Vol. 54, No. 1 DUKE MATHEMATICAL JOURNAL © 1987

A NOTE ON PSEUDO-CM REPRESENTATIONS AND DIFFERENTIAL GALOIS GROUPS

Dedicated to Y. I. Manin on his fiftieth birthday

NICHOLAS M. KATZ AND RICHARD PINK

Introduction. This note, a sequel to [Ka-1], falls into two parts. In the first, we give a criterion for a connected semisimple algebraic subgroup of $\mathrm{GL}(n)$ to be one of the following subgroups:

$\mathrm{SL}(n)$, if $n \geqslant 2$
$\mathrm{Sp}(n)$ or $\mathrm{SO}(n)$, if n is even and $\geqslant 4$.

The criterion is based on the classification of what we call "pseudo-CM representations", a natural generalization of the notion of "CM representation" introduced in [Ka-1]. The second part applies these results to determine the differential galois groups of some concrete differential equations, including the general Kloosterman equation on $\mathbf{G}_m$.

Part 1. Throughout this section, k is an algebraically closed field of characteristic zero, n is an integer $\geqslant 2$, V is an n-dimensional vector space over k, G is a Zariski closed subgroup of $\mathrm{GL}(V)$, and G^0 is the identity component of G.

THEOREM 1. *Suppose that*

(1) G^0 *lies in* $\mathrm{SL}(V)$.
(2) *As* G^0*-representation,* V *is irreducible.*
(3) *There exists an element* g *in* G, *and a connected torus* T *in* G^0 *such that*
  (a) *As* T*-representation,* V *is the direct sum of* n *distinct characters* $c_1, \ldots, c_n$.
  (b) T *is* $\mathrm{Ad}(g)$*-stable, i.e.,* $gTg^{-1} = T$.
  (c) *The automorphism* $\mathrm{Ad}(g)$ *of* T *cyclically permutes the* n *characters* $c_1, \ldots, c_n$.

Then there exist

an integer $r \geqslant 1$
a factorization of n *as* $n = n_1 \ldots n_r$ *with all* $n_i \geqslant 2$ *and the* n_i *pairwise relatively prime.*
algebraic groups $G_1, \ldots, G_r$, *with each* G_i *equal to one of the groups*
  $\mathrm{SL}(n_i)$ *is odd or* $= 2$
  $\mathrm{SL}(n_i)$ *or* $\mathrm{Sp}(n_i)$ *or* $\mathrm{SO}(n_i)$ *if* n_i *is even* $\geqslant 4$.

Received October 11, 1986. Second author supported by deutscher Akademischer Austauschdienst (DADD) during the academic year 1985–86.

such that (G^0, V) *is isomorphic to* $(\Pi(G_i), \otimes(\mathrm{std}(n_i)))$, *where* $\mathrm{std}(n_i)$ *denotes the standard* n_i*-dimensional representation of* G_i.

THEOREM 2. *Hypotheses as in Theorem* 1, *suppose in addition that*

(4) *The group of components* G/G^0 *is cyclic.*
(5) *As representation of* G, V *is not isomorphic to the tensor product of two strictly lower-dimensional representations of* G.

Then $r = 1$, *i.e.*, G^0 *is either*

$\mathrm{SL}(n)$ *if* $n = 2$ *or* n *odd*
$\mathrm{SL}(n)$ *or* $\mathrm{SO}(n)$ *or* $\mathrm{Sp}(n)$ *if* n *is even and* $\geqslant 4$.

Moreover, in the case $G^0 = \mathrm{SO}(n)$, G *is not contained in* $\mathbf{G}_m \cdot \mathrm{SO}(n)$.

Proof. We first explain how Theorem 2 follows from Theorem 1. Consider the action of G on G^0 by conjugation. This action must respect the individual factors G_i of G^0, simply because between the various groups G_i in question, there are no nontrivial homomorphisms. By the unicity of the decomposition of an irreducible representation of a product group into a tensor product of irreducible representations of the factors, each representation $\mathrm{std}(n_i)$ of G_i, viewed as a representation of G^0, must remain isomorphic to itself under G-conjugation. Because G/G^0 is cyclic, any irreducible representation of G^0 whose isomorphism class is G-invariant extends to an irreducible representation of G. In particular, the representations $\mathrm{std}(n_i)$ of G^0 each extend to representations $\mathbf{std(n_i)}$ of G itself. Consider the representation $\otimes(\mathbf{std(n_i)})$ of G. It coincides on the normal subgroup G^0 with the G^0-irreducible representation V of G, so it is G-irreducible, and as a G-representation it must be the tensor product of V with a character c of G/G^0 (namely the one-dimensional space of G^0-homomorphisms from V to $\otimes(\mathbf{std(n_i)})$). Twisting a single one of the $\mathrm{std}(n_i)$ by the inverse of this character, we find that V is itself a tensor product of strictly lower-dimensional representations of G unless $r = 1$.

