# 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 we 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

## 1.1 Examples of descent phenomena

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 $\sigma$ 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 $\partial$. If $L \in k[\partial]$ then $L$ is called *rational*. Two operators $L_1, L_2$ 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 $k[\partial]$.
- $E_R$    Equivalent to an element of $k[\partial]$.
- $E_C$    Equivalent to all its conjugates over $k$.
- $E_R^p$    Projectively equivalent to an element of $k[\partial]$.
- $E_C^p$    Projectively equivalent all its conjugates over $k$.

The following implications are obvious:

$$\text{R} \implies \text{E}_R \implies (\text{E}_C \text{ and } \text{E}_R^p), \qquad (\text{E}_C \text{ or } \text{E}_R^p) \implies \text{E}_C^p.$$

These implications leave seven possible combinations for the truth-values of $\text{R}, \text{E}_R, \text{E}_C, \text{E}_R^p, \text{E}_C^p$. 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 | $E_R$ | $E_C$ | $E_R^p$ | $E_C^p$ | Example |
|------|---|-------|-------|---------|---------|---------|
| 1 | Y | Y | Y | Y | Y | $\partial$ |
| 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 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 $\text{E}_C$ but not $\text{E}_R$. 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 the descent phenomenum "$\text{E}_C$ without $\text{E}_R$" (case 3 or 4) is related to skew fields $F^o$ of finite dimension over their center $C_k$. The main result in section 2 is that any such skew field yields examples for "$\text{E}_C$ without $\text{E}_R$". Case 6 (a descent phenomenum

up to projective equivalence) 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 $k$. The main result in section 3 is that all skew fields of this type (all non-degenerate conics) produce examples for case 6. For most of our constructions it will be more convenient to use modules instead of operators. We used operators in the above table for compactness of notation.

## 1.2 Descent problems

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 obstruction to descent is a 2-cocycle which corresponds to a skew field, see theorem 2.10 and proposition 2.11 for a general differential field $k$, with additional results for $k = C_k((x))$ in theorem 2.4 and for $k = C_k(x)$ in theorem 2.8. In section 2.4 we show how all possible examples over $k = C_k(x)$ can be constructed. For completeness, Amitsur's completely different construction (which makes a very special case of the descent problem explicit, namely part (a) of proposition 2.11) is presented in section 2.5.

In section 3 we study the problem whether a 3-dimensional differential module $M$ is the second symmetric power of a 2-dimensional differential module $N$. At the heart of the rationality issues in this problem is a conic, and we show that every conic over $k = C_k(x)$ occurs. A surprising result is theorem 4.7 in section 4, which states that the isomorphism class of a solution $N$ of this problem is unique up to tensoring with 1-dimensional modules, if the field of constants is algebraically closed. This implies that the rationality issues in section 3 can also be viewed as a "projective descent problem", which is the subject of theorem 4.4. In this type of descent problem we consider modules that are not necessarily isomorphic to their conjugates, but only isomorphic up to tensoring with 1-dimensional modules.

## 1.3 Motivation and overview of the main results

In section 2.3 we follow standard Galois cohomology techniques to describe descent phenomena for differential modules. This way one can explain the descent phenomena in terms of 2-cocycles or skew fields, and classify descent phenomena in one direction "a differential module that is isomorphic to its

conjugates $\Longrightarrow$ a skew field" but not in the opposite direction: Which skew fields occur this way? Our goal is a thorough classification and hence we study this question in detail for several common differential fields. In theorem 2.4 in section 2.1 we show that over the field of formal Laurent series only the trivial case occurs (there is no obstruction to descent) whereas in section 2.4 we show that over the rational functions every skew field occurs. Each of these results require completely different techniques. The key ingredient in our construction "skew field $\Longrightarrow$ differential module" is the introduction of differential modules over skew fields, which are then viewed as differential modules over a commutative subfield. To illustrate this idea we give explicit examples. We then give an construction that we prove to be complete (it provides explicit examples for every skew field, and every example can be constructed this way). Our construction also implies an interesting complexity result, namely that factoring fourth order operators in $\mathbf{Q}(x)[\partial]$ is at least as hard as finding rational points on a conic over $\mathbf{Q}$, a problem related to factoring integers, which is generally assumed to be very hard.

One of the motivations to study the descent problem is the question which extensions of the constants need to be considered in algorithms for solving differential equations, and the results in section 2 are of interest for factoring differential operators.

Section 3 is motivated by the problem of trying to reduce a third order linear differential equation to a second order equation by determining if the corresponding 3-dimensional differential module is the symmetric square of a 2-dimensional module. This problem requires finding a point on a conic that is defined over the differential field $k$. Such a conic corresponds to a skew field of dimension 4 over its center $k$. A natural question is: Can every conic occur? For the formal Laurent series again only the trivial case occurs, but for the rational functions $k = C_k(x)$ we show explicitly in section 3.2 that every conic over $k$ occurs. This result implies that if an algorithm tries to reduce a third order differential equation by trying to write the corresponding module as a symmetric square, then a high degree extension of the constants could be necessary, see section 3.2.2. Our construction in section 3 differs from the one in section 2, it uses skew fields over $k$ instead of over $C_k$ (the field of constants of $k$).

In theorem 4.7 in section 4 we show that if a 3-dimensional differential module is the symmetric square of a 2-dimensional module, then this 2-dimensional module is unique up to projective equivalence, provided that the field of constants is algebraically closed. Corollary 4.2 shows that this

4

is then also true over $C_k(x)$ without $C_k$ algebraically closed except in the imprimitive case, and to complete the result we give counter examples for the imprimitive case in examples 4.3. The conic occurs in sections 3 and 4 as 1-dimensional submodule of the symmetric square of a 3-dimensional module. How to view the skew field that corresponds to this conic in terms of Galois cohomology is shown in theorem 4.4 combined with 4.7.

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 $\sigma$ 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 $\lambda * v := \sigma^{-1}(\lambda)v$ for all $\lambda \in K$ and $v \in V$. One has $^{\sigma_1}\left(^{\sigma_2}V\right) = {}^{\sigma_1\sigma_2}V$. 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. If $b$ is the matrix of $f$ with respect to a basis of $V$ and a basis of $W$, then $\sigma(b)$ is the matrix of $^\sigma f$ with respect to the same bases. Here $\sigma$ acts on $b$ by acting on the entries.

Let $V$, $W$ be $K$-vector spaces and let $\sigma$ be an automorphism of $K$. The map $f : V \to W$ is called $\sigma$-*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 $f : {}^\sigma V \to W$ we associate a $\sigma$-linear map $F : V \to W$ by composing the set-theoretic identity $V \to {}^\sigma V$ with $f$.

**Observation**: Let $K \supset k$ be a finite Galois extension with Galois group $G$. *Let $V$ be a vector space over $K$. Then there exists a natural linear map from $K \otimes_k V$ to $^\sigma V$, and a natural isomorphism from $K \otimes_k V$ to $\oplus_{\sigma \in G} {}^\sigma V$.*

The maps are given by $a \otimes v \mapsto a * v = \sigma^{-1}(a)v$. The map to $\oplus_{\sigma \in G} {}^{\sigma}V$ is one to one (hence onto by comparing dimensions) because of the linear independence of automorphisms.

**Definitions 2.2** *Descent data and the descent problem.*
(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 $\mathcal{D}$-module ${}^{\sigma}M$ is $M$ as additive group, has a new scalar multiplication as defined in 2.1 and has the same operator $\partial$.

