{4A_1} n_2^0 \otimes n_2^0 - n_3^0 \otimes n_3^0.$$

Thus $sym^2_k N^0$ contains a one dimensional submodule and the quadratic form associated to this submodule has the form $\frac{A_2}{4} X_1^2 - \frac{A_2}{4A_1} X_2^2 - X_3^2$. This form is equivalent to the quadratic form $A_1 X^2 + A_2 Y^2 - Z^2$ associated to the quaternion field F.

Remark: M, N, and N^0 depend on the choices for F, d, and also F_i. Choosing the F_i determines the differentiation on F, see lemma 3.5.

Theorem 3.6 *Let K be an algebraic extension of k. Let $d \in F$ and view $M = Fe$, with $\partial e = de$, as differential module over F_1. Let $\tilde{F}_1 = F_1 \cdot K$ and assume that $\tilde{F}_1 \otimes_{F_1} M$ is an irreducible and primitive differential module over $\tilde{F}_1$. Then $N_K := K \otimes_k N^0$ is the second symmetric power of a 2-dimensional differential module over K if and only if K is a splitting field for F.*

Proof. The assumption implies that $sym^2 N_K$ contains either 1 or 3 differential submodule of dimension 1. In the latter case, the three non-singular quadrics have rational points in the same fields because of lemma 3.4. The theorem follows from the known generator $\frac{A_2}{4}n_1^0 \otimes n_1^0 - \frac{A_2}{4A_1}n_2^0 \otimes n_2^0 - n_3^0 \otimes n_3^0$ of a 1-dimensional submodule of $sym^2 N_K$, the observation that its associated quadratic form is equivalent to the quadratic form of F, and lemma 3.1. $\Box$

Remarks 3.7
(1) If the differential Galois group of $\underline{M} := \overline{C_k}F_1 \otimes_{F_1} M$ contains SL_2 then the assumption on $\tilde{F}_1 \otimes_{F_1} M$ holds for any K algebraic over k.
(2) Suppose $K = C_K \cdot k$. Then the assumption on $\tilde{F}_1 \otimes_{F_1} M$ is equivalent to M being irreducible and primitive over F_1. Under this assumption, N^0 is irreducible and thus $b_2 e \otimes e \in N^0$ is a cyclic vector. One can explicitly compute the minimal (so the order is 3) monic operator $L_3 \in k[\partial]$ of this cyclic vector. By construction, L_3 is equivalent over F_1 with the second symmetric power of an operator in $F_1[\partial]$. According to 3.6, L_3 is equivalent to the second symmetric power of an operator L_2 with coefficients in a field $C_K \cdot k$, if and only if $C_K \cdot k$ is a splitting field for F.
(3) Suppose $k = C_k(x)$. The Brauer group of $\overline{C_k}(x)$ is trivial. This implies that there exists a finite extension C_K of C_k such that $C_K(x)$ is a splitting field for F.

3.2.1 An example with $A_1 = x$ and $A_2 = s_0 - s_1 x$

We keep the notations of subsection 3.2. Assume that $s_0, s_1 \in \mathbf{Q}$ and $s_0 \neq 0$, $s_1 \neq 0, 1$. The central simple algebra F over $\mathbf{Q}(x)$ need not be a skew field. In fact $K \supset \mathbf{Q}(x)$ is a splitting field for F if and only if the quadratic equation $A_1 X^2 + A_2 Y^2 - Z^2 = 0$ has a solution $(X, Y, Z) \neq (0,0,0)$ in K^3. For $K = C_K(x)$ this condition is equivalent to s_0 and s_1 being squares in C_K. Indeed, if s_0, s_1 are squares, then one easily sees that there are $a, b \in C_K$ such that $xa^2 + (s_0 - s_1 x)b^2 - 1 = 0$. On the other hand, let $(X, Y, Z) \in C_K(x)^3$ be a non trivial solution of the quadratic equation. Then one can normalize this solution such that $X, Y, Z \in C_K[x]$ and the g.c.d. of X, Y, Z is 1. Substitution of $x = 0$ and $x = \frac{s_0}{s_1}$ in the equation $xX^2 + (s_0 - s_1 x)Y^2 - Z^2 = 0$ yields that s_0 and s_1 are squares in C_K.

Now we suppose that not both s_0 and s_1 are squares in $\mathbf{Q}$.
Then F is a quaternion field. Examples of splitting fields for F are:
$\mathbf{Q}(\sqrt{s_0}, \sqrt{s_1})(x)$ or $\mathbf{Q}(\sqrt{x})$ or $\mathbf{Q}(\sqrt{s_0 - s_1 x + m^2 x})$ for any $m \in \mathbf{Q}$. The F-vector space $M = Fe$ is made into a differential module over F by $\partial e = de$

and $d = b_1 + xb_2$. We want to show that M is irreducible and primitive as F_1-differential module. Suppose that M contains a one-dimensional F_1-vector space V, invariant under ∂. Then b_2V is also a 1-dimensional F_1-vector space, invariant under ∂ (indeed, $b_1b_2 = -b_2b_1$ and $b_2' = \frac{A_2'}{2A_2}b_2$). Thus M is always semi-simple over F_1. Then also $sym^2_{F_1}M$ is semi-simple. If M is reducible or imprimitive then $sym^2_{F_1}M$ contains a 1-dimensional submodule over F_1. Being semi-simple, $sym^2_{F_1}M$ contains also a two-dimensional submodule.
A computation shows that the minimal operator L_3 for the cyclic vector $b_2e \otimes e$ of N^0 is equal to:

$$x(s_0 - s_1x)\partial^3 + 3(s_0/2 - s_1x)\partial^2 + (4(s_1-1)x - 3s_1/4 - 4s_0)\partial + 6(s_1 - 1).$$