If $G^0 = \mathrm{SO}(n)$, then G cannot lie in $\mathbf{G}_m \cdot \mathrm{SO}(n)$, for then the element g in hypothesis (3) of Theorem 1 would induce an inner automorphism of G^0, so could be rechosen to lie in G^0, in which case we would find that the standard representation of $\mathrm{SO}(n)$ is CM, and this is known (cf. [Ka-1], 3.2.7) not to be the case. This completes the deduction of Theorem 2 from Theorem 1.

We now turn to the proof of Theorem 1. Because G^0 is a connected irreducible subgroup of $\mathrm{SL}(n)$, it is automatically semisimple (cf. [Ka-2], 11.5.3.2). We reduce to the case when the torus T is a maximal torus of G^0. Let $\mathbf{T}$ be any maximal torus of G^0 which contains the given torus T. Then we have obvious inclusions

$$\mathbf{T} \subset Z_G(T) \subset Z_{GL(V)}(T).$$

The hypothesis (3a) of Theorem 1 shows that $Z_{\mathrm{GL}(V)}(T)$ is precisely the group of

all diagonal (with respect to a T-eigenbasis of V) matrices in $\mathrm{GL}(V)$. Therefore $(Z_G(T))^0$ is itself a torus, so by maximality of $\mathbf{T}$ it must be equal to $\mathbf{T}$ itself. In particular there is a unique maximal torus $\mathbf{T}$ of G^0 which contains T. By unicity, $\mathbf{T}$ must be $\mathrm{Ad}(g)$-stable if T is. Because T acts on V as the direct sum of n distinct characters c_i, $\mathbf{T}$ respects each c_i-eigenspace. The characters $\mathbf{c}_i$ of $\mathbf{T}$ on these eigenspaces must be n distinct characters of $\mathbf{T}$ which are cyclically permuted by $\mathrm{Ad}(g)$, simply because the $\mathbf{c}_i$ are determined by their restrictions c_i to T, and this holds for the c_i. This completes the reduction to the case when T is maximal.

We now state and prove a classification theorem for pseudo-CM representations of semisimple Lie algebras, which, when applied to $\mathrm{Lie}(G^0)$ and its given embedding into $\mathrm{End}(V)$, leads immediately to Theorem 1 exactly as in Chapter 3 of [Ka-1].

Let $\mathfrak{G}$ be a nonzero semisimple Lie algebra over k, $\mathfrak{T}$ a cartan subalgebra, and β a Lie algebra automorphism of $\mathfrak{G}$ which maps $\mathfrak{T}$ to itself. We say that a finite-dimensional representation V of $\mathfrak{G}$ is pseudo-CM, or pseudo-CM with respect to β and $\mathfrak{T}$, if the following conditions hold:

(1) V is faithful and irreducible.
(2) As $\mathfrak{T}$-representation, V is the direct sum of $n = \dim(V)$ distinct weights $w_1, \ldots, w_n$ of $\mathfrak{T}$.
(3) V is $\mathfrak{G}$-isomorphic to its β-transform, i.e., there exists an element B in $\mathrm{GL}(V)$ which, acting by conjugation on $\mathrm{End}(V)$, normalizes (the images of) $\mathfrak{G}$ and $\mathfrak{T}$, and induces β on $\mathfrak{G}$.
(4) The element B, acting on V, cyclically permutes the n distinct one-dimensional weight spaces of $\mathfrak{T}$.

(In the application, the element B in $\mathrm{GL}(V)$ will be the element g occurring in hypothesis (3) of Theorem 1, and β will be $\mathrm{Ad}(g)$.)