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 $\sigma(L)$.

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

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

Let $\Phi(\sigma) : M \to M$ be the $\sigma$-linear map associated to $\phi(\sigma)$. Then the two conditions can be formulated as follows:

(i) $\Phi(\sigma) : M \to M$ is a $\sigma$-linear bijection, commuting with $\partial$,
(ii) satisfying $\Phi(\sigma)\Phi(\tau) = \Phi(\sigma\tau)$ for all $\sigma, \tau \in G$.

The above definition coincides with the one used in algebraic geometry. Indeed, let $K/k$ be a finite Galois extension. The algebra $K \otimes_k K$ has a left and a right $K$-algebra structure. 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. The first part (I) of the descent data is a $K \otimes_k K$-linear isomorphism $N_l \to N_r$ which commutes with $\partial$. The second part (II) of the descent data is a relation between the various structures on $(K \otimes_k K \otimes_k K) \otimes_K M$. Now $N_l$ is isomorphic with the direct sum of $[K : k]$ copies of $M$ and $N_r \cong K \otimes_k M$ is isomorphic to $\oplus_{\sigma \in G} {}^{\sigma}M$. Therefore (I) is equivalent to (i). Furthermore, one can show that (II) is equivalent with (ii).

(3) One says that $M$ *descends to* $k$ if there exists a differential module $N$

6

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 $m_1, .., m_n$ 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)     $b(\sigma\tau) = b(\sigma)\ \sigma(b(\tau))$

in other words $\sigma \mapsto b(\sigma)$ is a 1-cocycle for $G$ and $\mathrm{GL}_n(K)$. Here $\sigma \in G$ acts on a matrix by acting on its entries. 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. Now $N := k\tilde{m}_1 \oplus \cdots \oplus k\tilde{m}_n = \{m \in M \,|\, \forall_\sigma\ \Phi(\sigma)(m) = m\}$ is a differential module over $k$ because the $\Phi(\sigma)$ commute with $\partial$. The natural map $K \otimes_k N \to M$ is an isomorphism of differential modules, so $M$ 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 $\{\phi(\sigma) : {}^\sigma M \to M\}$ is given. The *descent problem* is to decide whether $M$ descends to $k$ or, more generally, to find the differential fields $\ell$ (say with $K \supset \ell \supset k$) such that $M$ descends to $\ell$. 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.

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

*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 $E := \mathrm{End}_{k[\partial]}(N) = \mathrm{Hom}_{k[\partial]}(N, N)$. 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), $\mathrm{End}_{K[\partial]}(M) = C_K$ and $\mathrm{Aut}_{K[\partial]}(M) = C_K^*$. $\square$

**Remark:** If $K \neq C_K \cdot k$ then the the lemma does not hold in general. Let $M = K \otimes_k N_1$ and assume $\mathrm{Aut}_{K[\partial]}(M) = C_K^*$. Then $M$ descends to a differential module $N_2$ over $k$ if and only if there exists a one-dimensional differential module $L$ over $k$ for which $K \otimes_k L$ is trivial and $N_2 \cong L \otimes_k N_1$. See also lemma 2.7.1 in [Ka].

**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 property: $^\sigma M$ is isomorphic to $M$ for all $\sigma \in G$.*
*Then $M$ descends to $k$.*

*Proof.* First we treat the case that $M$ is irreducible. 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 $Q \in \bigcup_{m \geq 1} \overline{C_K}[x^{-1/m}]$ the one dimensional differential module $K(Q)e$ over the finite field extension $K(Q)$ of $K$, given by $\partial e = Qe$ (recall that $\partial$ 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 $\tau$ 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 ${}^\sigma M$ is isomorphic to $M$ for all $\sigma$. 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 $\sigma$ to an automorphism $\tilde{\sigma}$ of $\overline{K}/k$. Then ${}^\sigma M$ 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 $\sigma$ 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 $M$. This completes the proof in case $M$ is irreducible.

We now sketch the proof that the assumption that $M$ is irreducible can be omitted. 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 $\partial$ 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. $\square$

**Remarks 2.5**
(1) The following example illustrates that theorem 2.4 does not hold for

positive characteristic. Let $\mathbb{F}_2$ resp. $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ denote the fields with 2 resp. 4 elements. Let $\sigma$ be the non-trivial automorphism $\sigma(\alpha) = \alpha^2 = \alpha + 1$. Let $k = \mathbb{F}_2((x))$ and $K = \mathbb{F}_4((x))$ with differentiation $x' = 1$. Let $M = Ke$ with $\partial e = \frac{\alpha}{x}e$. Then $e \mapsto x\,e$ defines an isomorphism $^\sigma M \cong M$, but $M$ does not descend to $k$. In the rest of this paper we will only consider characteristic 0.

(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 $K$ 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 formal Laurent series fields. For convergent Laurent series field, the situation is quite different, see [P]. 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 $\sigma$ 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 that 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 sub-module $N'$ 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 $\partial$. 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 $G$. As in 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 a $k$-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). $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

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 $D_i \not\equiv D_j$ 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 $\mathrm{Matr}(n_i, F_i)$.

Here $\mathrm{Matr}(n, F)$ denotes the ring of $n$ by $n$ matrices with entries in $F$. 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 $F$.

In the remainder of this section we recall some standard 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 $\mathbf{Q}$.

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 $[A]$ of the central simple algebras over $C$. Two such algebras $A_i = \mathrm{Matr}(d_i, F_i)$ are called equivalent, $[A_1] = [A_2]$, if the (skew) fields $F_1, F_2$ are isomorphic. The group structure on $\mathrm{Br}(C)$ is induced by the tensor product.

If $C_K/C_k$ is a finite Galois extension with group $G$ then one defines the following subgroup of $\mathrm{Br}(C_k)$

$$\mathrm{Br}(C_K/C_k) = \{[A] \in \mathrm{Br}(C_k) \mid A \text{ is split by } C_K\}.$$

Let $c$ be a 2-cocycle with values in $C_K^*$, i.e. $c(\sigma, \tau) \in C_K^*$ for all $\sigma, \tau \in G$ and $c$ satisfies the 2-cocycle relation. Now $c$ is called normalized if $c(1, \sigma) = c(\sigma, 1) = 1$ for all $\sigma$. The image of $c$ in $H^2(G, C_K^*)$ is trivial, i.e. $\bar{c} = 1$, if and only if there exists a map $f : G \to C_K^*$ such that $c(\sigma, \tau)f(\sigma\tau) = f(\sigma)\sigma(f(\tau))$ for all $\sigma, \tau$. Now take the $C_K$-vector space $A$ with basis $\{b_\sigma \mid \sigma \in G\}$ where $b_1 = 1$. One turns $A$ into an algebra (a so-called *crossed-product algebra*) with multiplication rules: $b_\sigma \cdot b_\tau = c(\sigma, \tau)b_{\sigma\tau}$, and $b_\sigma \cdot \lambda = \sigma(\lambda)b_\sigma$ for $\lambda \in C_K$. The 2-cocycle relation guarantees that $A$ is associative, in fact, $A$ is a central simple algebra over $C_k$. Now $\bar{c} \mapsto [A]$ defines an isomorphism

$$H^2(G, C_K^*) \cong \mathrm{Br}(C_K/C_k).$$

Taking the limit over all finite Galois extensions one finds

$$H^2(\mathrm{Gal}(\overline{C_k}/C_k), \overline{C_k}^*) \cong \mathrm{Br}(C_k).$$

The *inflation homomorphism* $H^2(G, C_K^*) \to H^2(\mathrm{Gal}(\overline{C_k}/C_k), \overline{C_k}^*)$ is injective, and corresponds to the embedding of $\mathrm{Br}(C_K/C_k)$ in $\mathrm{Br}(C_k)$.