Therefore one has to show that L_3 has no right hand factor of order 1. This can be verified by a local analysis at the singular points $x = 0, s_0/s_1, \infty$ of L_3. The first two points are regular singular with local exponents $0, 1, 1/2$. The point ∞ is irregular singular and has only one "generalized local exponent" which is unramified, i.e., does not involve a root of the local parameter $\frac{1}{x}$ at ∞. This exponent is $3/2$ and gives a local right hand factor of the form $\partial + 3/2x^{-1} + \cdots$. Let $\partial - u$ be a right hand factor, then u has the form $u = \frac{l_0}{x} + \frac{l_1}{x - s_0/s_1} + \frac{f'}{f}$ with $f \in \overline{\mathbf{Q}}[x]$, where $l_0, l_1 \in \{0, 1, 1/2\}$. This cannot produce the prescribed local right hand factor at ∞.
Let $K = C_K(x)$. From theorem 3.6 one concludes that there exists $L_2 \in K[\partial]$ whose symmetric square is equivalent to L_3, if and only if the equation $A_1X^2 + A_2Y^2 - Z^2 = 0$ has a non trivial solution in K^3, which is equivalent with $\sqrt{s_0}, \sqrt{s_1} \in C_K$.

Observation. One can compute a monic operator $L_2 \in \mathbf{Q}(\sqrt{s_0}, \sqrt{s_1})(x)[\partial]$ with Sym^2L_2 equivalent to L_3 above. Suppose that $\mathbf{Q}(\sqrt{s_0}, \sqrt{s_1})$ has degree 4 over $\mathbf{Q}$. Let σ be a non trivial automorphism of $\mathbf{Q}(\sqrt{s_0}, \sqrt{s_1})$. Then $\sigma(L_2)$ is not equivalent to L_2. But according to theorem 4.7 it must be *projectively equivalent* (see section 4) to L_2. We verified this: Let σ_i interchange $\sqrt{s_i}$ and $-\sqrt{s_i}$, and leave $\sqrt{s_j}$ invariant where $j \neq i$. Let $t_0 = \sqrt{A_1A_2}$ and let $t_1 = \sqrt{A_2}$. Then computer computation (one can compute a basis of homomorphisms between two differential modules, see [P-S]) shows that $\sigma_0(L_2)$ is equivalent to $L_2 \otimes (\partial - \frac{t_0'}{t_0})$ and $\sigma_1(L_2)$ is equivalent to $L_2 \otimes (\partial - \frac{t_1'}{t_1})$. If one of these operators is equivalent to L_2 then (the module corresponding to) L_2 is imprimitive by lemma 4.1. The latter is excluded by the irreducibility of L_3.

3.2.2 Quaternion fields with general A_1 and A_2

One considers elements $A_1, A_2 \in \mathbf{Q}(x)$. F need not be a skew field. One defines ∂ on $M = Fe$ by $\partial e = de$ where $d = b_1 + xb_2$. We exclude the cases $A_1' = 0$ or $A_2 = 0$. Then $b_2 e \otimes e$ is a cyclic vector for N^o and L_3 denotes an operator of order 3 with $L_3(b_2 e \otimes e) = 0$. The operator R of order < 3, with coefficients in a possible larger field $K \supset \mathbf{Q}(x)$ plays the following role. The least common left multiple $\mathrm{LCLM}(R, L_3)$ of R and L_3 has the form $AR = BL_3$ where A is the second symmetric power $Sym^2 L_2$ of an operator $L_2 \in K[\partial]$ of order 2. In other words, R provides the isomorphism $K[\partial]/K[\partial]Sym^2 L_2 \to K[\partial]/K[\partial]L_3$.

$$
\begin{aligned}
L_3 &= 4A_2\partial^3 - 2(A_1'A_2/A_1 + 2A_1''A_2/A_1' - 2A_2')\partial^2 \\
&\quad -(16A_1{A_1'}^2A_2 + {A_2'}^2/A_2 + A_1'A_2'/A_1 + 2A_1''A_2'/A_1' - 2A_2'' + 16)\partial \\
&\quad +8(A_2'/A_2 + A_1'/A_1 + 2A_1''/A_1') \\
R &= uA_2\partial^2 + (2A_1'A_2w + A_2'u/2)\partial + 4A_1'A_2v - 4u
\end{aligned}
$$

where (u, v, w) is a nonzero point on the conic

$$
A_1u^2 + A_2v^2 - w^2 = 0 \tag{1}
$$

Assuming that $K \otimes_{\mathbf{Q}(x)} sym^2 N^o$ has only one submodule of dimension 1, namely the one with generator

$$
\frac{A_2}{4} n_1^0 \otimes n_1^0 - \frac{A_2}{4A_1} n_2^0 \otimes n_2^0 - n_3^0 \otimes n_3^0,
$$

we have a one to one correspondence between all nonzero points $(u, v, w) \in K^3$ on the conic, and all operators $R \in K[\partial]$ of order < 3 with the required property $\mathrm{LCLM}(R, L_3) = Sym^2 L_2 \cdot R$ for some L_2 of order 2. We note that $\overline{\mathbf{Q}}(x)$ is a C_1-field, and hence there is always a field K of the form $C_K(x)$ with $[C_K : \mathbf{Q}] < \infty$ such that (1) has a non-trivial solution. The degree $[C_K : \mathbf{Q}]$ can be arbitrarily high as is shown in the following example:

$$
A_1 = x, \quad A_2 = (x-2)(x-3)(x-5)\cdots(x-p_n),
$$

where p_n is the nth prime number. The smallest field extension C_K of $\mathbf{Q}$ for which (1) has a non-trivial solution in $K = C_K(x)$ is $\mathbf{Q}(\sqrt{2}, .., \sqrt{p_n}, \sqrt{(-1)^n})$.