THEOREM 3. *Notations as above, let V be a pseudo-*CM *representation of a semisimple $\mathfrak{G}$. Then there exist*

an integer $r \geqslant 1$,
a factorization of n as $n = n_1 \ldots n_r$ with all $n_i \geqslant 2$ and the n_i pairwise relatively prime,
Lie algebras $\mathfrak{G}_1, \ldots, \mathfrak{G}_r$, with each $\mathfrak{G}_i$ equal to one of
$\mathfrak{sl}(n_i)$ *if n_i is odd or $= 2$*
$\mathfrak{sl}(n_i)$ *or* $\mathfrak{sp}(n_i)$ *or* $\mathfrak{so}(n_i)$ *if n_i is even $\geqslant 4$,*

such that $(\mathfrak{G}, V)$ is isomorphic to $(\Pi(\mathfrak{G}_i), \otimes(\mathrm{std}(n_i)))$, where $\mathrm{std}(n_i)$ denotes the standard n_i-dimensional representation of $\mathfrak{G}_i$.

Proof. First write $\mathfrak{G}$ as a product of simple Lie algebras $\mathfrak{G}_i$, and then factor V as $\otimes(V_i)$, where V_i is an irreducible representation of $\mathfrak{G}$ which factors through $\mathfrak{G}_i$. Because the set of simple factors of $\mathfrak{G}$ and the corresponding tensor factors of V are unique, the β-invariance of V shows that the β-transform of a given V_i

must be one of the V_j. Group together in clumps the factors $(\mathfrak{G}_i, V_i)$ according to β-orbit. This gives us a new, "coarser" factorization of $(\mathfrak{G}, V)$ as a product of situations $(\mathfrak{G}_i, V_i)$ each of which is β-stable by construction. Let us denote by β_i the automorphism of $\mathfrak{G}_i$ induced by β, so that β is the product of the β_i, and choose elements B_i (unique up to scalars) in $\mathrm{GL}(V_i)$ inducing β_i, such that B is their tensor product. The cartan subalgebra $\mathfrak{T}$ is the product of its projections $\mathfrak{T}_i$ onto the factors $\mathfrak{G}_i$, and each of these $\mathfrak{T}_i$ is necessarily normalized by its B_i. It is immediate (compare [Ka-1], 3.1.6) that V is a pseudo-CM representation of $\mathfrak{G}$ with respect to β and $\mathfrak{T}$ if and only if both the following two conditions hold:

(a) the numbers $n_i = \dim(V_i)$ are pairwise relatively prime,
(b) for each i, V_i is a pseudo-CM representation of $\mathfrak{G}_i$ w.r.t. β_i and $\mathfrak{T}_i$.

This reduces us to showing that if $(\mathfrak{G}, V)$ is isotypical, i.e., a product of several copies of a single situation (simple Lie algebra $\mathfrak{G}_0$, irreducible representation V_0) and if V is a pseudo-CM representation of $\mathfrak{G}$ of dimension $n \geqslant 2$ with respect to an automorphism β which cyclically permutes the factors, then the only possibilities for $\mathfrak{G}$ are

$\mathfrak{SL}(n)$ if $n = 2$ or if n odd
$\mathfrak{SL}(n)$ or $\mathfrak{SO}(n)$ or $\mathfrak{Sp}(n)$ if n even $\geqslant 4$,

with $V = \mathrm{std}(n)$. To do this, we first show that ither $\mathfrak{G}$ is itself simple, or $\mathfrak{G}$ is $\mathfrak{SO}(4)$, with $V = \mathrm{std}(4)$. Indeed, if there are $k \geqslant 2$ factors cyclically permuted by β, and if we use β to identify them successively, we may suppose the automorphism B of the kth tensor power $(V_0)^{\otimes k}$ of V_0 to be of the form

$$v_1 \otimes v_2 \otimes \cdots \otimes v_k \mapsto v_2 \otimes v_3 \otimes \cdots \otimes v_k \otimes A(v_1),$$

for some A in $\mathrm{GL}(V_0)$ which normalizes both $\mathfrak{G}_0$ and $\mathfrak{T}_0$. The kth iterate of B is the automorphism $A \otimes \cdots \otimes A$, under which any weight of the form $(w, w, \ldots, w)$ of $\mathfrak{T} = \mathfrak{T}_0 \times \cdots \times \mathfrak{T}_0$ has an orbit of cardinality at most $\dim(V_0)$. Therefore the B-orbit of such a weight has cardinality at most $k \cdot \dim(V_0)$. By hypothesis, there is a single B-orbit, and its cardinality is $\dim(V)$. Thus we obtain the inequalities