## 2.3 The associated two-cocycle and skew fields

**Theorem 2.8** The associated 2-cocycle 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) $\overline{c} \in H^2(G, C_K^*) \cong \mathrm{Br}(C_K/C_k) \subset \mathrm{Br}(C_k)$ 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 $\phi(\sigma) : {}^\sigma M \to M$ 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 $\sigma$-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 $\partial$. 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 definitions 2.2 part (3).
(b) Consider the case where $M$ has dimension 1. Write $M = Ke$ and write $\partial e = ae$. For any $\sigma$ 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

14

$C_K[x]$. In other words, the first coefficient in the series expansion of $b(\sigma)$ at $x = \infty$ is 1. 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). The statement in (c) is a standard fact on Brauer groups, see the previous section.

(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 the observation in 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 $A \subset E$ 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 $c_\sigma$ are 0. $A$ is a crossed-product algebra with multiplication rules (a factor set) given by the $c(\sigma, \tau)$. So $A$ is a simple algebra that represents the image of $\overline{c}$ in $\mathrm{Br}(C_k)$. By comparing dimensions one finds $A = E$. 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 all 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 $\ell$ 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. $\qquad\square$

**Corollary 2.9** *We keep the notations and assumptions of theorem 2.8.*
*(1) Suppose that $M$ is irreducible as a $K$-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 $\sigma$ 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 $\sigma$-linear map which commutes with $\partial$. $\square$

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. Parts (a) and (b) of the following proposition can be proved along the lines of the proof of theorem 2.8. Part (c) follows from 2.11 (a) below, and part (d) follows from 2.11 (c).

**Theorem 2.10** The associated 2-cocycle in the general case.
*Let $K/k$ be a 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 $\bar{c} \in H^2(G, C_K^*)$ of an order $d$, dividing $[K : k]$ if $K$ is finite over $k$. Moreover $M$ descends to $k$ if and only if $\bar{c} = 1$.*
(b) *The tensor product $M \otimes \cdots \otimes M$ of $d$ copies of $M$ has associated 2-cocycle $\bar{c}^d$ and therefore this tensor product descends to $k$. The same holds*

16

for $\text{sym}^d M$, the symmetric tensor product of $d$ copies of $M$.

(c) *The image of $\bar{c}$ 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 $\ell$ 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 $\sigma \in \text{Gal}(K/\ell)$ and $L \otimes M$ descends to $\ell$.*

(d) *If $K = \bar{k}$, and $F, \ell$ as in part (c), then $\ell$ is a splitting field if and only if $M$ descends to $\ell$.*

The condition ${}^\sigma L \cong L$ in (c) is irrelevant when $M$ is not cyclic-imprimitive (for a definition see section 4, see also theorem 4.4).

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 $I$. Then $E := \text{End}_{k[\partial]}(M)$ 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 $\ell$ with $k \subset \ell \subset K$ if and only if the field of constants $C_\ell$ 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 $C_k$.*

(c) *If $K = \bar{k}$ then $I = I_0$.*

*Proof.* (a) For any differential field $L$ one writes $\mathcal{Q}(L)$ for the isomorphism classes of the 1-dimensional differential modules over $L$. The tensor product makes $\mathcal{Q}(L)$ into a commutative group and there is an exact sequence

$$0 \to L^*/C_L^* \to L \to \mathcal{Q}(L) \to 0,$$

where $C_L$ denotes the field of constants of $L$; the first non trivial arrow is defined by $f \mapsto \frac{f'}{f}$ and the second non trivial arrow maps $f \in L$ to the isomorphism class of the differential module $(Le, \partial)$ with $\partial e = fe$. We consider this exact sequence with $L = K$ and the exact sequence $0 \to C_K^* \to K^* \to K^*/C_K^* \to 0$. These sequences of $G$-modules induce the usual long

exact sequences. Using that $H^1(G, K) = 0$ and $H^1(G, K^*) = 0$ one obtains exact sequences

$$0 \to H^1(G, C_K^*) \to \mathcal{Q}(k) \to \mathcal{Q}(K)^G \to H^1(G, K^*/C_K^*) \to 0,$$

$$0 \to H^1(G, K^*/C_K^*) \to H^2(G, C_K^*) \to H^2(G, K^*).$$

Clearly $I = \mathcal{Q}(K)^G$ and $I_0$ is the image of $\mathcal{Q}(k) \to \mathcal{Q}(K)^G$.

(c) If $K = \bar{k}$, then the group $K^*/C_K^*$ is a vector space over $\mathbf{Q}$ and hence $H^1(G, K^*/C_K^*) = 0$.

(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 $\ell$. Then $K = C_K \cdot \ell$. So $K/\ell$ and $C_K/C_\ell$ have the same Galois group $H$. Now $M$ descends to $\ell$ if and only if the restriction of the 2-cocycle $\bar{c}$ to $H$ is trivial, if and only if $C_\ell$ 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. $\square$

**Remarks**: Assume $K = C_K \cdot k$. Then theorem 2.8 is valid for a differential field $k$ precisely when $I = I_0$. The proof of 2.8 part (b) shows $I = I_0$ for $k = C_k(x)$. A similar argument shows that if $k$ is the function field of a nonsingular algebraic curve with a point defined over $C_k$ then $I = I_0$.

In subsection 2.5 we will show that proposition 2.11 is related to Amitsur's construction.

## 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 $\text{Matr}(m, F^o)$, we will produce an irreducible differential module $M$ over $K = C_K(x)$ which satisfies (i) and (ii) of 2.8 and such that $\text{End}_{k[\partial]}(M) = \text{Matr}(m, F^o)$. The basic feature of the construction is the introduction of differential modules over skew differential fields. By 2.9, $M$ corresponds to a $k[\partial]$-module $N$ with $\text{End}_{k[\partial]}(N) = F^0$. So $N$ is a $k[\partial]$-module as well as an $F^0$-module. Then $N$ is an $F[\partial]$-module where $F$ is defined in 2.13 below. Hence, every example for 2.8/2.9 comes from a differential module over a skew field.

**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 $e_1, \ldots, e_n$ be a basis of $M$ over $F$. Then $\partial$ is determined by the elements $\partial e_1, \ldots, \partial e_n$. 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 a $k$-differential module and $\text{End}_{k[\partial]}(N) = F^o$.*

*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 $\alpha$. 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 $O_L$ with $C[[t]]$. The embedding $C_k[x] \to O_L$ has dense image. 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 valuation associated to the irreducible polynomial $P$.

Let $V = \operatorname{End}_F(N)$ and $W = \operatorname{End}_{C(x)}(N)$. 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 $k$. Consider a property (*) of elements $B \in W$ which is preserved for all $\tilde{B}$ such that $\tilde{B}$ is close to $B$ w.r.t. a metric on $W$ induced by the embedding $W \subset \operatorname{End}_L(L \otimes_{C(x)} N)$. Then, since $k$ is dense in $C(x)$, there exists an element in $V$ with property (*).