Remark: For any specific choice, say of $A_1, A_2 \in \mathbf{Q}[x]$ with $A_1' \neq 0 \neq A_2$, we need to verify that L_3 has the desired properties (i.e., N^o is irreducible and $K \otimes_{\mathbf{Q}(x)} sym^2 N^o$ has only one submodule of dimension 1). If one knows in advance that the differential module $\underline{M} := \overline{\mathbf{Q}}F_1 \otimes_{F_1} M$ has a differential Galois group containing SL_2, then this verification is immediate, even if we allow any algebraic extension K of $\mathbf{Q}(x)$. If at a point p formal solutions involve logarithms, then the differential Galois group of $\underline{M}$ contains SL_2. Indeed, the differential Galois group is a reductive group (recall that $\underline{M}$ is semi-simple) and contains the additive group $\mathbf{G}_a$. Examples, somewhat more complicated than before, with this feature are obtained by a different choice for ∂e, namely $\partial e = (\frac{A_1'}{A_1-1}b_0 + \frac{A_1'}{A_1(A_1-1)}b_1 + \frac{A_1'}{A_2}b_2)e$. If A_2 is not a multiple of $A_1 - 1$, then one can verify (it is sufficient to check this for the case $A_1 = x$, $A_2 \in \overline{\mathbf{Q}(x)}$ because one can then generalize the result by applying a pullback $x \mapsto A_1$) that if p is a solution of $A_1 - 1 = 0$ but not of $A_2 = 0$, then this will lead to logarithms at $x = p$. The operator obtained this way is:

$$
\begin{aligned}
L_3 \;=\; & 4\partial^3 + (4B_2 - 12A_1''/A_1' + (6A_1 - 2)A_1'/B_1)\partial^2 \\
& +(2A_2''/A_2 + (3A_1 - 1)A_1'B_2/B_1 - 6A_1''B_2/A_1' - 4A_1'''/A_1' \\
& -B_2^2 + 12(A_1''/A_1')^2 - 2(3A_1 - 1)A_1''/B_1 - 16{A_1'}^2/(A_1(A_1 - 1)^2) \\
& -16{A_1'}^2/A_2)\partial + 8({A_1'}^2 B_2 - (3A_1 - 1){A_1'}^3/A_2)/A_2
\end{aligned}
$$

where $B_1 = A_1(A_1 - 1)$ and $B_2 = A_2'/A_2$.

This operator has the same conic (1). After, if necessary, replacing A_1 with $c^2 A_1$ for some nonzero $c \in \mathbf{Q}(x)$, we obtain that A_2 is not a multiple of $A_1 - 1$. The conic (1) changes into an equivalent one. We conclude that for any algebraic extension K of $\mathbf{Q}(x)$, the operator L_3 is equivalent to a symmetric power of some $L_2 \in K[\partial]$ if and only if (1) has a nonzero solution in K^3. Furthermore, such examples exist for every (up to equivalence) nondegenerate conic over $\mathbf{Q}(x)$.

4 Projective equivalence

Some notations and definitions.

Let k be a differential field with field of constants C_k. Put $\underline{k} = \overline{C_k}k$, where $\overline{C_k}$ is the algebraic closure of C_k. The trivial 1-dimensional differential module is denoted by $\mathbf{1}$. The determinant $\det(M)$ of a differential module M is the 1-dimensional module $\Lambda^n M$, where n is the dimension of M. For a 1-dimensional differential module L, one writes $L^{\otimes n}$ for the tensor product $L \otimes \cdots \otimes L$ of n copies of L.

Two differential modules M_1, M_2 will be called *projectively equivalent* if there exists a differential module L of dimension 1 such that M_2 is isomorphic to $L \otimes M_1$. The translation in terms of monic differential operators $L_1, L_2 \in k[\partial]$ reads as follows: L_1 and L_2 are projectively equivalent if there exists $f \in k$ such that the k-algebra automorphism $\phi_f : k[\partial] \to k[\partial]$, given by $\phi_f(\partial) = \partial + f$, has the property that $\phi_f(L_1)$ is equivalent to L_2. The term "projectively" equivalent comes from the well known fact that multiplication by g is a bijection between the solution spaces of $\phi_{g'/g}(L)$ and L.

The problem. Let M be an irreducible differential module over K of dimension n. Suppose that ${}^{\sigma}M$ is projectively equivalent to M for every $\sigma \in \mathrm{Gal}(K/k)$. The problem is to find the fields $k \subset \ell \subset K$ for which there exists a differential module N, projectively equivalent to M, such that N descends to ℓ. The main case of interest is $K = \underline{k}$ and $\ell = C_\ell k$.

Lemma 4.1 *Suppose that M is irreducible of dimension $n > 1$ over k and that k contains a primitive n^{th}-root of unity. The following are equivalent:*
(1) *There exists a 1-dimensional $L \not\cong \mathbf{1}$ with $L \otimes M \cong M$.*
(2) *There exists a cyclic field extension $k \subset k(t) \not\subset \underline{k}$ with equation $t^d = f \in k$ of degree d dividing n, such that $k(t) \otimes M$ is a direct sum of d irreducible differential submodules over $k(t)$.*

Proof. (1)⇒(2). $\det(M) \cong \det(L \otimes M) \cong L^{\otimes n} \otimes \det(M)$ and so $L^{\otimes n} = \mathbf{1}$. Let d be the minimal divisor of n such that $L^{\otimes d} = \mathbf{1}$. Put $L = ke$ with $\partial e = be$. There exists an element $f \in k^*$ with $\frac{f'}{f} = db$. The isomorphism $M \to M \otimes ke$ can be written as $m \mapsto \phi(m) \otimes e$, where $\phi : M \to M$ is a bijective k-linear map. One finds that $\phi\partial\phi^{-1} = \partial + b$ and $\phi^d\partial\phi^{-d} = \partial + db = f^{-1}\partial f$. Then $f\phi^d$ commutes with ∂ and thus $f\phi^d \in C_k^*$. After changing f we may suppose that $f\phi^d = 1$. One considers the field extension $k(t) \supset k$, given by $t^d = f$. Define $\psi := t\phi : k(t) \otimes M \to k(t) \otimes M$. Then $\psi\partial = \partial\psi$ and $\psi^d = 1$. Let $N_0, \dots, N_{d-1} \subset N =: k(t) \otimes M$ denote the eigenspaces of ψ corresponding to the eigenvalues $\zeta_d^i, i = 0, \dots, d-1$, where ζ_d denotes a primitive d^{th}-root of unity. Then $N = \oplus_i N_i$ and the N_i are submodules of N. We will use a cyclic notation for the N_i, e.g. $N_d = N_0$.
Let $\sigma \in \mathrm{Gal}(k(t)/k)$ be the generator of this Galois group, given by $\sigma(t) = \zeta_d^{-1}t$. Then σ acts also on N and one has $\sigma(N_i) = N_{i+1}$ for all i. Indeed, for $n_i \in N_i$ one has $\psi(\sigma n_i) = t\phi\sigma n_i = t\sigma\phi n_i = \zeta_d\sigma t\phi n_i = \zeta_d\sigma\zeta_d^i n_i = \zeta_d^{i+1}\sigma n_i$. Now suppose that (say) N_0 has a non-trivial submodule N_0'. Then $N' := N_0' \oplus \sigma N_0' \oplus \cdots \oplus \sigma^{d-1}N_0'$ is a non-trivial submodule of N, stable under the

