# THE CAMPBELL-HAUSDORFF GROUP AND A POLAR DECOMPOSITION OF GRADED ALGEBRA AUTOMORPHISMS 

A. Baider and R. C. Churchill


#### Abstract

Let $A=\prod_{k=k_{0}}^{\infty} \mathrm{gr}_{k}(A)$ be a complete graded (associative or Lie) algebra over a field of characteristic zero, filtered by the decreasing filtration $F_{j}(A)=\prod_{k=,}^{\infty} \operatorname{gr}_{k}(A)$. We let $\operatorname{Aut}(A)$ denote the group of filtration preserving automorphisms of $A$, and $\operatorname{Aut}_{0}(A)$ the subgroup consisting of those elements of $\operatorname{Aut}(A)$ which preserve the grading. In this paper we prove that every element of $\operatorname{Aut}(A)$ has a unique polar decomposition of the form $u_{0} \exp (d)$, where $u_{0} \in \operatorname{Aut}_{0}(A)$ and $d: A \rightarrow$ $A$ is a filtration increasing derivation.


Our central results, presented in $\S 4$, generalize and were inspired by theorems on decompositions of diffeomorphisms and symplectic mappings found in the dynamical systems literature; they also touch on the related topic of one-parameter group extensions. Particularly influential were Broer's treatment of normal forms of vector fields [4], and Sternberg's work on the formal aspects of dynamical systems [11]. The setting adopted here is that of filtered groups and algebras, for the reason that certain functorial properties of these structures are particularly well suited for the treatment of convergence questions arising from the use of the CampbellHausdorff formula. Broer (loc. cit.) credits Gérard and Levelt [6] with the first use of filtration techniques in this field.

A second aspect of our work is the introduction of a restricted class of "analytic functions" which map the ground field into appropriate filtered objects. Such functions turn out to be rather peculiar, in that they are always "entire" and have (except when identically zero) only finitely many zeros. Our study is limited to those properties which are relevant to this paper.

Applications of Theorem 4.5 are presented in the last two sections; we offer short proofs of two of these decompositions. That implied by the upper exact sequence of Theorem 5.4 is classical: C. L. Bouton was working on related problems as early as 1916 [2] (also see Lewis [8] and Sternberg [11]). The decomposition implied by Theorem 6.2 is also wellknown (see van der Meer [14, Lemma 2.11, p. 27]). The novelty of the
presentation here is that the relationships between the group structures are formulated explicitly.

The splittings of $\S 5$ and $\S 6$ are only the first step toward "normal form" theory. How such forms can be achieved by transforming coordinates is well-known (for vector fields and diffeomorphisms see e.g. Takens [12] and [13], and for Hamiltonian systems see e.g. Moser [9]), and will not be addressed here, although we briefly touch on the subject in examples ending these sections. For detailed historical surveys of normal form theory see van der Meer [14, pp. 42-45], Brjuno [3, pp. 134-9 and 142-3], and Dixon and Esterle [5, pp. 152-3].

The authors would like to thank the referee for constructive comments and criticisms regarding the original manuscript, and Richard Cushman for useful discussions of the literature.

1. The categories $\mathscr{G}, \mathscr{A}$ and $\mathscr{L}$. Here we collect basic definitions and establish notation. For more detail see [1] or [10].

Unless stated to the contrary $K$ denotes a field of characteristic zero and an algebra simply means a vector space over $K$ which admits a $K$-bilinear mapping $(x, y) \rightarrow x y$ into itself.

A filtered group (vector space, algebra) is a group (vector space, algebra) $X$ together with a decreasing sequence $F_{j_{0}}(X)=X \supset F_{j_{0}+1}(X)$ $\supset \cdots$ of normal subgroups (subspaces, ideals) such that

$$
\left(F_{p}(X), F_{q}(X)\right) \subset F_{p+q}(X)
$$

for all $p, q \geq j_{0}$, where $(x, y)=x y x^{-1} y^{-1}$, and, in the case of an algebra,

$$
F_{p}(X) F_{q}(X) \subset F_{p+q}(X)
$$

Throughout we assume $1 \geq j_{0} \in Z$, and when confusion cannot result we write $F_{j}(X)$ as $F_{j}$. The filtration $\left\{F_{j}\right\}$ is separated if $\bigcap_{j} F_{j}=\{e\}$ ( 0 ), the identity (origin) of $X$.

The order function of a filtered group (vector space, algebra) $X$ will be denoted by $\nu$, i.e. $\nu(x)=\sup \left\{j: x \in F_{j}\right\}, x \in X$. We recall the following properties:
(a) $\nu(e)=+\infty(\nu(0)=+\infty$ for vector spaces and algebras);
(b) $\nu\left(x y^{-1}\right)(\nu(x-y)$ for vector spaces and algebras) $\geq$ $\inf \{\nu(x), \nu(y)\} ;$
(c) $\nu(x)=\nu\left(x^{-1}\right)(\nu(-x)$ for vector spaces and algebras);
(d) $\nu((x, y)) \quad(\nu(x y)$ for algebras $) \geq \nu(x)+\nu(y)$;
(e) $\nu\left(x a x^{-1}\right) \geq \nu(x)$ (for groups); and
(f) $\nu(x y)=\nu(y x)$ (for groups).

In terms of the order function $X$ is separated if and only if $\nu(x)<\infty$ for all $x \neq e(0)$. In this case we set $|x|=2^{-\nu(x)}$, where $2^{-\infty}$ denotes 0 , and we have
(i) $|x| \geq 0$;
(ii) $|x|=0$ if and only if $x=e(0)$;
(iii) $|x y|(|x+y|$ for vector spaces and algebras) $\leq \max \{|x|,|y|\}$;
(iv) $|\lambda x|=|x|$ for $0 \neq \lambda \in K$ (for vector spaces and algebras); and
(v) $|x y| \leq|x||y|$ (for algebras).

When $X$ is separated the metric $(x, y) \rightarrow\left|x y^{-1}\right|(|x-y|)$ defines the topology on $X$ for which the $F_{j}$ constitute a basis of (open and closed) neighborhoods of the origin. All algebraic operations are continuous, assuming in the vector space and algebra cases that $K$ is given the discrete topology or, equivalently, the trivial filtration $F_{0}(K)=K, F_{1}(K)=\{0\}$. $X$ is complete if the metric is such.