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 $\partial$ of $N$ as a differential module over $F$ has the form $\partial n = n' + A(n)$ with $A \in V$. A structure $\partial$ on $N$ as a differential module over $C(x) = C(t)$ has the form $\partial n = n' + B(n)$ with $B \in W$. Property (*) is defined by: the Newton polygon of a cyclic element of the module $C((t)) \otimes_{C(t)} N$ has slope $\frac{1}{r}$, where $r$ is the dimension of $N$ as $C(x)$-vector space. This property implies that $\widehat{N} := \overline{C}((t)) \otimes_{C(t)} N$ is irreducible and $\operatorname{End}_{\overline{C}((t))[\partial]}(\widehat{N}) = \overline{C}$. Thus $N$ is an irreducible differential module over $C(x)$ and $\operatorname{End}_{C(x)}(N) = C$. Clearly (*) is preserved under a small perturbation w.r.t. a metric on $W$ induced by the embedding $W \subset \operatorname{End}_L(L \otimes_{C(x)} N)$. We conclude 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 $\operatorname{End}_{\overline{C}(x)[\partial]}(\overline{C}(x) \otimes_{C(x)} N) = \overline{C}$.*

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

We now give *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) $\operatorname{End}_{K[\partial]}(M) = C_K$.
(b) $^\sigma M \cong M$ *for all* $\sigma \in \operatorname{Gal}(K/k)$.
(c) $\operatorname{End}_{k[\partial]}(M) = F^o$ *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) $\operatorname{End}_{\overline{C}_K(x)[\partial]}(\underline{M}) = \overline{C}_K$.

*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 $\partial$ of differential module over $F$ on $M$ is given by $\partial m = m' + mD$, with $D \in \operatorname{Matr}(a, F)$.

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 $\operatorname{Matr}(a, F^o)$ over $C_k$,
(3) $M$ is irreducible as a differential module over $F$.
For $a = 1$, property (3) is obvious. Moreover in that case we may replace (1)+(2) by: $D_0, \ldots, D_N$ 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) $\operatorname{End}_{k[\partial]}(M) = F^o$.
For any algebra $B$ we write $B^{opp}$ for the opposite algebra. For any algebra $B$ we write $\operatorname{Matr}(a, B)$ for the algebra of the $a \times a$-matrices with coordinates in $B$. Now $F$ and $\operatorname{Matr}(a, F)^{opp}$ are central simple algebras over $k$. By [Ren], Corollaire 4, p 107, the algebra $F \otimes_k \operatorname{Matr}(a, F)^{opp}$ 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 $b_1, \ldots, b_{d^2}$ 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 $A_i' + A_i D - D A_i$. Hence $L$ commutes with $\partial$ if and only if $A_i' + A_i D - D A_i = 0$ 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 $\mathbf{1}, A, A^2, A^3, \ldots$ all belong to $V$. In particular, there is a non-trivial relation $\lambda_0 \mathbf{1} + \lambda_1 A + \cdots + \lambda_s A^s = 0$ 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 only the trivial idempotents 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 $\sigma$-linear bijection, commuting with $\partial$. This proves (b). Statements (d) and (e) follow from 2.7 and 2.3. $\qquad\square$

**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 $\partial$ 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 $\sigma$ 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 $\sigma$-linear bijection commuting with $\partial$. 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 an 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 an 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 $\sigma$-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 $\partial$. 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: $b_1^2 = A_1$, $b_2^2 = A_2$, $b_2 b_1 = -b_1 b_2$, replacing $\mathbf{H}$ by $F^o = \mathbf{Q} + \mathbf{Q}b_1 + \mathbf{Q}b_2 + \mathbf{Q}b_1 b_2$, and $d$ by $b_1 + b_2 x$ then we find the following $L_2$

$$L_2 = \partial^2 - x^{-1}\partial + \sqrt{A_1}x^{-1} - A_1 - A_2 x^2.$$

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

$$A_1 X^2 + A_2 Y^2 - 1 = 0$$

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

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

24

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

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

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 $\bar{c}$ 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 $\phi(\sigma)$ by a suitable element of $C_K$. This means solving a norm equation, which is equivalent to 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 a differential module over $\mathbf{Q}(x)$, is then also computationally hard, so 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 equally hard as finding a point on the conic.

25

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

$$\partial v = v' + v \begin{pmatrix} 0 & 1 \\ b_1 + b_2 x & 0 \end{pmatrix}.$$

$\mathrm{End}_{\mathbf{Q}(x)[\partial]}(M) = F^o$, see 2.14. $M$ 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 $\alpha$ be a solution of $\alpha^3 - 3\alpha - 1 = 0$. Then $\mathbf{Q}(\alpha)$ is Galois over $\mathbf{Q}$ with Galois group generated by $\sigma$, where $\sigma$ maps $\alpha$ 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 $\alpha$ 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 an 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 $C_k$ 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 $C_k$. Now $k \otimes_{C_k} E$ is the $k$-algebra of all $k$-linear maps $M \to M$. It follows that $E$ is a skew field with center $C_k$ and that $k$ is a splitting field for $E$.
If $C_K \supset C_k$ is a finite extension and a splitting field for $E$, and $K = C_K \cdot k$,

26

then the differential module $K \otimes_k M$ is a direct sum of copies of a 1-dimensional differential module over $K$. Indeed, $\mathrm{End}_{K[\partial]}(K \otimes_k M)$ is isomorphic to the matrix algebra $\mathrm{Matr}(n, C_K)$.

One of the main results, Theorem 16 of [A] is:
*Any skew field $E$ of dimension $n^2$ over its center $C_k$ that has $k$ as splitting field is obtained in this way.*

We sketch the proof of this result. Put $M = k^n$. By definition there is a homomorphism $a \in E \mapsto P_a \in \mathrm{End}_k(M)$. One defines $\partial_0 : M \to M$ by $\partial_0(f_1, \cdots, f_n) = (f_1', \cdots, f_n')$. 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 two representations $E \to \mathrm{End}_k(M \oplus M)$, 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 $a \in E$. Define now $\partial : M \to M$ by $\partial = \partial_0 - Q$. This makes $M = (M, \partial)$ into a differential module over $k$ and there is a homomorphism $E \to \mathrm{End}_{k[\partial]}(M)$. Hence $\mathrm{Hom}(M, M)$ is a trivial differential module and $\mathrm{End}_{k[\partial]}(M) = E$. This is Amitsur's construction.

The differential field $k = C_k(x)$ does not produce an example for Amitsur's theorem, since it is not a splitting field for any non-trivial skew field of finite dimension over its center $C_k$. Consider the differential field $k = \mathbf{Q}(s, t)$ with $s^2 + t^2 = -1$ and $s' = 1$, $t' = -st^{-1}$. Then $k$ is a splitting field for Hamilton's quaternions $\mathbf{H} = \mathbf{Q} + \mathbf{Q}i + \mathbf{Q}j + \mathbf{Q}k$ over $C_k = \mathbf{Q}$. One defines $a \in \mathbf{H} \mapsto P_a \in \mathrm{End}_k(M)$ with $M = k^2$ by $P_i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $P_j = \begin{pmatrix} s & t \\ t & -s \end{pmatrix}$. One calculates that $Q = \begin{pmatrix} 0 & 1/2t \\ -1/2t & 0 \end{pmatrix}$ and that the minimal monic operator that annihilates the cyclic vector $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \in M$ is $L = (s^2 + 1)\partial^2 + s\partial - \frac{1}{4}$.
Let $m$ be a positive squarefree integer and $K = k(\sqrt{-m})$. From the above it follows that $L$ is irreducible as an element of $k[\partial]$, and that $L$ factors in $K[\partial]$ if and only if $m$ is the sum of $\leq 3$ squares in $\mathbf{Q}$.