$$k \cdot \dim(V_0) \geqslant \dim(V) = \big(\dim(V_0)\big)^k, \quad \text{with } k \geqslant 2 \text{ and } \dim(V_0) \geqslant 2,$$

which are only satisfied for $k = 2 = \dim(V_0)$, in which case $\mathfrak{G}_0$ must be $\mathfrak{SL}(2)$, $\mathfrak{G}$ is $\mathfrak{SL}(2) \times \mathfrak{SL}(2) = \mathfrak{SO}(4)$, and V is $\mathrm{std}(2) \otimes \mathrm{std}(2) = \mathrm{std}(4)$. We leave to the reader the verification that the standard representation of $\mathfrak{SO}(2k)$ is in fact a pseudo-CM representation for any $k \geqslant 2$.

It remains only to treat the case in which $\mathfrak{G}$ is simple. If β is inner, then V is a CM-representation, and by ([Ka-1], 3.2.7) we know that $\mathfrak{G}$ is either $\mathfrak{SL}(n)$ or (if n is even) $\mathfrak{Sp}(n)$, with $V = \mathrm{std}(n)$.

Suppose now that β is not inner. Because the weights of V are transitively permuted by an automorphism β of $(\mathfrak{G}, \mathfrak{T})$, they all have the same length with respect to any W-invariant scalar product on the $\mathbf{Q}$-span of the roots of $(\mathfrak{G}, \mathfrak{T})$. Therefore V is a minuscule representation of $\mathfrak{G}$, so in terms of any choice of base of the root system of $(\mathfrak{G}, \mathfrak{T})$, V is a fundamental representation ω_α. The β-invariance of V (together with Bourbaki Lie Chapter 8, Section 5, No. 2, corollary of Proposition 4 applied to β) shows that α is fixed under the nontrivial automorphism of the diagram induced by β. A glance at the tables (Bourbaki Lie Chapter 8, Section 7, No. 3, and Chapter 6, Planches) shows that the only such minuscule representations are the standard representation of $\mathfrak{SO}(2k)$ for $k \geqslant 3$, and the jth exterior power of the standard representation of $\mathfrak{Sl}(2j)$ for $j \geqslant 3$. (The case $j = 2$ coincides with the case $k = 3$.) It remains only to check that the second case is not a pseudo-CM representation of $\mathfrak{Sl}(2j)$ for $j \geqslant 3$.

For this, we argue as follows. The square ∂ of β is inner, so corresponds to an element of the symmetric group on $2j$ letters, while the weights of the V in question correspond to the subsets of these $2j$ letters having exactly j elements. Because β is supported to permute the weights transitively, ∂ can have at most two orbits acting on the weights. Consider the decomposition of ∂ as a disjoint product of cycles, of lengths $d_1, \ldots, d_r$, with each $d_i \geqslant 1$, $d_1 + \cdots + d_r = 2j$. Let S_i be the "support" of the ith cycle in ∂, so that the S_i are just the orbits of ∂ acting on the set $(1, 2, \ldots, 2j)$. For any subset K consisting of j elements, let us define

$$e_i = e_i(K) = \text{card}(K \text{ intersects } S_i).$$

The e_i are clearly constant on ∂-orbits, and, equally clearly, any set of integers $(e_1, \ldots, e_r)$ satisfying

$$(*) \qquad 0 \leqslant e_i \leqslant d_i \quad \text{for } i = 1, \ldots, r, \text{ and } e_1 + \cdots + e_r = j,$$

actually occurs for some K with j elements. Because ∂ has at most two orbits acting on the set of K's, there can be at most two solutions $(e_1, \ldots, e_r)$ of the above equations $(*)$. This implies that either $r = 1$, or that $r = 2$ and $d_1 = 1$, $d_2 = 2j - 1$. In either case, ∂ has order at most $2j$, so $\dim(V) \leqslant 4j$. But binomial coefficients increase towards the middle, so we have

$$4j \geqslant \dim(V) = \dim\big(\Lambda^j(\text{std}(2j))\big) \geqslant \dim\big(\Lambda^2(\text{std}(2j))\big) = j(2j - 1)$$

a contradiction since $j \geqslant 3$. This completes the proof of Theorem 3, and concludes Part 1. QED