action of σ. Then the set of the σ-invariant elements of N' forms a non-trivial submodule of M. This contradicts the assumptions.

(2)$\Rightarrow$(1). Write again $N = k(t) \otimes M$ and let σ have the same meaning as before. Take an irreducible submodule N_0 of N. Put $N_i := \sigma^i N_0$ for $i = 0, \ldots, d-1$. Then $N' := \sum_{i=0}^{d-1} N_i$ is a differential submodule of N, invariant under the action of σ. The set of the σ-invariant elements of N' forms a non-zero submodule of M. Hence $N' = N$. The assumption in (2) implies that $N = \oplus_{i=0}^{d-1} N_i$. Define the $k(t)$-linear map $\psi : N \to N$, by $\psi n_i = \zeta_d^i n_i$ for any $i = 0, \ldots, d-1$ and any $n_i \in N_i$. Then $\psi\partial = \partial\psi$ and $\psi\sigma = \zeta_d \sigma\psi$. Define the $k(t)$-linear $\phi : N \to N$ by $\phi = t^{-1}\psi$. Then $\phi\partial\phi^{-1} = \partial + \frac{f'}{df}$ and $\sigma\phi = \phi\sigma$. The last equality implies that $\phi(M) = M$ and that the restriction ϕ' of ϕ to M is a k-linear bijection. The relation $\phi'\partial = (\partial + \frac{f'}{df})\phi'$ implies that $L \otimes M$ is isomorphic to M, where $L = ke$ is given by $\partial e = \frac{f'}{df} e$. This L is not trivial because if $f'/df = t'/t$ equals g'/g for some $g \in k$ then $t \in \underline{k}$ which contradicts the assumptions. $\square$

Example. Case 3 in the table in section 1 implies part (1) of the lemma.

Remarks. An irreducible differential module M of dimension $n > 1$ will be called *cyclic-imprimitive* if M satisfies property (2) (and thus also property (1)) of lemma 4.1. We recall that an irreducible action of a group G on a finite dimensional vector space V is called *imprimitive* if V has a direct sum decomposition $V = V_1 \oplus \cdots \oplus V_d$ (with $d > 1$) such that G permutes the V_i. This induces a homomorphism $G \to S_d$ which has as image a transitive subgroup of S_d since the action of G is irreducible. The action of G is called *cyclic-imprimitive* if the image of $G \to S_d$ is a cyclic group of order d.

If C_k is algebraically closed then the solution space V of the irreducible differential module M and the action of the differential Galois group G on V is well defined. In this situation, it is easily seen that M is cyclic-imprimitive if and only if the action of G on V is cyclic-imprimitive.

Corollary 4.2 *Let $k = C_k(x)$ and $\underline{k} = \overline{C_k}(x)$ and let M_1, M_2 be differential modules over $\underline{k}$, which descend to differential modules N_1, N_2 over k. Suppose that M_1 and M_2 are projectively equivalent and that M_1 is not cyclic-imprimitive. Then N_1 and N_2 are projectively equivalent.*

Proof. There is a one-dimensional module L over $\underline{k}$, unique up to isomorphism because M_1 does not satisfy 4.1 (1), such that $L \otimes M_1 \cong M_2$. For any

σ in the Galois group of $\underline{k}/k$ one has ${}^{\sigma}L \otimes {}^{\sigma}M_1 \cong {}^{\sigma}M_2$. Since ${}^{\sigma}M_i \cong M_i$ for $i = 1, 2$, one has ${}^{\sigma}L \cong L$. By 2.8, there exists a one dimensional L_0 over k with $L \cong \underline{k} \otimes L_0$. The two modules $L_0 \otimes N_1$ and N_2 are isomorphic after tensoring with $\underline{k}$ over k. By 2.3, $L_0 \otimes N_1$ is isomorphic to N_2. $\square$

Suppose M_1, M_2 are 2-dimensional differential modules over $\underline{k}$, are irreducible, projectively equivalent, have imprimitive differential Galois group $D_n^{\mathrm{SL}_2}$, and descend to the modules N_1, N_2 defined over k. Up to isomorphism, the number of one-dimensional modules L for which $L \otimes M_1 \cong M_2$ is 4 if $n = 2$ and 2 if $n > 2$. This provides an upper bound for the degree of the extension of C_k needed for N_1 and N_2 to become projectively equivalent. Example 4.3 shows that this bound is sharp.

Example 4.3 Let N_1, N_2 denote the differential modules over $\mathbf{Q}(x)$ defined by the differential operators

$$L_1 = \partial^2 + \frac{3(5x^4 - 2)}{2x^2(x^4 - 2)^2} \quad \text{and} \quad L_2 = \partial^2 - \frac{3x^2(x^4 - 10)}{4(x^4 - 2)^2}$$

The modules N_1, N_2 are not projectively equivalent. But they become projectively equivalent after extending the constants with a solution of the equation $x^4 + 2 = 0$ (not $x^4 - 2$ as the denominators would suggest). The differential Galois group is $D_2^{\mathrm{SL}_2}$.