Note that Amitsur's theorem follows from proposition 2.11 (a). Consider a differential field $k$ with field of constants $C_k$ and a skew field $E$ of dimension $n^2$ over its center $C_k$, such that $k$ is a splitting field for $E$.

Let $C_K$ be a splitting field for $E$, and a finite Galois extension of $C_k$. Let $G$ be the Galois group of $C_K/C_k$. Then $[E] \in \mathrm{Br}(C_K/C_k) \cong H^2(G, C_K^*)$. Now $G$ is also the Galois group of $K/k$, where $K = C_K \cdot k$, so $H^2(G, K^*) \cong \mathrm{Br}(K/k)$. Since $k$ is a splitting field, $[E \otimes k]$ is trivial, hence $[E]$ is in the kernel of $H^2(G, C_K^*) \to H^2(G, K^*)$. According to proposition 2.11 (a), $[E]$ is the image of some $N \in I = \mathcal{Q}(K)^G$. This $N$ is a 1-dimensional differential module over $K$ such that $^\sigma N \cong N$ for all $\sigma \in G$. Let $M$ be $N$ considered as a differential module over $k$. Explicit construction of the map $\mathcal{Q}(K)^G \to H^2(G, C_K^*)$ shows that $[\mathrm{End}_{k[\partial]}(M)] = [E]$. Then $M$ has a submodule $M'$ of dimension $n$ over $k$ (if $C_K$ is a maximal commutative subfield of $E$ then $M = M'$), and $\mathrm{End}_{k[\partial]}(M') = E$. Since $N$ is unique up to $I_0$, see proposition 2.11 (a), the isomorphism class of $M'$ is unique up to tensoring with 1-dimensional modules over $k$. Thus it must correspond to Amitsur's construction up to this equivalence.

# 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]) showed that the question has a positive answer if and only if one can produce a certain conic and a $K$-rational point on this conic. This raises a second question: Which conics can occur? 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 $\partial$ 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

**Proposition 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 $\phi$ is a 1-dimensional submodule of $sym_K^2 B$.
(2)$\Rightarrow$(1). The assumptions on the quadric $\sum_{1 \leq i \leq j \leq 3} c_{i,j} X_i X_j = 0$ imply that there exists a linear change of the variables $X_1, X_2, X_3$ which transforms the quadratic form into a multiple of $X_1 X_2 - X_3^2$. 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 $\partial$ 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 $\phi$ is an isomorphism of differential modules. $\square$

**Some observations:** Let $C$ be an algebraically closed field of characteristic 0. Let $K = C(x)$ be the differential field with differentiation $f \mapsto \frac{df}{dx}$. For this field $K$, one can omit in part (2) of proposition 3.1 the assumption that the quadric has a $K$-rational point. Indeed, $K$ is a $C_1$-field. The Tannakian equivalence between differential modules over $K$ and finite dimensional $C$-linear representations of the universal differential Galois group of $K$ leads to the following translation of 3.1 in terms of representations of linear algebraic groups over $C$:

29

*Let $G$ be a linear algebraic subgroup of* $\mathrm{GL}(W)$, *where $W$ is a vector space of dimension 3 over $C$. Suppose that $sym^2W$ contains a $G$-invariant line that defines a non-degenerate quadric. Then there exists a linear algebraic group $H \subset \mathrm{GL}(V)$, where $V$ has dimension 2 over $C$, such that $H/(H \cap \{\pm 1\}) \cong G$ and the two $G$-modules $sym^2V$ and $W$ are isomorphic.*

A similar result seems to be valid for Galois representations.

**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 $B$. $\square$

**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 $\sigma$ 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

30

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 $\{g \in \mathrm{GL}_2 \mid \{gL_1, gL_2\} = \{L_1, L_2\}\}$.

**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 $A_4^{\mathrm{SL}_2}$ (see remarks 4.6 part (3) for a list of groups), then the symmetric power $sym_K^4 \underline{A}$ 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 $sym_K^2 B$ 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 $sym_K^2(\underline{L}_1 \otimes \underline{A})$ is isomorphic to $\underline{B}$ and that the kernel of $sym_{\underline{K}}^2 \underline{B} \to sym_{\underline{K}}^4(\underline{L}_1 \otimes \underline{A})$ is $sym_K^4 \underline{L}_1 = M_1$. 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 $L_2 := sym_K^2 L_1$. In the same way, $L_2$ is the kernel of the morphism $sym_K^2 B \cong sym_K^2(L_2 \otimes B) \to sym^4(L_2 \otimes A)$. An application of proposition 3.1 ends the proof. $\square$

## 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 $F$. Differentiations on $F$ are not unique, but we can choose one as follows.

**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 $b_3' \in F_3$.   $\square$

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 $\sigma$ denote the non-trivial element of the Galois group of $F_1/k$. One considers the $\sigma$-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 $N := sym_{F_1}^2 M$ descends to $k$. We will make this explicit by a calculation.

On the differential module $N =: sym_{F_1}^2 M$ 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 $\sigma$-linear, commutes with $\partial$, 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 $\partial$ 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 a 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 proposition 3.1, $sym_{F_1}^2 N$ 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 $sym_k^2 N^0$ contains a one dimensional submodule $L$ and the quadratic form associated to $L$ 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 $F$.

**Theorem 3.6** *Let $F, F_1, k, M, N^0$ be as above and let $K$ be an algebraic extension of $k$.*

*(1) If $K$ is a splitting field for $F$ then $K \otimes_k N^0$ is the second symmetric power of some differential module over $K$.*

*(2) Assume that $K \otimes_k N^0$ is the second symmetric power of some differential module over $K$ and that $KF_1 \otimes_k N^0$ is irreducible. Then $K$ is a splitting field for $F$.*

*Proof.* (1) Apply proposition 3.1 to the 1-dimensional submodule $K \otimes_k L$ of $sym^2(K \otimes_k N^0)$. By assumption the quadratic form associated to $L$ has a non-zero $K$-rational point.

(2) By proposition 3.1, $sym^2(K \otimes_k N^0)$ contains a 1-dimensional submodule $Z$ such that the associated quadratic form is non degenerate and has a non-zero $K$-rational point. In general, this does not imply that $K$ is a splitting field for $F$ since $Z$ need not be $K \otimes_k L$.

The assumption that $KF_1 \otimes_k N^0$ is irreducible is equivalent, by lemma 3.3, to $\tilde{M} := KF_1 \otimes_{F_1} M$ is irreducible and primitive. One applies lemma 3.4 to $\tilde{N} := sym^2 \tilde{M}$. Thus $sym^2 \tilde{N}$ satisfies (1) or (2) of lemma 3.4. Then the same holds for $sym^2(K \otimes_k N^0)$. In particular the quadratic form associated to $L$ has a non-zero $K$-rational point and thus $K$ is a splitting field for $F$. $\qquad \square$