Part 2. We continue to work over an algebraically closed field k of characteristic zero. Let U be a smooth connected affine curve over k, X its complete nonsingular model, $\infty \in X - U$ a "point at infinity", ω a fiber-functor on

D.E.(X/k), $n \geqslant 2$ an integer, $\mathbf{V}$ a D.E. on X/k of rank n, $V = \omega(\mathbf{V})$ its fiber at ω, $G_{\text{gal}} \subset \mathrm{GL}(V)$ its differential galois group with respect to ω, and $(G_{\text{gal}})^0$ the identity component of G_{gal}.

THEOREM 4. *Notations as above, suppose that*

(1) $\mathrm{Det}(\mathbf{V})$ *is of finite order, i.e.,* $(G_{\text{gal}})^0$ *lies in* $\mathrm{SL}(n) = \mathrm{SL}(V)$.
(2) *As representation of* $(G_{\text{gal}})^0$, V *is irreducible.*
(3) *At* ∞, *all the slopes of* $\mathbf{V}$ *have exact denominator* n.

Then $(G_{\text{gal}})^0$ *is either*

$\mathrm{SL}(n)$ *if* $n = 2$ *or* n *odd*
$\mathrm{SL}(n)$ *or* $\mathrm{SO}(n)$ *or* $\mathrm{Sp}(n)$ *if* n *is even and* $\geqslant 4$.

Moreover, in the case $(G_{\text{gal}})^0 = \mathrm{SO}(n)$, G_{gal} *is not contained in* $\mathbf{G}_m \cdot \mathrm{SO}(n)$.

Proof. We apply Theorem 2 not to G_{gal} but rather to the subgroup G of G_{gal} generated by $(G_{\text{gal}})^0$ and by the image $\rho(I_\infty)$ of I_∞ in G_{gal}. By ([Ka-1], 2.6.3), the image of I_∞ in the finite group $G_{\text{gal}}/(G_{\text{gal}})^0$ is cyclic, so $G^0 = (G_{\text{gal}})^0$, and $G/(G_{\text{gal}})^0$ is cyclic. To apply Theorem 2 we take for the torus T the image of $(I_\infty)^{(0+)}$, and we take for $g \in G$ the image of any element in I_∞ which generates its unique cyclic quotient of order n. By ([Ka-1], 2.5.9.3 and 2.6.6), all the conditions (1) through (5) of Theorems 1 and 2 are satisfied. QED

Remark 4.1. In the proof of Theorem 4 above, we could also have taken for T the smaller but "more explicit" torus which is the image in G_{gal} of $(I_\infty)^{(r/n)}$, where r/n is the unique slope at ∞ (cf. [Ka-1], 2.6.6).

In order for the above theorem to be useful, we need a criterion to decide the G^0-irreducibility of an irreducible representation of G, when G/G^0 is cyclic.

LEMMA 5. *Let* V *be a finite-dimensional* k*-vector space,* $G \subset \mathrm{GL}(V)$ *a Zariski closed subgroup of* $\mathrm{GL}(V)$, *and* $H \subset G$ *a Zariski closed normal subgroup of* G *such that the quotient* G/H *is a finite cyclic group. Suppose that* V *is* G*-irreducible. Then either* V *is* H*-irreducible, or* V *as* G*-representation is induced from a proper subgroup* K *of* G *which contains* H.

Proof. Because H is a normal subgroup of G of finite index and V is G-irreducible, either V is induced as in the assertion of the lemma or the restriction of V to H is H-isotypical, say $V = rW$ as H-representation, where W is an irreducible representation of H. By Jordan-Hölder theory, the isomorphism class of W must be invariant by G-conjugation. Because G/H is cyclic, W extends to a representation $\mathbf{W}$ of G. We have a natural map of G-representations

$$\mathbf{W} \otimes \mathrm{Hom}_H(\mathbf{W}, V) \to V,$$

which, being an isomorphism of H-representations, must be a G-isomorphism as well. Because V is G-irreducible, its two tensor factors must themselves be

G-irreducible. Thus $\mathrm{Hom}_H(\mathbf{W}, V)$ is G-irreducible. As it is an r-dimensional representation which factors through the cyclic quotient G/H, it can only be G-irreducible if $r = 1$, i.e., if V is itself H-irreducible. QED