A morphism $\varphi: X \rightarrow Y$ between filtered groups (vector spaces, algebras) is a homomorphism which preserves filtrations; in particular, all morphisms are continuous. Our interest will be in the following categories:
$\mathscr{G}$ : The category of filtered, separated complete groups;
$\mathscr{A}$ : The category of filtered, separated complete associative algebras with identity (always denoted 1 ), with all morphisms preserving 1 ; and
$\mathscr{L}:$ The category of filtered, separated and complete Lie algebras.
If $A \in \mathscr{A}$ we denote by $A_{L}$ the Lie algebra obtained from $A$ by using the commutator $[x, y]=x y-y x$ as bracket. The filtration on $A$ is compatible with this multiplication; hence $A_{L} \in \mathscr{L}$.

An infinite product $\Pi x_{j}$ in an object of $\mathscr{G}$ converges if and only if $x_{j} \rightarrow e$. Likewise, an infinite series $\sum x_{j}$ in an object of $\mathscr{A}$ or $\mathscr{L}$ converges if and only if $x_{j} \rightarrow 0$. Moreover, in either case we have

$$
\begin{equation*}
|x| \leq \max _{j}\left\{\left|x_{j}\right|\right\} \tag{1.1}
\end{equation*}
$$

where $x$ is the limit of the product or series in question. An important consequence is that if $A \in \mathscr{A}$, then any power series $\sum a_{j} x^{j}$ with coefficients in $A$ converges for all $x$ in the neighborhood $F_{1}$ of 0 . In fact the series will also converge for all $x \in A$ satisfying $x^{n} \in F_{1}$ for some $n \geq 1$. Because of this property $F_{1}$ will play a particularly special role in our considerations. This is the reason we assume w.l.o.g. that $j_{0} \leq 1$ for the first level $F_{j_{0}}$ of a filtration; otherwise we could define $F_{j}$ to be $F_{j_{0}}$ for $j=1, \ldots, j_{0}$.

To any graded group (vector space, algebra) $X=\Pi_{j \geq j_{0}} X_{j}$ we associate the filtration $F_{j}(X)=\prod_{n \geq j} X_{n}$, and to any filtered group (vector
space, algebra) we associate the graded group (vector space, algebra) $\operatorname{gr}(X)=\Pi_{j} \operatorname{gr}_{j}(X)$, where $\operatorname{gr}_{j}(X)=F_{j} / F_{j+1}$. Note that, contrary to standard usage, $\operatorname{gr}(X)$ represents the product rather than the direct sum of the $\operatorname{gr}_{j}(X)$. For a filtered, separated and complete vector space $X$ we have $X \simeq \operatorname{gr}(X)$, although the isomorphism is not natural.
2. The Campbell-Hausdorff group. For an arbitrary set $S$ let $V=V_{S}$ be the vector space freely generated by $S$ over $K$ and let $\tilde{T}_{S}=K \oplus V \oplus$ $(V \otimes V) \oplus \cdots$ denote the tensor algebra of $S . \tilde{T}_{S}$ is graded but not complete under the associated decreasing filtration; the completion $T_{S}$ is the graded algebra of formal series $a_{0}+a_{1}+\cdots$, where $a_{n} \in V^{\otimes n}$.
2.1. Proposition. The mapping $S \rightarrow F_{1}\left(T_{S}\right)$ is universal in the sense that for any $A \in \mathscr{A}$ and any mapping $\alpha: S \rightarrow F_{1}(A)$ there is a unique morphism $T_{S} \rightarrow A$ in $\mathscr{A}$ extending $\alpha$.

The extension will also be denoted by $\alpha$.
Proof. The universal property of $\tilde{T}_{S}$ implies that $\alpha$ extends uniquely to a homomorphism $\tilde{T}_{S} \rightarrow A$. Since we assume $\alpha(S) \subset F_{1}(A)$, induction shows this extension to be filtration preserving, hence uniformly continuous. Since $\tilde{T}_{S}$ is dense in $T_{S}$, the claim follows.

Let $L_{S}$ denote the closure in $\left(T_{S}\right)_{L}$ of the Lie subalgebra generated by $S$. Since $L_{S}$ is the completion of the free Lie algebra of $S$ ([7], p. 225) we have the following analogue in $\mathscr{L}$ of Proposition 2.1.
2.2. Proposition. The mapping $S \rightarrow F_{1}\left(L_{S}\right)$ is universal: for any $L \in \mathscr{L}$ and any mapping $\alpha: S \rightarrow F_{1}(L)$ there is a unique morphism $L_{S} \rightarrow L$ extending $\alpha$.

When $S=X=\left\{X_{1}, \ldots, X_{n}\right\}$ is a finite set, the tensor algebra $T_{S}=T_{X}$ is simply the algebra of formal non-commutative power series $f$ in the variables $X_{1}, \ldots, X_{n}$. In view of Proposition 2.1 such an $f$ defines a (universal) function $f_{A}: F_{1}(A)^{n} \rightarrow A$ through the substitution of variables $X \rightarrow x \in F_{1}(A)^{n}$. More explicitly: if $\alpha: T_{X} \rightarrow A$ is the morphism extending $\alpha: X_{i} \rightarrow x_{i}$, then $f_{A}(x)=\alpha(f)$.
2.3. Proposition. For $f \in F_{p}\left(T_{X}\right)$ the mapping $f_{A}$ is continuous. Moreover, the collection $\left\{f_{A}\right\}_{A \in \mathscr{A}}$ defines a natural transformation between the functors $F_{1}(A)^{n}$ and $F_{p}(A)$ on $\mathscr{A}$, i.e. for any morphism $\varphi: A \rightarrow B$ the
diagram

$$
\begin{array}{ccc}
F_{1}(A)^{n} & \varphi \times \cdots \times \varphi & F_{1}(B)^{n} \\
f_{A} \downarrow & & \downarrow f_{B} \\
F_{p}(A) & \xrightarrow{\varphi} & F_{p}(B)
\end{array}
$$

commutes. The analogous statements hold when $T_{X}$ is replaced by $L_{X}$.
Proof. Let $x=\left(x_{1}, \ldots, x_{n}\right) \in F_{1}(A)^{n}$ and $h=\left(h_{1}, \ldots, h_{n}\right) \in F_{j}(A)^{n}$. Then for any finite sequence $i_{1}, \ldots, i_{k}$ of the integers $1, \ldots, n$ and any non-negative integers $q_{1}, \ldots, q_{k}$ the difference $\prod_{m=1}^{k}\left(x_{i_{m}}+h_{i_{m}}\right)^{q_{m}}$ $\prod_{m=1}^{k} x_{i_{m}}^{q_{m}}$ belongs to the closed subspace $F_{j}(A)$ of $A$, and the same holds for the difference $f_{A}(x+h)-f_{A}(x)$, which is a convergent series of such monomials. Continuity follows.