For $D_n^{\mathrm{SL}_2}$ with $2 < n < \infty$ we give an example that requires a quadratic extension. Take $c \in \mathbf{Q}$, not a square. Take $L_1, L_2 \in \mathbf{Q}(x)[\partial]$ with 3 regular singularities $\sqrt{c}, -\sqrt{c}, \infty$, as follows: Both L_1 and L_2 have exponent-difference $1/2$ at $\pm\sqrt{c}$. Let L_1 resp. L_2 have exponent-difference $\frac{1}{n}$ resp. $1 + \frac{1}{n}$ at $x = \infty$. Then the $\mathbf{Q}(x)[\partial]$-modules corresponding to L_1, L_2 are not projectively isomorphic, but become projectively isomorphic after extending the constants with $\sqrt{c}$.

Theorem 4.4 *Let K be Galois over k. Let M be an irreducible, not cyclic-imprimitive, differential module of dimension $n > 1$ over K such that* $\det(M)$ *descends to k. Suppose that for any $\sigma \in \mathrm{Gal}(K/k)$ the twisted differential module ${}^{\sigma}M$ is projectively equivalent to M. Then:*
(1) M induces a 2-cocycle class $\overline{c} \in H^2(\mathrm{Gal}(K/k), K^*)$, having an order d with $d|n$. Let F denote the simple algebra with center k corresponding to $\overline{c}$.
(2) A field $k \subset \ell \subset K$ is a splitting field for F if and only if M is projectively equivalent to some N which descends to ℓ.

Proof. (1) For any $\sigma \in \mathrm{Gal}(K/k)$ there is an isomorphism $A(\sigma) : M \stackrel{\cong}{\to} L(\sigma) \otimes {}^{\sigma}M$ with $L(\sigma)$ a differential module of dimension 1, unique up to isomorphism. In particular, $L(\sigma_1\sigma_2) \cong L(\sigma_1) \otimes {}^{\sigma_1}L(\sigma_2)$. From $\det({}^{\sigma}M) = \det(M) = L(\sigma)^{\otimes n} \otimes \det({}^{\sigma}M)$ one concludes that $L(\sigma)^{\otimes n} = \mathbf{1}$. After fixing a basis $e(\sigma)$ for each $L(\sigma)$, one identifies $L(\sigma) \otimes {}^{\sigma}M$ with M by $e(\sigma) \otimes m \mapsto m$. Then $A(\sigma)$, seen as a σ-linear map $M \to M$, has the property:
$A(\sigma)\partial = (\partial + a(\sigma))A(\sigma)$ with $a(\sigma) \in K$ given by $\partial e(\sigma) = a(\sigma)e(\sigma)$.
One has $c(\sigma_1, \sigma_2)A(\sigma_1\sigma_2) = A(\sigma_1)A(\sigma_2)$ with $c(\sigma_1, \sigma_2) \in K^*$. Moreover $a(\sigma_1\sigma_2) = a(\sigma_1) + \sigma_1(a(\sigma_2)) + \frac{c(\sigma_1,\sigma_2)'}{c(\sigma_1,\sigma_2)}$. The collection $\{c(\sigma_1, \sigma_2)\}$ defines a 2-cocycle with class $\overline{c} \in H^2(\mathrm{Gal}(K/k), K^*)$. The 2-cocycle class $\overline{c}^n$ is associated to the differential module $\det(M)$. By assumption, $\det(M)$ descends to k and thus $\overline{c}^n = 1$.
(2) It suffices to consider the case $\ell = k$. Suppose that $\overline{c} = 1$, then one may suppose that $c(\sigma_1, \sigma_2) = 1$ for all σ_1, σ_2. Now $\{a(\sigma)\}$ is a 1-cocycle with values in K. Such a 1-cocycle is trivial and thus has the form $a(\sigma) = \sigma(b) - b$ for a certain $b \in K$. The differential module $N = M \otimes Ke$, with $\partial e = be$, descends to k. Indeed, for N one has that the corresponding maps $A(\sigma)$ commute with ∂ and $A(\sigma_1)A(\sigma_2) = A(\sigma_1\sigma_2)$ holds for all σ_1, σ_2.
On the other hand, if N with property (2) is given, then clearly $\overline{c} = 1$. □

Example 4.5 *A skew field F of dimension 9 over $\mathbf{Q}(x)$.*
Let α be a root of the polynomial z^3-3z-1. Then $\mathbf{Q}(\alpha)$ is Galois over $\mathbf{Q}$. Let σ be the automorphism that sends α to $2 - \alpha^2$. Let F be the skew field with center $\mathbf{Q}(x)$, with basis $1, b, b^2$ as $\mathbf{Q}(\alpha, x)$-vector space, and multiplication rules $b^3 = x$ and $bf = \sigma(f)b$.

We turn the vector space Fe into a $\mathbf{Q}(\alpha, x)[\partial]$-module by defining $\alpha' = 0$, $b' = \frac{b}{3x}$ and $\partial e = \frac{\alpha+b}{x}e$. Taking a cyclic vector then leads to the following operator:

$$L = L_0L_1L_2 - x \quad \text{where} \quad L_i = x\partial - \sigma^i(\alpha) - i/3.$$

Now L, $\sigma(L)$, $\sigma^2(L)$ are not equivalent but are projectively equivalent. They are not projectively equivalent to an element of $\mathbf{Q}(x)[\partial]$.