We now turn to some concrete applications of the theory developed so far. We work on the curve $U = \mathbf{G}_m$. For every integer $d \geqslant 1$, we denote by

$$[d]\colon \mathbf{G}_m \to \mathbf{G}_m$$

the dth power mapping. We say that a D.E. $\mathbf{V}$ on $\mathbf{G}_m$ is "Kummer-induced" if it is of the form $[d]_*(\mathbf{W})$ for some $d \geqslant 2$ and some D.E. $\mathbf{W}$ on $\mathbf{G}_m$ (cf. [Ka-1], 1.4.6 and 1.4.7 for the compatibility with the representation-theoretic sense of "induced"). Note that if $\mathbf{V}$ is Kummer-induced, then its rank n must be divisible by d, and the quotient n/d is the rank of $\mathbf{W}$.

COROLLARY 6. *Notations as above, let* $\mathbf{V}$ *be an irreducible D.E. on* $\mathbf{G}_m$. *Then either* $\mathbf{V}$ *is Kummer-induced, or* V *is* $(G_{\mathrm{gal}})^0$*-irreducible.*

Proof. By ([Ka-1], 1.2.5 and 1.4.4), the finite quotient $G_{\mathrm{gal}}/(G_{\mathrm{gal}})^0$, for any D.E. on $\mathbf{G}_m$, is finite cyclic, being a finite quotient of $\pi_1(\mathbf{G}_m)$ corresponding to some Kummer covering of $\mathbf{G}_m$ by itself. The result now follows from Lemma 5, in virtue of ([Ka-1], 1.4.6). QED

If $\mathbf{V}$ is regular singular at zero, there is a simple criterion, in terms of its exponents at zero, to insure that it is not Kummer-induced. Let $a_1, \ldots, a_n$ be these exponents, viewed as lying in the additive quotient group $k/\mathbf{Z}$. If in fact $\mathbf{V} = [d]_*(\mathbf{W})$, then $\mathbf{W}$ is itself regular singular at zero, and if $b_1, \ldots, b_{n/d}$ are its exponents at zero, then the n exponents a_i of $\mathbf{V}$ at zero are simply the n quantities

$$(b_i + j)/d \bmod \mathbf{Z}, \quad \text{for } i = 1, \ldots, n/d \text{ and } j = 1, \ldots, d.$$

Let us say that a set of n not-necessarily-distinct elements of $k/\mathbf{Z}$ is Kummer-induced if there exist a divisor $d \geqslant 2$ of n and n/d elements b_i of $k/\mathbf{Z}$ such that the a_i are the n quantities displayed above. Thus we have:

CRITERION 7. *Let* $\mathbf{V}$ *be a D.E. on* $\mathbf{G}_m$ *which is regular singular at zero. If the exponents of* $\mathbf{V}$ *at zero are not Kummer-induced, then* $\mathbf{V}$ *is not Kummer-induced.*

Combining the above results, we find

THEOREM 8. *Let* $\mathbf{V}$ *be a D.E. on* $\mathbf{G}_m$ *of rank* $n \geqslant 2$. *Suppose that*

(1) $\mathrm{Det}(\mathbf{V})$ *is of finite order.*
(2) *At* ∞, *all the slopes of* $\mathbf{V}$ *have exact denominator* n.
(3) *At zero,* $\mathbf{V}$ *is regular singular and its exponents are not Kummer-induced.*

Then $(G_{\text{gal}})^0$ *is either*

$\mathrm{SL}(n)$ *if* $n = 2$ *or* n *odd*
$\mathrm{SL}(n)$ *or* $\mathrm{SO}(n)$ *or* $\mathrm{Sp}(n)$ *if* n *is even and* $\geqslant 4$.

Moreover, in the case $(G_{\text{gal}})^0 = \mathrm{SO}(n)$, G_{gal} *is not contained in* $\mathbf{G}_m \cdot \mathrm{SO}(n)$.