To prove naturality simply note that when $x \in F_{1}(A)^{n}$ the unique morphism $T_{X} \rightarrow B$ sending $x_{i}$ to $\varphi\left(x_{i}\right)$ is $\varphi \circ \alpha$. Therefore

$$
f_{B}\left(\varphi\left(x_{1}\right), \ldots, \varphi\left(x_{n}\right)\right)=(\varphi \circ \alpha)(f)=\varphi(\alpha(f))=\varphi\left(f_{A}(x)\right)
$$

In view of this naturality we drop the subscript $A$ from $f_{A}$.
As an example consider the Neumann series $f(X)=1+X+X^{2}$ $+\cdots \in K[[X]]$. This defines the function $x \rightarrow(1-x)^{-1}=1+x+x^{2}$ $+\cdots$ on $F_{1}(A)$ for any $A \in \mathscr{A}$, and shows that all elements of the neighborhood $1+F_{1}(A)$ of 1 are invertible.

The exponential and $\operatorname{logarithmic}$ series $\exp (X)$ and $\log (1+X)$ will play an important role in the sequel. The corresponding functions establish homomorphisms between the neighborhoods $F_{1}(A)$ of the origin and $1+F_{1}(A)$ of 1 . Moreover, for any $\mathscr{A}$-morphism $\varphi: A \rightarrow B$ the diagram

$$
\begin{array}{ccc}
F_{1}(A) & \xrightarrow{\varphi} & F_{1}(B) \\
\exp \downarrow \uparrow \log & & \exp \downarrow \uparrow \log  \tag{2.4}\\
1+F_{1}(A) & \xrightarrow{\varphi} & 1+F_{1}(B)
\end{array}
$$

commutes.
2.5. Remark. For $A \in \mathscr{A}$ define the radical of $F_{1}(A)$ as $\operatorname{rad}\left(F_{1}(A)\right)=$ $\left\{a \in A: a^{n} \in F_{1}(A)\right.$ for some $\left.n \geq 1\right\}$; this is an ideal if $A$ is commutative. The power series defining $(1-x)^{-1}, \exp (x)$ and $\log (1+x)$ converge for $x \in \operatorname{rad}\left(F_{1}(A)\right)$, and we may regard these functions as being defined on these (possibly) larger domains.

Let $T_{X, Y}$ be the complete free algebra in two variables $X, Y$ and consider the formal power series $W=W(X, Y)=\log (\exp (X) \exp (Y)) \in$ $T_{X, Y}$. By the Campbell-Hausdorff formula ([7], p. 227) we have $W \in$ $F_{1}\left(L_{X, Y}\right)$, where

$$
\begin{align*}
W= & X+Y+(1 / 2)[X, Y]+(1 / 12)[X,[X, Y]]  \tag{2.6}\\
& +(1 / 12)[Y,[Y, X]]+\cdots .
\end{align*}
$$

By Proposition 2.3 the power series $W$ defines a natural transformation between the functors $F_{1}(L) \times F_{1}(L)$ and $F_{1}(L)$ on $\mathscr{L}$ which we denote by *.
2.7. Theorem. * is a group operation, and gives $F_{1}(L)$ the structure of a filtered, separated complete group with filtration $\left\{F_{j}(L)\right\}_{j \geq 1}$. Moreover, the assignment $L \in \mathscr{L} \rightarrow\left(F_{1}(L), *\right) \in \mathscr{G}$ is functorial, and is characterized by the property that the identity

$$
\begin{equation*}
x * y=\log (\exp (x) \exp (y)) \tag{2.8}
\end{equation*}
$$

holds for any $L \in \mathscr{L}$ of the form $A_{L}$ for some $A \in \mathscr{A}$.
We call $\left(F_{1}(L), *\right)$ the Campbell-Hausdorff group of $L$.

Proof. First assume $L=A_{L}$ for some associative $A \in A$. If $x, y \in$ $F_{1}(L)=F_{1}(A)$, then the $\mathscr{A}$-morphism $\alpha: T_{X, Y} \rightarrow A$ sending $X$ to $x$ and $Y$ to $y$ restricts to an $\mathscr{L}$-morphism sending $W$ to $x * y$. Naturality of exp, $\log$ and $*$ then gives (2.8) for Lie algebras of this special form, as well as for Lie subalgebras thereof; the group properties follow immediately.

Now suppose $L \in \mathscr{L}$ is arbitrary and $x, y, z \in F_{1}(L)$. Then we can find an associative $A \in \mathscr{A}$, an $\mathscr{L}$-subalgebra $\tilde{L} \subset A_{L}$ and an $\mathscr{L}$-morphism $\varphi: \tilde{L} \rightarrow L$ with range including $x, y$ and $z$, e.g. take $A=T_{X, Y, Z}$ and $\tilde{L}=L_{X, Y, Z}$. By the previous paragraph $\left(F_{1}(\tilde{L}), *\right)$ is a group, hence $(x * y) * z=x *(y * z)$ by naturality; the other group properties for $\left(F_{1}(L), *\right)$ are proven in a similar manner.

To verify the required commutator relation for $\left\{F_{J}(L)\right\}_{J \geq 1}$ assume $x \in F_{p}(L), y \in F_{q}(L)$ and set $z=x * y *(-x) *(-y)$. From (2.6) we see that for $a \in F_{r}(L)$ and $b \in F_{s}(L)$ we have $a * b \equiv a+b+(1 / 2)[a, b]$ $\left(\bmod F_{r+s+1}(L)\right)$, and so

$$
\begin{aligned}
z & \equiv(x+y+(1 / 2)[x, y]) *(-x-y+(1 / 2)[x, y]) \\
& \equiv[x, y] \quad\left(\bmod F_{p+q+1}(L)\right)
\end{aligned}
$$

But $[x, y] \in F_{p+q}(L)$, hence $z \in F_{p+q}(L)$ as desired.