### 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 $F_1 = \mathbf{Q}(\sqrt{x})$ 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 $d = b_1 + x b_2$. We want to apply 3.6 with $K = C_K(x)$ where $C_K$ is any algebraic extension of $\mathbf{Q}$. Thus we have to show that $\tilde{N} := \overline{\mathbf{Q}}(\sqrt{x}) \otimes_{\mathbf{Q}(x)} N^0$ is irreducible, since the composite of the fields $\overline{\mathbf{Q}}(x)$ and $F_1$ is $\overline{\mathbf{Q}}(\sqrt{x})$. Suppose that $M$ contains a one-dimensional $F_1$-vector space $V$, invariant under $\partial$. Then $b_2 V$ is also a 1-dimensional $F_1$-vector space, invariant under $\partial$ (indeed, $b_1 b_2 = -b_2 b_1$ and $b_2' = \frac{A_2'}{2A_2} b_2$) and $M = V \oplus b_2 V$. Thus $M$ is always semi-simple over $F_1$. Then also $\tilde{N}$ is semi-simple. Suppose that $\tilde{N}$ is reducible. Then $\tilde{N}$ has a direct sum decomposition. The Galois group of the extension $\overline{\mathbf{Q}}(\sqrt{x}) \supset \overline{\mathbf{Q}}(x)$ acts on these direct sum decompositions. From this one concludes that $\overline{\mathbf{Q}}(x) \otimes N^0$ is also reducible and moreover that $\overline{\mathbf{Q}}(x) \otimes N^0$ contains a submodule of dimension 2. Let $L_3$ denote the minimal monic operator $L_3$ for the cyclic vector $b_2 e \otimes e$ of $N^0$. We will prove that $\tilde{N}$ is irreducible by showing that $L_3$ has no right hand factor of order 1 in $\overline{\mathbf{Q}}(x)[\partial]$. One calculates that $L_3$ is equal to

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

Suppose that $\partial - u$ with $u \in \overline{\mathbf{Q}}(x)$ is a right hand factor of $L_3$. We make now 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 $\infty$ 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 $\infty$. This exponent is

34

$3/2$ and gives a local right hand factor of the form $\partial + 3/2x^{-1} + \cdots$. 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 $\infty$.

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 $A_1 X^2 + A_2 Y^2 - Z^2 = 0$ has a non-trivial solution in $K^3$. The latter is equivalent to $\sqrt{s_0}, \sqrt{s_1} \in C_K$.

**Observation.** One can compute a monic operator $L_2 \in \mathbf{Q}(\sqrt{s_0}, \sqrt{s_1})(x)[\partial]$ with $Sym^2 L_2$ equivalent to $L_3$ above. Suppose that $\mathbf{Q}(\sqrt{s_0}, \sqrt{s_1})$ has degree 4 over $\mathbf{Q}$. Let $\sigma$ 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 by computer computation the following:

Let $\sigma_i$ interchange $\sqrt{s_i}$ and $-\sqrt{s_i}$, and leave $\sqrt{s_j}$ invariant where $j \neq i$. Let $t_0 = \sqrt{A_1 A_2}$ and let $t_1 = \sqrt{A_2}$. Then $\sigma_0(L_2)$ 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 $A_2$

Consider elements $A_1, A_2 \in \mathbf{Q}(x)$ with $A_1' \neq 0 \neq A_2$. Even if $F$ is not a skew field, one can define $\partial$ on $M = Fe$ by $\partial e = de$ where $d = b_1 + xb_2$. Again $M$ is a differential module over $F_1$ and $sym_{F_1}^2 M = F_1 \otimes_{\mathbf{Q}(x)} N^0$. Moreover $b_2 e \otimes e$ is a cyclic vector for $N^0$. Let $L_3$ denote the monic operator of order 3 with $L_3(b_2 e \otimes e) = 0$. In the following we will make the equivalence between $L_3$ and the second symmetric power of some operator $L_2$ over some field $K \supset \mathbf{Q}(x)$ explicit. For this purpose we introduce an operator $R$ of order $< 3$, with coefficients in $K \supset \mathbf{Q}(x)$. One describes $R$ by: the least common left multiple $LCLM(R, L_3)$ of $R$ and $L_3$ has the form $Sym^2 L \cdot R = B \cdot L_3$ for some $L_2 \in K[\partial]$ of order 2. In other words, $R$ provides the isomorphism $K[\partial]/K[\partial]Sym^2 L_2 \to K[\partial]/K[\partial]L_3$ of differential modules.

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

where $(u, v, w)$ is a non-zero point on the conic

$$A_1 u^2 + A_2 v^2 - w^2 = 0 \tag{1}$$

Assuming that $K \otimes_{\mathbf{Q}(x)} sym^2 N^0$ 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 non-zero 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 $n$th 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., $K \otimes_{\mathbf{Q}(x)} sym^2 N^o$ has only one submodule of dimension 1). Suppose that the differential Galois group $G$ of $\underline{M} := \overline{\mathbf{Q}}F_1 \otimes_{F_1} M$ satisfies $G \supset \mathrm{SL}_2$. Then the differential Galois group of $\overline{F_1} \otimes_{F_1} M$ is $G^o$ and contains $\mathrm{SL}_2$. Then for any algebraic extension $K$ of $\mathbf{Q}(x)$, the second symmetric power of $K \otimes_{\mathbf{Q}(x)} N^0$ has a unique submodule of dimension 1.

If at a point $p$ formal solutions involve logarithms, then the differential Galois group of $\underline{M}$ contains $\mathrm{SL}_2$. 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 with this feature are obtained by a different choice for $\partial e$, namely $\partial e = (\frac{A_1'}{A_1 - 1} b_0 + \frac{A_1'}{A_1(A_1 - 1)} b_1 + \frac{A_1'}{A_2} b_2) e$. Suppose that the point $p$ satisfies $A_1(p) = 1$ and $A_2(p) \neq 0$, then one can verify that local solutions at $p$ contain logarithms (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 $x \mapsto A_1$). Thus logarithms will appear in local solutions if $A_2$ is not a multiple of $A_1 - 1$.

The operator obtained this way is:

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

$$
\text{where } B_1 = A_1(A_1 - 1) \text{ and } B_2 = A_2'/A_2.
$$

This operator has the same conic (1). After, if necessary, replacing $A_1$ with $c^2 A_1$ for some non-zero $c \in \mathbf{Q}$, we obtain that $A_2$ is not a multiple of $A_1 - 1$ (if $A_1 \in \mathbf{Q}$ then take $c \in \mathbf{Q}(x)$ instead of in $\mathbf{Q}$). 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 non-zero solution in $K^3$. Furthermore, such examples exist for every non degenerate 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 **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 $L \otimes M_1$. Suppose that $C_k$ is algebraically closed, then $M_1, M_2$ correspond to representations of the universal differential Galois group $\mathcal{U}$ on finite dimensional $C_k$-vector spaces. These representations are projectively equivalent if and only $M_1$ and $M_2$ are projectively equivalent.
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 problem**. Let $M$ be an irreducible differential module over $K$ of dimension $n$. Suppose that $^\sigma M$ is projectively equivalent to $M$ for every

$\sigma \in \text{Gal}(K/k)$. 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 $\ell$. 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 $n^{\text{th}}$-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 $k \subset k(t)$ with equation $t^d = f \in k$ of degree $d \neq 1$ dividing $n$, such that $[\underline{k}(t) : \underline{k}] = d$ and $k(t) \otimes M$ is a direct sum of $d$ irreducible differential submodules over $k(t)$.*

*Proof.* (1)$\Rightarrow$(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 $\partial$ 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 $t^d = f$. It is easily seen that $[\underline{k}(t) : \underline{k}] = d$. Define $\psi := t\phi : k(t) \otimes M \to k(t) \otimes M$. Then $\psi \partial = \partial \psi$ and $\psi^d = 1$. Let $N_0, \ldots, N_{d-1} \subset N =: k(t) \otimes M$ denote the eigenspaces of $\psi$ corresponding to the eigenvalues $\zeta_d^i$, $i = 0, \ldots, d-1$, where $\zeta_d$ denotes a primitive $d^{\text{th}}$-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 $\sigma \in \text{Gal}(k(t)/k)$ be the generator of this Galois group, given by $\sigma(t) = \zeta_d^{-1} t$. Then $\sigma$ 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 $\sigma$. Then the set of the $\sigma$-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 $\sigma$ 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 $\sigma$. The set of the $\sigma$-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