If we increase our differential field to $\mathbf{Q}(\alpha, x^{1/3})$ then these three modules become isomorphic and descend to a module over $\mathbf{Q}(x^{1/3})$ given by the following operator

$$\begin{aligned} &9x^3(x+1)\partial^3 + 3x^2(9 - x^{\frac{1}{3}} + x^{\frac{2}{3}} + 8x)\partial^2 - 3x(6 + 2x^{\frac{1}{3}} - x^{\frac{2}{3}} \\ &\quad +7x + x^{\frac{4}{3}})\partial - 9 + 5x^{\frac{1}{3}} - 11x^{\frac{2}{3}} - 10x - 3x^{\frac{4}{3}} - 3x^{\frac{5}{3}} - 9x^2 \end{aligned}$$

This operator was obtained through a cyclic vector computation of Fe, but this time viewed as $\mathbf{Q}(b)[\partial]$-module.

Remarks 4.6
(1) Let the differential module M over K of dimension $n > 1$ satisfy the assumptions of theorem 4.4. Then $sym^n_K M$ descends to k. Indeed, the 2-cocycle associated to this module is $\overline{c}^n = 1$.
(2) A converse for (1) can be obtained from 4.2 and 4.7 below when $n = 2$, $K = \underline{k}$ and M is not (cyclic)-imprimitive.
(3) We recall the classification of irreducible algebraic subgroups of $\mathrm{SL}_2(C)$, where C is an algebraically closed field of characteristic 0

$$D_\infty^{\mathrm{SL}_2},\ D_n^{\mathrm{SL}_2},\ A_4^{\mathrm{SL}_2},\ S_4^{\mathrm{SL}_2},\ A_5^{\mathrm{SL}_2},\ \mathrm{SL}_2(C).$$

The first five groups are the preimages in $\mathrm{SL}_2(C)$ of the subgroups D_∞^{pr}, D_n, A_4, S_4 and A_5 of $\mathrm{PSL}_2(C)$. Further D_∞^{pr} is the projective dihedral group consisting of the elements of $\mathrm{PSL}_2(C)$ which stabilize the subset $\{0, \infty\}$ of $\mathbf{P}^1(C)$. Using this classification we will prove theorem 4.7.
(4) Theorem 4.7 below does not hold for higher symmetric powers. We give two examples where M_1, M_2 are not projectively equivalent, and $sym^3 M_1 \cong sym^3 M_2$. Let $E(Q)$ be the one-dimensional module given by $\partial e = Q/x\ e$. Then $E(Q_1) \otimes E(Q_2) \cong E(Q_1 + Q_2)$ and $E(1) \cong E(0)$.
(i). $M_1 = E(0) \oplus E(\frac{1}{5})$ and $M_2 = E(\frac{1}{15}) \otimes (E(0) \oplus E(\frac{2}{5}))$.
(ii). $M_1 = E(0) \oplus E(\frac{1}{10}) \oplus E(\frac{3}{10})$ and $M_2 = E(\frac{1}{6}) \otimes (E(0) \oplus E(\frac{-1}{10}) \oplus E(\frac{-3}{10}))$.

Theorem 4.7 *Let M_1, M_2 denote differential modules over $\underline{k}$ of dimension 2. If $sym^2_{\underline{k}} M_1 \cong sym^2_{\underline{k}} M_2$, then there exists a one-dimensional differential module L over $\underline{k}$ such that $M_2 \cong L \otimes M_1$.*

Proof. The theorem is in fact a statement concerning representations. The translation is as follows. Let $\mathcal{U}$ denote the universal differential Galois group of the field $\underline{k}$. The category of the differential modules over $\underline{k}$ is equivalent to the category of the finite dimensional C-linear representations of the affine group scheme $\mathcal{U}$. Here $C = C_{\underline{k}}$ is the field of constants of $\underline{k}$. One associates to a differential module M over $\underline{k}$ its solution space V equipped with the action of $\mathcal{U}$. Let $\rho_i : \mathcal{U} \to \mathrm{GL}(V_i)$ for $i = 1, 2$, denote the representations associated to M_i. Put $W_i = sym^2 V_i$ equipped with the induced representation $sym^2 \rho_i$. There is given an isomorphism $B : W_1 \to W_2$ between the two representations. Now it suffices to show that there exists a

C-linear bijection $A : V_1 \to V_2$ such that $sym^2 A = B$. Indeed, for any $g \in \mathcal{U}$ one has that $A\rho_1(g)A^{-1}$ and $\rho_2(g)$ have the same second symmetric power. Hence there exists a $\chi(g) \in \{\pm 1\}$ such that $A\rho_1(g)A^{-1} = \chi(g)\rho_2(g)$. The map $g \in \mathcal{U} \mapsto \chi(g) \in \{\pm 1\}$ is a one dimensional representation and corresponds to a one-dimensional differential module L over $\underline{k}$. It follows that $M_1 \cong L \otimes M_2$.

Since we are dealing with only two differential modules M_1 and M_2, we may replace in the sequel the (somewhat fancy) affine group scheme $\mathcal{U}$ by the differential Galois group of $M_1 \oplus M_2$, which is an ordinary linear algebraic group over C.

As before, one considers the canonical surjective map $sym^2_C W_i \to sym^4 V_i$ and its one-dimensional kernel K_i for $i = 1, 2$. One observes that a C-linear bijection $B : W_1 \to W_2$ has the form $sym^2 A$ for some C-linear bijection $A : V_1 \to V_2$ if and only if $sym^2 B : sym^2_C W_1 \to sym^2_C W_2$ maps K_1 to K_2.

Let G_i denote the image of ρ_i. The isomorphism between W_1 and W_2 implies that the induced morphisms $\mathcal{U} \to G_i/\{\pm 1\},\ i = 1, 2$ coincide.

(1a) Suppose that V_1 is reducible and that it has precisely one proper invariant subspace L_1. It easily follows that the only non-trivial invariant subspaces of W_1 are $L_1 \otimes L_1$ and $L_1 \otimes V_1$. Also V_2 has a unique proper invariant subspace L_2, since $G_1/\{\pm 1\} \cong G_2/\{\pm 1\}$. Thus $L_1 \otimes V_1$ is isomorphic to $L_2 \otimes V_2$. Hence $V_2 \cong L_1 \otimes L_2^{-1} \otimes V_1$.