As for uniqueness, let $\left(F_{1}(L), \#\right)$ be a second functor with the same properties. By (2.8) \# and * must agree on Lie algebras of the form $A_{L}$, and by naturality on Lie subalgebras thereof. For arbitrary $L \in \mathscr{L}$ and $x, y \in L$ simply construct $\tilde{L}$ and $\varphi: \tilde{L} \rightarrow L$ as above; then $x \# y=x * y$ by naturality.

Remark. In ([10], Prop. 2.3) it is shown that if $G$ is a filtered group then $L=\Pi_{j} F_{j} / F_{j+1}$ is a graded Lie algebra over $Z$, where the Lie bracket on $L$ is induced by the commutator on $G$. The above proof shows that $\left(\operatorname{gr}\left(F_{1}(L)\right), *\right) \simeq \operatorname{gr}(L)$ in positive degrees, so that if $L=\Pi_{j} L_{j}$, $j \geq 1$, then $F_{1}(L)=L$ and $\operatorname{gr}(L, *) \simeq L$. In this sense the CampbellHausdorff group can be viewed as a partial inverse of the functor $\mathrm{gr}: \mathscr{G} \rightarrow \mathscr{L}_{Z}$, where $\mathscr{L}_{Z}$ is the category of filtered complete Lie algebras over $Z$. As we will not pursue this matter we leave it to the reader to formulate the precise statement describing the relationship between these functors.
3. Analytic functions. The initial results in this section do not require our standing hypothesis that the characteristic of $K$ be zero. $V$ will be a filtered, separated and complete $K$-vector space.

We will consider functions $f(t)$ on $K$ defined by power series $\sum a_{j} t^{j}$, where $a_{j} \in V$, and we will call such functions analytic. Note, however, that if such a power series converges at a point $0 \neq t_{0} \in K$ then it converges for all $t \in K$, Indeed, we have $\left|a_{j} t^{j}\right|=\left|a_{j}\right|=\left|a_{j} t_{0}^{j}\right| \rightarrow 0$. Thus "analytic" is equivalent to "entire" in our context. More general definitions can obviously be formulated, e.g. assuming domains in a filtered algebra $A$, but this will be sufficient for our purposes.
3.1. Lemma. Let $t_{0}, \ldots, t_{n} \in K$ be distinct and let $b_{0}, \ldots, b_{n} \in V$. Then there is a unique polynomial $p(t)=\sum_{j=0}^{n} a_{j} t^{j}, a_{j} \in V$, such that $p\left(t_{i}\right)=b_{i}$ for $i=0, \ldots, n$. Moreover,

$$
\left|a_{j}\right| \leq \max \left\{\left|b_{i}\right|\right\}, \quad j=0, \ldots, n
$$

Proof. Simply view $p\left(t_{i}\right)=b_{i}$ as a set of $n$ linear equations for $a_{0}, \ldots, a_{n}$; the system has a unique solution since the coefficient matrix is the invertible Vandermonde matrix $\left(t_{i}^{j}\right)$. Since each $a_{j}$ can be expressed as a linear combination of the $b_{i}$, the estimates follow from (iii) and (iv) of §1.
3.2. Elementary properties of analytic functions. Assume $f(t)=\sum a_{j} t^{j}$ is analytic and let $p_{n}(t)=\sum_{j=0}^{n} a_{j} t^{j}, r_{n}(t)=\sum_{j=n+1}^{\infty} a_{j} t^{j}$.
(a) $p_{n} \rightarrow f$ uniformly. By (1.1) and (iv) of $\S 1$ we have $\left|r_{n}(t)\right| \leq$ $\max _{j \geq n+1}\left\{\left|a_{j}\right|\right\}$, and $\left|a_{j}\right| \rightarrow 0$.
(b) All a, vanish if f has infinitely many distinct zeros. In particular, a non-trivial analytic function has only finitely many distinct zeros. Suppose $t_{0}, \ldots, t_{n}$ are distinct zeros of $f$, and set $b_{j}=-r_{n}\left(t_{j}\right), j=0, \ldots, n$. Then $f\left(t_{j}\right)=0$ may be written as $p_{n}\left(t_{j}\right)=b_{j}$, hence $\left|a_{j}\right| \leq \sup _{t}\left\{\left|r_{n}(t)\right|\right\}$ by Lemma 3.1, and the result then follows from (a).
(c) When $K$ is infinite the coefficients of $f$ are uniquely determined. This is immediate from (b).

In view of (c) we henceforth assume $K$ is infinite.
The space of analytic functions is filtered by $F_{j}=\left\{f: K \rightarrow F_{j}(V)\right\}$. It is clear that the associated metric is defined by the supremum norm $|f|=\sup _{t}\{|f(t)|\}$.
(d) We have $|f|=\max _{j}\left\{\left|a_{j}\right|\right\}=\max _{t}\{|f(t)|\}$. This is immediate from (c) when $|f|=0$, so assume $|f|>0$ and note from (1.1) and (iv) of $\S 1$ that $|f| \leq \sup _{j}\left\{\left|a_{j}\right|\right\}$. To obtain the reverse inequality first observe using (a) that $\left|r_{n}\right| \rightarrow 0$, and so $\left|r_{n}\right| \leq|f|$ for $n \geq n_{0}$. But then (iii) of $\S 1$ implies $\left|p_{n}(t)\right| \leq \max \left\{\left|f_{n}(t)\right|,\left|r_{n}(t)\right|\right\} \leq|f|$, whereas Lemma 3.1 gives $\left|a_{j}\right| \leq \max _{k}\left\{\left|p_{n}\left(t_{k}\right)\right|\right\} \leq|f|$ provided $j \leq n$ and the $t_{k}, k=0, \ldots, n$, are distinct points of $K$. Therefore $|f| \geq \sup _{j}\left\{\left|a_{j}\right|\right\}$. Sup can be replaced by max since 0 is the only accumulation point of the values of the metric on $V$ and $|f|>0$.
(e) The space of analytic functions is complete. If $\left\{f_{n}\right\}$ is Cauchy then for each $j$ the coefficient sequence of $t^{j}$ also has this property, hence converges to some element $a_{j} \in V$. One now checks that $f_{n} \rightarrow \sum a_{j} t^{j}$.
(f) If $A \in \mathscr{A}$ the space of analytic $f: K \rightarrow A$ is an algebra. If $f(t)=$ $\sum a_{j} t^{j}$ and $g(t)=\Sigma b_{n} t^{n}$ then it is a straightforward verification that $f(t) g(t)=\sum c_{n} t^{n}$, where $c_{n}=\sum a_{j} b_{n-j}$.