38

$\phi\partial\phi^{-1} = \partial + \frac{f'}{df}$ and $\sigma\phi = \phi\sigma$. The last equality implies that $\phi(M) = M$ and that the restriction $\phi'$ of $\phi$ 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 $\partial e = \frac{f'}{df}e$. The assumption $[\underline{k}(t) : \underline{k}] = d$ implies that $d$ is minimal such that $L^{\otimes d} \cong \mathbf{1}$. $\qquad\qquad\qquad\qquad\square$

**Remarks**. A differential module $M$ of dimension $n > 1$ will be called *cyclic-imprimitive* if $M$ satisfies 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. An example of a cyclic-imprimitive operator is given in case 3 in the table in section 1 (if $k = C_k(x)$, $K = C_K(x)$ then case 3 implies part (1) of lemma 4.1).

**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 $\sigma$ 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 $N_2$. $\qquad\square$

**Example 4.3** Corollary 4.2 is no longer valid if $M_1$ is cyclic-imprimitive. We give two examples. Let $M_i = \overline{\mathbf{Q}}(x) \otimes_{\mathbf{Q}(x)} N_i$ for $i = 1, 2$, where $N_1$, $N_2$ denote the differential modules over defined by the differential operators $L_1, L_2$. In the first example one chooses

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

One can verify the following. The differential Galois group of $M_1$ is $D_2^{\mathrm{SL}_2}$. Moreover $sym^2 N_1 \cong sym^2 N_2$ and the modules $N_1$, $N_2$ are not projectively equivalent. They become projectively equivalent after extending the constants with a solution of the equation $t^4 + 2 = 0$ (not $t^4 - 2$ as the denominators would suggest). The proof of these statements can be deduced from part (2d) of the proof of theorem 4.7.

In the second example one fixes $c \in \mathbf{Q}$, not a square, an integer $n > 2$, and considers monic operators $L_1, L_2 \in \mathbf{Q}(x)[\partial]$ of degree 2, defined by the data: three regular singularities $\sqrt{c}, -\sqrt{c}, \infty$, exponent-difference $1/2$ at $\pm\sqrt{c}$ for $L_1, L_2$, $L_1$ resp. $L_2$ have exponent-difference $\frac{1}{n}$ resp. $1 + \frac{1}{n}$ at $x = \infty$. The differential Galois group of $M_1$ is $D_n^{\mathrm{SL}_2}$, $n > 2$. The modules $N_1, N_2$ are not projectively equivalent, but become projectively equivalent after extending the constants with $\sqrt{c}$. The proof of these statements can be deduced from part (2b) of the proof of theorem 4.7.

**Theorem 4.4** *Let $K$ be Galois over $k$ and $G = \mathrm{Gal}(K/k)$. Let $M$ be an irreducible, not cyclic-imprimitive, differential module of dimension $n > 1$ over $K$ such that $\det(M)$ descends to $k$ and $\mathrm{End}_{K[\partial]}(M) = C_K$. Suppose that for any $\sigma \in G$ the twisted differential module ${}^{\sigma}M$ is projectively equivalent to $M$. Then:*
*(1) $M$ induces a 2-cocycle class $\overline{c} \in H^2(G, K^*)$, having an order $d$ with $d|n$. Let $F$ denote the (skew) field with center $k$ associated 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 a module $N$ that descends to $\ell$.*

*Proof.* (1) For $\sigma \in G$ there is an isomorphism $\phi(\sigma) : {}^{\sigma}M \to M \otimes L(\sigma)$ of differential modules. Then one has isomorphisms:

$$ {}^{\sigma\tau}M \overset{{}^{\sigma}\phi(\tau)}{\to} {}^{\sigma}(M \otimes L(\tau)) = {}^{\sigma}M \otimes {}^{\sigma}L(\tau) \overset{\phi(\sigma)\otimes 1}{\to} M \otimes L(\sigma) \otimes {}^{\sigma}L(\tau) $$

and $\phi(\sigma\tau) : {}^{\sigma\tau}M \to M \otimes L(\sigma\tau)$. The assumption on $M$ implies that $L(\sigma\tau) \cong L(\sigma) \otimes {}^{\sigma}L(\tau)$. From $\det(M) = \det({}^{\sigma}M) = \det(M) \otimes L(\sigma)^{\otimes n}$ one concludes that $L(\sigma)^{\otimes n} = \mathbf{1}$. Fix a basis $e(\sigma)$ for each $L(\sigma)$. Let $A(\sigma)$ be the $\sigma$-linear map $M \to M$ for which $m \mapsto A(\sigma)(m) \otimes e(\sigma)$ is the $\sigma$-linear map $M \to M \otimes L(\sigma)$ associated to $\phi(\sigma)$. Then $A(\sigma)\partial = (\partial + a(\sigma))A(\sigma)$ 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

40

$a(\sigma_1\sigma_2) = a(\sigma_1) + \sigma_1(a(\sigma_2)) + \frac{c(\sigma_1,\sigma_2)'}{c(\sigma_1,\sigma_2)}$. The collection $\{c(\sigma_1,\sigma_2)\}$ defines a 2-cocycle with class $\bar{c} \in H^2(G, K^*)$. The 2-cocycle class $\bar{c}^n$ is associated to the differential module $\det(M)$. By assumption, $\det(M)$ descends to $k$ and thus $\bar{c}^n = 1$.

(2) It suffices to consider the case $\ell = k$. Suppose that $\bar{c} = 1$, then one may suppose that $c(\sigma_1, \sigma_2) = 1$ for all $\sigma_1, \sigma_2$. 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 $\partial$ and $A(\sigma_1)A(\sigma_2) = A(\sigma_1\sigma_2)$ holds for all $\sigma_1, \sigma_2$.
On the other hand, if $N$ with property (2) is given, then clearly $\bar{c} = 1$. $\qquad\square$

The condition that $\det(M)$ descends to $k$ is not a serious restriction because every $M$ is projectively equivalent to a module with this property. Note that if $K = \bar{k}$ then $L(\sigma)^{\otimes n} = \mathbf{1}$ implies $L(\sigma) = \mathbf{1}$, so the theorem follows from 2.10 (d) in this case.

**Example 4.5** *A skew field $F$ of dimension 9 over $\mathbf{Q}(x)$.*
Let $\alpha$ be a root of the polynomial $z^3 - 3z - 1$. Then $\mathbf{Q}(\alpha)$ is Galois over $\mathbf{Q}$. Let $\sigma$ be the automorphism that sends $\alpha$ 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:

$$L = L_0 L_1 L_2 - x \quad \text{where} \quad L_i = x\partial - \sigma^i(\alpha) - i/3.$$

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

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

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 $sym_K^n M$ is projectively equivalent to a module that descends to $k$. Indeed, the 2-cocycle associated to this module is $\bar{c}^n = 1$.

(2) If $K = \underline{k}$ and $M$ is of dimension $n = 2$ over $K$ then a converse for (1) can be obtained from 4.7 below, and one finds: If $sym^2 M$ is projectively equivalent to a module that descends to $k$ then $M$ is projectively equivalent to its conjugates over $k$.