Example 9. Let $n \geqslant 2$, $a_1, \ldots, a_n$ a set of n elements in k whose image in $k/\mathbf{Z}$ is not Kummer-induced, and whose sum lies in $\mathbf{Q}$. Denote by D the invariant derivation zd/dz on $\mathbf{G}_m$. Let $m \geqslant 1$ be an integer prime to n, and $Q_m(z)$ a polynomial of degree m with $Q_m(0) = 0$. Then the D.E. on $\mathbf{G}_m$ corresponding to the n'th order operator

$$\Pi(D - a_i) - Q_m(z)$$

satisfies all the hypotheses of Theorem 8 (its exponents at zero are the $a_i \bmod \mathbf{Z}$, its determinant is the first order operator $D - \Sigma a_i$, and its slopes at ∞ are all equal to m/n), and hence its conclusion as well. In the particular case $m = 1$, we find the general Kloosterman equation, of which a very special case was treated in [Ka-1].

Algorithm 10. Here is a simple algorithm in terms of exponents to determine, when n is even and $\geqslant 4$ and the exponents are not Kummer-induced, which of the three possibilities SL, Sp, or SO for $(G_{\text{gal}})^0$ one has in the Kloosterman case $m = 1$. One first looks for a number c in k such that for the quantities b_i defined as $a_i - c$, the two sets of exponents $(b_1, \ldots, b_n)$ and $(-b_1, \ldots, -b_n)$ coincide $(\bmod \mathbf{Z})$. If no such c exists, then we are in the SL case. If such a c exists, then Σb_i is either an integer or a half-integer, and we are in the Sp or SO cases accordingly.

To see that this algorithm is correct, suppose first that such a quantity c exists. Then c is necessarily a rational number (because Σa_i is assumed rational), so the first-order operator $D - c$ is of finite order. Therefore tensoring our given D.E. by $D - c$, which exactly has the effect of replacing the a_i by the b_i, does not change the identity component of G_{gal}, and reduces us to the case where our Kloosterman equation is self-dual (cf. [Ka-1], 4.5.2 and 1.5.3). If the autoduality, unique up to a scalar, is alternating, then G_{gal} lies in the corresponding symplectic group Sp; since Sp lies in SL, the determinant $D - \Sigma b_i$ is trivial, which means exactly that Σb_i is an integer. If the autoduality is symmetric, then G_{gal} lies in the corresponding orthogonal group O, but by Theorem 8 it does not lie in SO; thus the determinant has order two but is nontrivial, which means exactly that Σb_i is a half-integer but not an integer.

Conversely, suppose that $(G_{\text{gal}})^0$ is equal to Sp or to SO. Then G_{gal} lies in the normalizer, inside GL, of either Sp or SO, so G_{gal} is itself contained in either $\mathbf{G}_m \cdot \mathrm{Sp}$ or $\mathbf{G}_m \cdot 0$. In either case, forming the square of the $\mathbf{G}_m$-factor is a well-defined character χ of G_{gal}, which corresponds to a rank one D.E. on $\mathbf{G}_m$ which is regular singular at both zero (because the original Kloosterman D.E. is)

and at ∞ (because its slope at ∞ is an integer which is $\leqslant 1/n$, the largest [and only] slope at ∞ of the original Kloosterman D.E., cf. [Ka-1], 2.5.8). Such a rank one D.E. must be of the form $D - d$, for some element d in k. Now define c to be $-d/2$. The $D - c$ is an inverse square root of $D - d$, so tensoring with $D - c$ turns our original Kloosterman D.E. into a self-dual one (i.e., into one whose G_{gal} is contained in either Sp or 0), whose exponents at zero, the b_i, are consequently stable mod $\mathbf{Z}$ by negation. This means exactly that we are in the situation of the previous paragraph. Hence the algorithm is correct in all cases.

References

[Bbk-1] N. Bourbaki, *Groupes et algebres de Lie*, Chapitres 4, 5, et 6, Paris, Masson, 1981.

[Bbk-2] _____, *Groupes et Algebres de Lie*, Chapitres 7 et 8, Paris, Diffusion CCLS, 1975.

[Ka-1] N. Katz, *On the calculation of some differential galois groups*, Inv. Math., **87** (1987) 13–61.

[Ka-2] _____, *Gauss Sums, Kloosterman Sums, and Monodromy Groups*, Annals of Math. Study **113**, to appear.

Katz: Department of Mathematics, Princeton University, Princeton, New Jersey 08544

Pink: Mathematisches Institut der Universität Bonn, Beringstrasse 1, D-5300 Bonn 1, Federal Republic of Germany