Henceforth we assume $K$ has characteristic zero. Since $K$ is infinite the formal definition $f^{\prime}(t)=\sum n a_{n} t^{n-1}$ of the derivative of an analytic function $f(t)=\sum a_{n} t^{n}$ is unambiguous by 3.2(c). One has $f^{(n)}(0)=n!a_{n}$, and as a result the Taylor formula

$$
\begin{equation*}
f(t)=\sum_{n=0}^{\infty}\left(\frac{1}{n!}\right) f^{(n)}(0) t^{n} \tag{3.3}
\end{equation*}
$$

holds.

If one wished to define $f^{\prime}$ analytically, rather than formally, a topology on $K$ would be needed. However, since the $F_{j}(V)$ are linear subspaces, (iv) of $\S 1$ shows that the only topology which makes scalar multiplication continuous is the discrete topology, so that $h \rightarrow 0$ in $K$ if and only if $h$ is eventually identically 0 . With this understanding it is easy to see that

$$
\begin{equation*}
f^{\prime}(t)=\lim _{h \rightarrow 0} \frac{f(t+h)-f(t)}{h}:=\left.\frac{f(t+h)-f(t)}{h}\right|_{h=0} . \tag{3.4}
\end{equation*}
$$

This last expression is symbolic for the following recipe: factor $h$ from $f(t+h)-f(t)$; divide by $h$; then set $h=0$.

We also define the primitive of $f(t)=\sum a_{n} t^{n}$ formally, i.e. $\int_{0}^{t} f(s) d s$ $=\Sigma\left(a_{n} /(n+1)\right) t^{n+1}$; (iii) and (iv) of $\S 1$ show this to be an analytic function. If $Q_{n}(t)=\sum_{j=0}^{n-1}\left(a_{j} /(j+1)\right) t^{j+1}$ is the $n$ th-partial sum, then $\left|Q_{n}(t)\right| \leq \max _{0 \leq j \leq n-1}\left\{\left|a_{j} / j+1\right|\right\}=\max _{0 \leq j \leq n-1}\left\{\left|a_{j}\right|\right\} \leq|f|$, hence

$$
\begin{equation*}
\left|\int_{0}^{t} f(s) d s\right| \leq|f| \tag{3.5}
\end{equation*}
$$

3.6. Theorem. Suppose $G: V \rightarrow V$ is Lipschitz with Lipschitz constant contained in $[0,1)$, and suppose $G \circ \xi: K \rightarrow V$ is analytic whenever $\xi: K \rightarrow V$ is analytic. Then for each $v \in V$ the initial-value problem

$$
\dot{\eta}=G(\eta), \quad \eta(0)=v
$$

has a unique solution.
Proof. The space $H$ of analytic $\xi: K \rightarrow V$ is complete, and $T: H \rightarrow H$, defined by $T \xi(t)=v+\int_{0}^{t} G(\xi(s)) d s$, is a uniform contraction by (3.5) and the Lipschitz assumption on $G$. The result thus follows from the contraction mapping principle.
4. The polar decomposition of $\operatorname{Aut}(A)$. In this section we let $A$ denote a fixed element of $\mathscr{A}$ or $\mathscr{L}$, and we let $\operatorname{end}(A)$ denote the space of endomorphisms of $A$ as a filtered vector space. (We write "end $(A)$ " rather than " $\operatorname{End}(A)$ " as a reminder that elements of $\operatorname{end}(A)$ are unrelated to the multiplicative structure of $A$.) If for $j \geq 0$ we let $F_{j}(\operatorname{end}(A))=\{u \in$ $\left.\operatorname{end}(A): u\left(F_{n}\right) \subset F_{n+j}\right\}$, then $\left\{F_{j}(\operatorname{end}(A))\right\}$ is a separated filtration of end $(A)$, and the resulting metric space is complete. Thus $\operatorname{end}(A) \in \mathscr{A}$. If $A=\prod_{j} A_{j}$ is graded so is end $(A)$ : set $\operatorname{end}_{j}(A)=\left\{u \in \operatorname{end}(A): u\left(A_{n}\right) \subset\right.$ $\left.A_{n+j}\right\}$. Notice that $u=\sum_{j=0}^{\infty} u_{j}$, where for $x=\sum x_{n} \in \Pi_{n} A_{n}$ we have

$$
\begin{equation*}
u_{j}(x)=\sum_{n}\left(u\left(x_{n}\right)\right)_{n+j} . \tag{4.1}
\end{equation*}
$$

Any $u \in \operatorname{end}(A)$ induces an endomorphism on $F_{j} / F_{j+1}$, and as a result an endomorphism $\Pi u \in \operatorname{end}_{0}(\operatorname{gr}(A))$. When $A$ is graded and $u=u_{0}+u_{1}+\cdots$ we simply have $\Pi u=u_{0}$. Since $A \simeq \operatorname{gr}(A)$ as vector spaces the homomorphism $\Pi: \operatorname{end}(A) \rightarrow \operatorname{end}_{0}(\operatorname{gr}(A))$ must be surjective, and we obviously have $\operatorname{Ker}(\Pi)=F_{1}(\operatorname{end}(A))$. In other words, the sequence

$$
\begin{equation*}
0 \rightarrow F_{1}(\operatorname{end}(A)) \rightarrow \operatorname{end}(A) \xrightarrow{\Pi} \operatorname{end}_{0}(\operatorname{gr}(A)) \rightarrow 0 \tag{4.2}
\end{equation*}
$$

is exact.
4.3. Lemma ([1], p. 178) $u \in \operatorname{end}(A)$ is invertible if and only if $\Pi u \in \operatorname{end}_{0}(\operatorname{gr}(A))$ has this property.

Now let $\operatorname{Aut}(A) \subset \operatorname{end}(A)$ denote the group of filtered algebra automorphisms of $A$, and as a filtration on $\operatorname{Aut}(A)$ let $F_{0}(\operatorname{Aut}(A))=\operatorname{Aut}(A)$ and $F_{j}(\operatorname{Aut}(A))=\left(1+F_{j}(\operatorname{end}(A))\right) \cap \operatorname{Aut}(A)$. To see that $\operatorname{Aut}(A) \in \mathscr{G}$ first notice that for $1+u \in F_{p}(\operatorname{Aut}(A))$ we have $(1+u)^{-1}$ given by the Neumann series, and as a consequence whenever $1+v \in F_{q}(\operatorname{Aut}(A))$ we have $(1+u, 1+v) \equiv 1+[u, v]\left(\bmod F_{p+q+1}(\operatorname{Aut}(A))\right)$. This gives the required commutator property, and since the topology on $\operatorname{Aut}(A)$ is that it inherits as a closed subspace of $\operatorname{end}(A), \operatorname{Aut}(A) \in \mathscr{G}$ follows.