(1b) Suppose that V_1 has at least two proper invariant subspaces. Then the same is true for V_2 because $G_1/\{\pm 1\} \cong G_2/\{\pm 1\}$. Let $\mathbf{1}$ be the trivial character, and write $V_i = \chi_i' \otimes (\mathbf{1} \oplus \chi_i)$ form some characters χ_i, χ_i'. Then $W_i = {\chi_i'}^2 \otimes (\mathbf{1} \oplus \chi_i \oplus \chi_i^2)$. Denote $|\chi_i| \in \{1, 2, \ldots, \infty\}$ as the order of χ_i. Consider the set $S_i = \{\chi_i^j | j = -2, \ldots, 2\}$ of all quotients of the characters appearing in W_i. This is a group $< \chi_i >$ if and only if $|\chi_i| \leq 5$, otherwise S_i is a set with 5 elements. Since $W_1 \cong W_2$ one sees that $S_1 = S_2$. From this equality (if $|\chi_1| = 5$ one needs $W_1 \cong W_2$ as well) one can derive that $\chi_2 \in \{\chi_1, \chi_1^{-1}\}$, which implies that V_1 is projectively equivalent to V_2.

(2) Now we consider the case where G_1 is irreducible. After multiplying ρ_1 by a character, one may assume that $G_1 \subset \mathrm{SL}_2$. The isomorphism between W_1 and W_2 implies that the image G_2 of the second representation lies in $\{Z \in \mathrm{GL}_2 | \det(Z)^3 = 1\}$. Using the above notations, we will show that there is a choice of the isomorphism B between W_1 and W_2 such that $sym^2(B)$ maps K_1 to K_2.

(2a) If $G_1 \in \{S_4^{\mathrm{SL}_2}, A_5^{\mathrm{SL}_2}, \mathrm{SL}_2(C)\}$, then $sym^4 V_i,\ i = 1,2$ has no invariant one-dimensional subspace. Then $sym^2 W_i,\ i = 1,2$ has only K_i as invariant subspace of dimension 1. Hence $B(K_1) = K_2$ and we are done.

(2b) If $G_1 = D_\infty^{\mathrm{SL}_2}$, then we have to make a more detailed calculation. Let $\{v_1, v_2\}$ be a basis of V_1 such that G_1 consists of the transformations with determinant 1 which permute the two lines Cv_1, Cv_2 in V_1. Then $b_1 = v_1 \otimes v_1, b_2 = v_2 \otimes v_2, b_3 = v_1 \otimes v_2$ is a basis of $W_1 = sym_C^2 V_1$. The space W_1 is the direct sum of the irreducible representations $Cb_1 \oplus Cb_2$ and Cb_3. The space $sym_C^2 W_1$ is the sum of the irreducible representations $Cb_1 \otimes b_1 + Cb_2 \otimes b_2$, $Cb_1 \otimes b_2$, $Cb_1 \otimes b_3 + Cb_2 \otimes b_3$ and $Cb_3 \otimes b_3$. The family of all invariant lines in $sym_C^2 W_1$ is $C(\lambda b_1 \otimes b_2 + \mu b_3 \otimes b_3)$ with $\lambda, \mu \in C$, not both zero. Each member of the family defines a quadric in W_1. The family has two special members namely $Cb_1 \otimes b_2$ and $Cb_3 \otimes b_3$, where the quadric consists of two lines or a double line. The situation is similar for W_2 and $sym^2 W_2$ (with adapted notations $v_1', v_2', b_1', b_2', b_3'$). Thus the isomorphism $B : W_1 \to W_2$ sends the family of quadrics of W_1 to the one of W_2. The special quadrics are mapped to the special quadrics and one concludes that Bb_3 is a multiple of b_3' and $\{Bb_1, Bb_2\}$ are multiples of $\{b_1', b_2'\}$. One has the freedom to change the isomorphism B by prescribing $Bb_3 = \lambda b_3'$ for any $\lambda \in C^*$. In this way one obtains that $sym^2 B$ maps the line K_1 with generator $b_1 \otimes b_2 - b_3 \otimes b_3$ to the line K_2 with generator $b_1' \otimes b_2' - b_3' \otimes b_3'$. Thus the changed B is a $sym^2 A$. For $G_1 = D_n^{\mathrm{SL}_2}$ with $n > 2$ the same proof works. Note that $sym^2 B$ depends quadratically on λ, which explains why $\sqrt{c}$ is needed in example 4.3.

(2c) Assume now that $G_1 = A_4^{\mathrm{SL}_2}$. Then W_1 is the irreducible representation D of $G_1/\{\pm 1\} = A_4$ of dimension 3. Further $sym^2 W_1$ is the direct sum of three invariant lines $L_1(0), L_1(1), L_1(2)$ and D. The group $G_1/\{\pm 1\} = A_4$ acts trivially on $L_1(0)$ which is the kernel K_1 of $sym^2 W_1 \to sym^4 V_1$. The action of G_1 on the other two lines is given by the two non-trivial characters of A_4. The space $sym^2 W_2$ has a similar decomposition $L_2(0) \oplus L_2(1) \oplus L_2(2) \oplus D$. The notation is chosen such that $L_2(0)$ is the kernel K_2 of $sym^2 W_2 \to sym^4 V_2$. Again, $L_2(0), L_2(1), L_2(2)$ correspond to the three 1-dimensional characters of $G_2/\{\pm 1\} = A_4$. However, $L_2(0)$ need not correspond to the trivial character of A_4 and B need not satisfy $sym^2(B)K_1 = K_2$. We will address this problem using the cyclic-imprimitivity of D.