(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 pre-images in $\mathrm{SL}_2(C)$ of the subgroups $D_\infty^{pr}$, $D_n$, $A_4$, $S_4$ and $A_5$ of $\mathrm{PSL}_2(C)$. Further $D_\infty^{pr}$ is the projective dihedral group consisting of the elements of $\mathrm{PSL}_2(C)$ which stabilize the subset $\{0, \infty\}$ of $\mathbf{P}^1(C)$. For more details see [Ko]. We will use this classification to prove theorem 4.7.

(4) Theorem 4.7 below does not hold for higher symmetric powers nor for second symmetric powers of modules of dimension $> 2$. We give three examples where $M_1$, $M_2$ are not projectively equivalent, and $sym^i M_1 \cong sym^i M_2$ with $i = 3$ for (a), (b) and $i = 2$ for (c). 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 $E(1) \cong E(0)$.

(a). $M_1 = E(0) \oplus E(\frac{1}{5})$ and $M_2 = E(\frac{1}{15}) \otimes (E(0) \oplus E(\frac{2}{5}))$.

(b). $M_1 = E(0) \oplus E(\frac{1}{10}) \oplus E(\frac{3}{10})$ and $M_2 = E(\frac{1}{5}) \otimes (E(0) \oplus E(\frac{-1}{10}) \oplus E(\frac{-3}{10}))$.

(c). $M_1 = E(0) \oplus E(\frac{1}{7}) \oplus E(\frac{3}{7})$ and $M_2 = E(\frac{1}{14}) \otimes (E(0) \oplus E(\frac{1}{7}) \oplus E(\frac{5}{7}))$.

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

**Remark:** Corollary 4.2 implies that over rational functions this result is also valid for non-algebraically closed field of constants *except* (see examples 4.3) in the imprimitive case (cases (2b) and (2d) in the proof below). The proof below is long because it distinguishes many cases. Bas Edixhoven informed us that a shorter proof can be obtained with the following ideas: replace the groups $G_i$ by the largest group that stabilizes both quadrics, consider

the intersection $R$ of these quadrics as a closed subscheme of length 4, and distinguish cases based on the structure of $R$.

*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 $sym_C^2 W_i \to sym^4 V_i$ 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 $sym^2 B : sym_C^2 W_1 \to sym_C^2 W_2$ maps $K_1$ to $K_2$.

Let $G_i$ denote the image of $\rho_i$. The isomorphism between $W_1$ and $W_2$ implies that the induced morphisms $\mathcal{U} \to G_i/\{\pm 1\} \cap G_i$, $i = 1, 2$ 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 precisely two proper invariant subspaces. We may assume that the representation $V_1$ is the sum of the trivial character (denoted by $\mathbf{1}$) and a non-trivial character $\chi_1$. Because $G_1/\{\pm 1\} \cap G_1 \cong G_2/\{\pm 1\} \cap G_2$

43

one has that $V_2$ is the direct sum of two distinct characters $\chi_2, \chi_3$. The two sequences of characters $1, \chi_1, \chi_1^2$ and $\chi_2^2, \chi_3^2, \chi_2\chi_3$ are equal up to their order. Suppose that $\chi_2^2 \neq \mathbf{1} \neq \chi_3^2$. Then we may suppose that $\chi_2\chi_3 = \mathbf{1}$, $\chi_2^2 = \chi_1$, $\chi_3^2 = \chi_1^2$. Then $\chi_1^3 = \mathbf{1}$, $\chi_2 = \chi_1^2$, $\chi_3 = \chi_1$ and $V_2 = \chi_1 \otimes V_1$.

If say $\chi_3^2 = \mathbf{1}$, then after changing $V_2$ into $\chi_3 \otimes V_2$. Thus we may suppose that $V_2 = \mathbf{1} \oplus \chi_2$. If $\chi_1 = \chi_2$, then $V_1 \cong V_2$. If $\chi_1 \neq \chi_2$, then $\chi_1 = \chi_2^2$, $\chi_1^2 = \chi_2$ and $\chi_1^3 = 1$. Thus $V_1 = \mathbf{1} \oplus \chi_1 = \chi_1 \otimes (\mathbf{1} \oplus \chi_2) = \chi_1 \otimes V_2$.

(1c) Suppose that $V_1$ has more than two invariant subspaces of dimension 1. Then $G_1/\{\pm 1\} = \{1\}$. Also $G_2/\{\pm 1\} = \{1\}$. Hence $V_1$ and $V_2$ differ by a character.

(2) Now we consider the case where $G_1$ is irreducible. After multiplying $\rho_1$ 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

44

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 $\lambda$, 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 $sym^2(B)K_1 = K_2$.

Now we replace $V_2$ by $V_2' := L_2(0)^{\otimes 2} \otimes V_2$. This new representation has the same kernel as $\rho_2$. Put $W_2' = sym^2 V_2' = L_2(0)^{\otimes 4} \otimes W_2$. 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 $L_2(0)^{\otimes 4} \otimes D$ and $D$ are isomorphic, since there is only one irreducible representation of $A_4$ with dimension 3. Thus $sym^2 V_2$ and $sym^2 V_2'$ are isomorphic. Then $sym^2 V_1$ and $sym^2 V_2'$ are isomorphic. Let $B'$ denote the isomorphism. The decomposition of $sym^2 W_2'$ is

$$L_2(0)^{\otimes 9} \oplus (L_2(1) \otimes L_2(0)^{\otimes 8}) \oplus (L_2(2) \otimes L_2(0)^{\otimes 8}) \oplus D,$$

where $L_2(0)^{\otimes 9}$ 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 $(V_i, \rho_i)$ of $\mathcal{U}$ having dimension 2, such that the image $G_1$ of $\rho_1$ is $D_2^{SL_2}$. 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 $K_2$.

In the first example of 4.3, the three lines $L_1, L_2, L_3$ are defined over the field of constants $\mathbf{Q}(\sqrt{2})$. The above proof then shows that $N_1, N_2$ must become projectively equivalent if we extend the constants to $C = \mathbf{Q}(\sqrt{2}, \frac{\lambda_1}{\lambda_3}, \frac{\lambda_2}{\lambda_3})$. In the example, $C$ turns out to be the splitting field of $x^4 + 2$, which has degree 8 over $\mathbf{Q}$. In general, if $N_1, N_2$ are differential modules over $\mathbf{Q}(x)$ that become projectively equivalent over $\overline{\mathbf{Q}}(x)$, and have differential Galois group $D_n^{SL_2}$, then they become projectively equivalent over $C'(x)$ for some field extension $C'$ of $\mathbf{Q}$ of degree $\leq 4$ when $n = 2$, and degree $\leq 2$ when $n > 2$. In the example one can show that the two subfields of $C$ that contain a solution of $x^4 + 2 = 0$ are the smallest fields of constants over which $N_1, N_2$ become projectively equivalent. $\square$

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 $\underline{k} \otimes_{\tilde{k}} sym_{\tilde{k}}^2 \tilde{M}$ 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.

[Ka] N. Katz - *Exponential sums and differential equations* - Annals of Mathematics Studies, 124. Princeton University Press, 1990.

[Ko] J. Kovacic - *An algorithm for solving second order linear homogeneous differential equations* - J. Symbolic Computation, **2**, 3-43, 1986.

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

[P] M. van der Put - *Skew differential fields* - preprint University of Groningen, 2002.

[P-S] M. van der Put and M. Singer - *Differential Galois Theory* - to appear, Grundlehren der Mathematik, Springer Verlag, 2003. 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.