Let $\operatorname{Der}(A)$ denote the collection of filtration preserving derivations of $A$. This is a closed Lie subalgebra of $(\operatorname{end}(A))_{L}$, and therefore belongs to $\mathscr{L}$.
4.4. Proposition. For any $a \in \operatorname{Der}(A) \cap \operatorname{rad}\left(F_{1}(\operatorname{end}(A))\right)$ we have $\exp (a) \in \operatorname{Aut}(A)$. In particular, exp: $F_{1}(\operatorname{Der}(A)) \rightarrow \operatorname{Aut}(A)$.

Proof. The argument is standard and uses the Leibniz rule $a^{n}(x y)=$ $\sum_{j=0}^{n}\binom{n}{j} a^{j}(x) a^{n-j}(y)$. The condition that $a \in \operatorname{rad}\left(F_{1}(\operatorname{end}(A))\right)$ insures convergence in the following computation:

$$
\begin{aligned}
\exp (a)(x y) & =\sum_{n}\left(\frac{1}{n!}\right) \sum_{j=0}^{n}\binom{n}{j} a^{j}(x) a^{n-j}(y) \\
& =\sum_{j=0}^{\infty} \sum_{n=j}^{\infty}\left(\frac{1}{j!}\right) a^{j}(x)\left(\frac{1}{(n-j)!}\right) a^{n-j}(y) \\
& =\exp (a)(x) \exp (a)(y)
\end{aligned}
$$

Let $A \in \mathscr{A}$ be graded and let $\mathrm{Aut}_{0}(A)$ denote those automorphisms of $A$ which preserve degree. We endow $\operatorname{Aut}_{0}(A)$ with the trivial filtration and thereby regard it as an object of $\mathscr{G}$.
4.5. Theorem. For graded $A$ we have a split exact sequence

$$
0 \rightarrow F_{1}(\operatorname{Der}(A)) \xrightarrow{\exp } \operatorname{Aut}(A) \xrightarrow{\Pi} \operatorname{Aut}_{0}(A) \rightarrow e
$$

of $\mathscr{G}$-morphisms, where $F_{1}(\operatorname{Der}(A))$ is the Campbell-Hausdorff group of $\operatorname{Der}(A)$. In particular, $\operatorname{Aut}(A)$ is the semidirect product of $F_{1}(\operatorname{Der}(A))$ with Aut $_{0}(A)$.

Stated less formally, the conclusion is that any $u \in \operatorname{Aut}(A)$ has a unique "polar decomposition" $u=u_{0} \exp (a)$ with $u_{0} \in \operatorname{Aut}_{0}(A)$ and $a \in F_{1}(\operatorname{Der}(A))$. Obviously we can also write $u$ as $\exp (b) u_{0}$, where $b=u_{0} a u_{0}^{-1}$.

Proof. (2.4) and Proposition 4.4 imply exp: $F_{1}(\operatorname{Der}(A)) \rightarrow \operatorname{Aut}(A)$ is an injection, and since $\operatorname{Aut}_{0}(A) \subset \operatorname{Aut}(A), \Pi: \operatorname{Aut}(A) \rightarrow \operatorname{Aut}_{0}(A)$ must be a surjection. Moreover, the inclusion $\exp \left(F_{1}(\operatorname{Der}(A))\right) \subset \operatorname{Ker}(\Pi)$ is obvious, and the inclusion $\operatorname{Aut}_{0}(A) \subset \operatorname{Aut}(A)$ provides the section defining the splitting. It remains only to prove that $\operatorname{Ker}(\Pi) \subset$ $\exp \left(F_{1}(\operatorname{Der}(A))\right)$.

To this end consider $g=1+u \in \operatorname{Ker}(\Pi) \subset \operatorname{Aut}(A)$, and notice that $g(x y)=g(x) g(y)$ implies $u(x y)=u(x) y+x u(y)+u(x) u(y)$. Now write $u=u_{1}+\cdots$, apply this last equality to homogeneous elements $x \in A_{p}, y \in A_{q}$, and consider the $(1+p+q)$ th-component; it follows that $u_{1}$ must be a derivation. On the other hand, (2.4) implies that $g=\exp (a)$ for some $a=a_{1}+a_{2}+\cdots \in F_{1}(\operatorname{end}(A))$, and on comparing degrees we see that $a_{1}=u_{1}$, hence $a_{1} \in F_{1}(\operatorname{Der}(A))$. Now assume, by induction, that $a_{i} \in F_{i}(\operatorname{Der}(A))$ for $1 \leq i \leq j-1$ and set $b=a_{1}$ $+\cdots+a_{j-1}$, so that $\exp (-b)$, and therefore $\exp ((-b) * a)=(\exp (-b)) g$ are in $\operatorname{Aut}(A)$. We observe that $(-b) * a \equiv(-b) *\left(b+a_{j}+\cdots\right) \equiv$ $-b+b+a_{j}+(1 / 2)\left[-b, b+a_{j}+\cdots\right]\left(\bmod F_{j+1}\right)$, so that $(-b) * a=$ $a_{j}+\cdots$; therefore $\exp ((-b) * a)=1+v$, where $v=a_{j}+\cdots$. But the argument for $1+u$ can now be applied to $1+v$ to show that $a_{j} \in F_{j}(\operatorname{Der}(A))$, and since $\operatorname{Der}(A)$ is complete it follows that $a=\sum a_{j} \in$ $\operatorname{Der}(A)$.

We now turn to the closely related question of interpolation. An (analytic) one-parameter group in an algebra $A \in \mathscr{A}$ is an analytic homomorphism $\varphi: K \rightarrow A$; an element of $A$ extends to a one-parameter
group if it is the value at 1 of such a mapping. Any derivation $a \in$ $\operatorname{rad}\left(F_{1}(A)\right)$ defines a one-parameter group by means of the formula $\varphi(t)=\exp (t a)$.