We replace V_2 by $V_2' := L_2(0) \otimes V_2$. This new representation has the same kernel as ρ_2. Put $W_2' = sym^2 V_2'$. This representation has the same kernel as $sym^2 \rho_2$. The image of $sym^2 \rho_2$ is identified with A_4. As representations of A_4

the two objects $L_2(0)^{\otimes 2} \otimes D$ and D are isomorphic, since there is only one irreducible representation of A_4 of dimension 3. Thus $sym^2 V_2$ and $sym^2 V_2'$ are isomorphic. Then $sym^2 V_1 \cong sym^2 V_2'$. Let B' denote the isomorphism. The decomposition of $sym^2 W_2'$ is

$$L_2(0)^{\otimes 3} \oplus (L_2(1) \otimes L_2(0)^{\otimes 2}) \oplus (L_2(2) \otimes L_2(0)^{\otimes 2}) \oplus D,$$

where $L_2(0)^{\otimes 3}$ is the kernel K_2' of $sym^2 W_2' \to sym^4 V_2'$. Now, as required, $sym^2(B')K_1 = K_2'$ and we conclude that V_1 and V_2' differ by a character. Hence V_1 and V_2 differ by a character.

(2d) Assume that $G_1 = D_2^{\mathrm{SL}_2}$.
Consider a two-dimensional vector space V and a representation $\rho : \mathcal{U} \to \mathrm{SL}(V)$ with image $D_2^{\mathrm{SL}_2}$. For a suitable basis v_1, v_2 of V the space $W = sym^2 V$ is a direct sum of the three invariant lines L_1, L_2, L_3 with generators $e_1 := v_1 \otimes v_1 + v_2 \otimes v_2$, $e_2 := v_1 \otimes v_1 - v_2 \otimes v_2$ and $e_3 := v_1 \otimes v_2$. They correspond to the three characters of D_2 having order two. Then $sym^2 W$ is a direct sum of the 3-dimensional space T spanned by $e_i \otimes e_i,\ i = 1, 2, 3$, having trivial D_2-action, and the three lines $L_1 \otimes L_2,\ L_1 \otimes L_3,\ L_2 \otimes L_3$. These lines correspond again to the three characters of D_2 of order two. The line K, kernel of $sym^2 W \to sym^4 V$, lies in T and is generated by an element $\sum_{i=1}^3 c_i e_i \otimes e_i$ with non-zero $c_1, c_2, c_3 \in C$. For any other element $\sum_{i=1}^3 d_i e_i \otimes e_i$ in T with all $d_i \neq 0$, there is an automorphism D of the representation W such that $sym^2 D$ maps the given element $\sum_{i=1}^3 c_i e_i \otimes e_i$ to $\sum_{i=1}^3 d_i e_i \otimes e_i$. Indeed, take D of the form $De_i = \lambda_i e_i$ for $i = 1, 2, 3$ where $\lambda_i^2 = d_i / c_i$.
Consider, as before, two representations (V_i, ρ_i) of $\mathcal{U}$ having dimension 2, such that the image G_1 of ρ_1 is $D_2^{\mathrm{SL}_2}$. Let an isomorphism $B : W_1 \to W_2$ be given. Using the automorphism D above, one changes B into B' such that $sym^2 B'$ maps K_1 to K_2. □

The following explains the constructions with quaternions in section 3.

Corollary 4.8 *Suppose that N is an irreducible differential module over $\underline{k}$ of dimension 3, which descends to k. Assume that $sym^2 N$ has a 1-dimensional submodule, such that the corresponding quadratic form has a $\underline{k}$-rational point. Then:*
(1) *There exists a differential module M over $\underline{k}$ with $sym^2 M \cong N$. For every $\sigma \in \mathrm{Gal}(\underline{k}/k)$ the modules ${}^{\sigma}M$ and M are projectively equivalent.*
(2) *Let $\overline{c} \in H^2(\mathrm{Gal}(\underline{k}/k), \underline{k}^*)$ denote the 2-cocycle of order 1 or 2, associated*

to M. Let F be the quaternion algebra over k associated to $\overline{c}$. An algebraic extension $C_{\tilde{k}} \supset C_k$ yields a splitting field $\tilde{k} = C_{\tilde{k}}k$ for F if and only if there exists a differential module $\tilde{M}$ over $\tilde{k}$ such that $\underline{k} \otimes_{\tilde{k}} sym^2_{\tilde{k}}\tilde{M}$ is isomorphic to N.

Proof. Apply 3.2, 3.1, 4.7 and 4.4 (observe that the differential Galois group of M is irreducible and primitive since N is irreducible). $\square$

References

[A] A.S. Amitsur - *Differential polynomials and division algebras.* - Ann. of Math. (2) **59**, p. 245-278, 1954.

[Bl] A. Blanchard - *Les corps non commutatifs* - Collection SUP, no 9, Presses universitaires de France, 1972.

[Bo] N. Bourbaki - *Éléments de mathématiques, Algèbres, Chapitre 8* - Hermann, Paris, 1958.

[C-W] E. Compoint, J-A. Weil - *Absolute reducibility of differential operators and Galois groups* - Preprint 2002.

[H-P] P.A. Hendriks and M. van der Put - *Galois action on solutions of a differential equation* - J. Symbolic Computation, **19**, 559-576, 1995.

[H] M. van Hoeij - *Factorization of Linear Differential Operators* - Ph.D. thesis, University of Nijmegen, 1996.

[L] A.H.M. Levelt - *Jordan decomposition for a class of singular differential operators* - Ark. Mat. **13**, p. 1-27, 1975.

[P-S] M. van der Put and M. Singer - *Differential Galois Theory* - to appear, Grundlehren der Mathematik, Springer Verlag, 2002. Available at: http://www4.ncsu.edu/~singer/ms_papers.html

[Ren] G. Renault - *Algèbre non commutative* - Gauthier-Villars, Paris, Bruxelles, Montreal, 1975.

[Rei] I. Reiner - *Maximal Orders* - Academic Press, London, 1975.

[S] J.-P. Serre - *Corps locaux* - Hermann, Paris, 1968.

[Si] M.F. Singer - *Solving homogeneous linear differential equations in terms of Second Order Linear Differential Equations* - American J. of Math., **107**, 663-696, 1985.

[So] R. Sommeling - *Characteristic classes for irregular singularities* - Ph.D. thesis, University of Nijmegen, 1993.