## "Tournants Dangereux:"

(1) The condition $a \in \operatorname{rad}\left(F_{1}(A)\right)$ is necessary to insure convergence of the exponential series.
(2) If $A$ is an algebra over $C$ or $R$ the classical one-parameter groups $t \rightarrow e^{k t}$ are not analytic in our sense.
4.6. Theorem. Let $A$ be an algebra in $\mathscr{A}$ or $\mathscr{L}$, and let $u \in \operatorname{Aut}(A)$. Then $u$ extends to an analytic one-parameter group if and only if $u=\exp (a)$ for some $a \in \operatorname{Der}(A) \cap \operatorname{rad}\left(F_{1}(\operatorname{end}(A))\right)$.

Proof. Suppose $u=u(1)$, where $u(t)$ is an analytic one-parameter group. Then (3.4) gives
$u^{\prime}(t)=(u(t+s)-u(t)) /\left.s\right|_{s=0}=\left.s^{-1}(u(s)-1) u(t)\right|_{s=0}=u^{\prime}(0) u(t)$, with $u^{\prime}(0)=a \in \operatorname{end}(A)$. Moreover, repeated differentiation now gives $u^{(n)}(0)=a^{n}$. Taylor's formula thus implies $u=\sum a^{n} / n!$, hence $a^{n} \rightarrow 0$, and therefore $a \in \operatorname{rad}\left(F_{1}(\operatorname{end}(A))\right)$. To see that $a \in \operatorname{Der}(A)$ simply note that

$$
\begin{aligned}
a(x y) & =u^{\prime}(0)(x y)=\left.(d / d t)(u(t)(x y))\right|_{t=0} \\
& =\left.(d / d t)(u(t) x u(t) y)\right|_{t=0}=a(x) y+x a(y)
\end{aligned}
$$

The converse is obvious: if $u=\exp (a)$, let $u(t)=\exp (t a)$.
Remark. The condition that $a \in \operatorname{rad}\left(F_{1}(\operatorname{end}(A))\right)$ is equivalent to $\Pi a$ being nilpotent.
5. Application: $\operatorname{Diff}(n)$. Let $A=A(n)=K[[x]] \in \mathscr{A}$ denote the graded $K$-algebra of formal power series in $x=\left(x^{1}, \ldots, x^{n}\right)$. Theorem 4.5 guarantees the existence of a split exact sequence

$$
\begin{equation*}
0 \rightarrow F_{1}(\operatorname{Der}(A)) \xrightarrow{\exp } \operatorname{Aut}(A) \xrightarrow{\Pi} \operatorname{Aut}_{0}(A) \rightarrow e \tag{5.1}
\end{equation*}
$$

of $\mathscr{G}$-morphisms; the aim of this section is to identify this with a second sequence

$$
\begin{equation*}
0 \rightarrow F_{1}(\operatorname{Vect}(n)) \xrightarrow{\mathrm{Exp}} \operatorname{Diff}(n) \xrightarrow{\mathrm{Jac}} \mathrm{Gl}\left(K^{n}\right) \rightarrow e \tag{5.2}
\end{equation*}
$$

which we now explain.
First, Vect $(n)$ denotes the space of formal vector fields $X=\sum X^{i} \partial / \partial x^{i}$ in $K^{n}$ with the usual Lie bracket and having the origin as an equilibrium
point. $\operatorname{Vect}(n) \in \mathscr{L}$ when graded by $\operatorname{Vect}_{j}(n)=\left\{X: X^{i}\right.$ is homogeneous of degree $j+1\}, j \geq 0$. In (5.2) $F_{1}(\operatorname{Vect}(n))$ denotes the CampbellHausdorff group.

Secondly, $\operatorname{Diff}(n)$ is the group of non-singular formal power series self-mappings of $K^{n}$ fixing the origin; the group operation is formal composition (which requires the absence of constant terms to be defined) and the identity is the $n$-tuple of coordinate functions $x=\left(x^{1}, \ldots, x^{n}\right)$. We note that $\operatorname{Diff}(n) \subset M_{0}(n):=F_{1}(A)^{n}$, the semigroup (again under composition) of formal power series $\varphi(x)=a x+\cdots$. One has $\varphi \in$ $\operatorname{Diff}(n)$ if and only if the Jacobian $a=\varphi^{\prime}(0)=\operatorname{Jac}(\varphi)$ is non-singular.

To define $\operatorname{Exp}: F_{1}(\operatorname{Vect}(n)) \rightarrow \operatorname{Diff}(n)$ associate with $X=\sum X^{i} \partial / \partial x^{i}$ the element $G=G_{X}=\left(X^{1}, \ldots, X^{n}\right) \in M_{0}(n)$ and consider the initialvalue problem

$$
\begin{equation*}
\dot{\eta}=G \circ \eta, \quad \eta(0)=x \tag{5.3}
\end{equation*}
$$

$\operatorname{Exp}(X)$ is the time-one map of the formal flow of $X$, i.e. $\operatorname{Exp}(X)=\eta(1)$, where $\eta(t)$ is the unique solution of (5.3).

The existence and uniqueness of $\eta(t)$ is a consequence of Theorem 3.6. Indeed, first observe that the self-map $\xi \rightarrow G \circ \xi$ of $M_{0}(n)$ is Lipschitz, with Lipschitz constant at most $1 / 2$, provided $G(x+h)-G(x) \in F_{j+1}$ whenever $h \in F_{j}$. In analogy with the proof of Proposition 2.3 it suffices to establish this when $G$ is a monomial of the form $x^{\alpha} v, v \in K^{n}$, but since $X \in F_{1}(\operatorname{Vect}(n))$ we have $|\alpha| \geq 2$, and so in this case the assertion is obvious. As for $G \circ \xi$ being analytic whenever $\xi: K \rightarrow M_{0}(n)$ is such, simply write $X^{i}=\sum a_{\alpha}^{i} x^{\alpha}, \quad x=\left(x^{1}, \ldots, x^{n}\right), \quad \alpha=\left(\alpha_{1}, \ldots, \alpha_{n}\right)$. Then $\left(X^{i} \circ \xi(t)\right)=\sum a_{\alpha}^{i}(\xi(t))^{\alpha}$, which is a convergent series in the complete algebra of analytic functions from $K$ into $A(n)(\mathrm{cf} .(3.2 \mathrm{e}, \mathrm{f})$ ). Now observe that $\eta(t)$ is an analytic one-parameter group for the usual reason: for fixed $s \in K$ the functions $\eta(t+s)$ and $\eta(t) \circ \eta(s)$ satisfy the same initial-value problem. Thus $\eta(1)=\operatorname{Exp}(X) \in \operatorname{Diff}(n)$.

We remark that $\operatorname{Vect}(n)$ can be identified with $\operatorname{Der}(A)$ as elements of $\mathscr{L}$. Indeed, an element $X \in \operatorname{Vect}(n)$ acts as a derivation $D=D_{X}$ on $A=A(n)$ in the usual way, and since $X^{i}=D\left(x^{i}\right)$ the vector field is uniquely determined by this action. On the other hand, any $D \in \operatorname{Der}(A)$ preserves the filtration, so that $X^{i}=D\left(x^{i}\right) \in F_{1}(A)$ and $D=\Sigma X^{i} \partial / \partial x^{l}$.

### 5.4. Theorem. There is an "anti-isomorphism" of split exact sequences


where the groups on the left are the Campbell-Hausdorff groups and the center and right vertical arrows denote the anti-isomorphism given by the formal pull-back mapping $\varphi \rightarrow \varphi^{*}$. In particular, $\operatorname{Diff}(n)$ is the semidirect product of $\mathrm{Gl}\left(K^{n}\right)$ with $F_{1}(\operatorname{Vect}(n))$.

Remark. The definitions of the mappings in this diagram follow standard usage. However, this results in Exp being an anti-homomorphism.

The theorem is an immediate consequence of the following two propositions. Let $\operatorname{end}(A)$ act on $A^{n}$ diagonally: if $u \in \operatorname{end}(A)$ and $f=$ $\left(f^{1}, \ldots, f^{n}\right) \in A^{n}$, write $u \cdot f$ for $\left(u\left(f^{1}\right), \ldots, u\left(f^{n}\right)\right)$.
5.5. Proposition. The pull-back mapping $\varphi \rightarrow \varphi^{*}$ establishes an antiisomorphism between $M_{0}(n)$ and the semi-group of algebra endomorphisms of $A$; the mapping $u \rightarrow u \cdot x$ is a left inverse.

Proof. Simply note that if $\varphi \in M_{0}(n)$ then $\varphi^{*} \cdot x=\varphi$, and that when $u \in \operatorname{end}(A)$ then $(u \cdot x)^{*}\left(x^{i}\right)=u\left(x^{l}\right)$, so that $(u \cdot x)^{*}=u$ whenever $u$ is an algebra endomorphism.
5.6. Proposition. The unique solution $\eta(t)$ of (5.3) is given by $t \rightarrow \exp (t D) \cdot x$, where $D=D_{X}$.

Proof. We claim that $d^{k} \eta / d t^{k}=G_{k} \circ \eta$, where $G_{k}=D^{k} \cdot x$. Indeed, the chain-rule is valid in this context and gives

$$
\begin{aligned}
d^{k+1} \eta / d t^{k+1} & =d / d t\left(G_{k} \circ \eta\right)=\sum \eta^{i}(t)\left(\left(\partial G_{k} / \partial x^{i}\right) \circ \eta\right) \\
& =\sum\left(X^{i} \circ \eta\right)\left(\left(\partial G_{k} / \partial x^{l}\right) \circ \eta\right) \\
& =\sum\left(X^{i}\left(\partial G_{k} / \partial x^{i}\right)\right) \circ \eta=D \cdot G_{k} \circ \eta=G_{k+1} \circ \eta
\end{aligned}
$$

Now apply the Taylor formula, and observe that $G_{k} \circ \eta(0)=D^{k} \cdot x$.
5.7. Example If $\varphi, \rho \in \operatorname{Diff}(n)$ have respective polar decompositions $A \circ \operatorname{Exp}(X)$ and $B \circ \operatorname{Exp}(Y)$, then the group structure inherent in Theorem 5.4 immediately gives the polar decomposition of $\varphi \circ \rho$. Indeed, we have

$$
\begin{aligned}
\varphi \circ \rho & =A \circ \operatorname{Exp}(X) \circ B \circ \operatorname{Exp}(Y)=A \circ B \circ \operatorname{Exp}\left(B_{*} X\right) \circ \operatorname{Exp}(Y) \\
& =(A \circ B) \circ \operatorname{Exp}\left(Y *\left(B_{*} X\right)\right)
\end{aligned}
$$

In particular, if $\varphi=A \circ \operatorname{Exp}(X)$ is in normal form, i.e. if $A_{*} X=X$, then induction gives $\varphi^{n}=A^{n} \circ \operatorname{Exp}(n X)$.
6. Formal symplectic diffeomorphisms. Here we let $x=(q, p) \in K^{n}$ $\times K^{n}$ represent a pair of canonical variables in $2 n$-dimensional space. In this case the algebra $A=K[[x]]$ of $\S 5$ is also a complete graded Lie algebra under the formal Poisson bracket

$$
\{f, g\}=\sum\left(\left(\partial f / \partial q_{k}\right)\left(\partial g / \partial p_{k}\right)-\left(\partial f / \partial p_{k}\right)\left(\partial g / \partial q_{k}\right)\right)
$$

and when so viewed it will be convenient to relabel $A$ as $L=\Pi_{j} L_{j}$, where $L_{j}=A_{j+2}$ is the space of homogeneous polynomials of degree $j+2$. We will exploit this double algebra structure.

To begin notice that $\operatorname{end}(L)=\operatorname{end}(A)$, since "end" ignores the multiplicative structure. As a consequence $\operatorname{Der}(A), \operatorname{Der}(L), \operatorname{Aut}(A)$ and $\operatorname{Aut}(L)$ are all included in $\operatorname{end}(A)$. Secondly, if $l \in L$ then $\operatorname{ad}(l) \in \operatorname{Der}(L)$ is also a ring derivation of $A$. But then ad $\left.\right|_{F_{j}(L)}$ has values in $F_{j}(\operatorname{Der}(A))$ $\cap F_{j}(\operatorname{Der}(L))$, and as a result must be a filtered group homomorphism of the Campbell-Hausdorff group of $L$ into $\operatorname{Aut}(A) \cap \operatorname{Aut}(L)$.
6.1. Proposition. ad : $F_{1}(L) \rightarrow F_{1}(\operatorname{Der}(A)) \cap F_{1}(\operatorname{Der}(L))$ is an isomorphism.

Proof. For $\operatorname{ad}(l)=0$ we have $\left\{l, q_{j}\right\}=\left\{l, p_{j}\right\}=0$, hence all partial derivatives of $l$ must vanish, and therefore $l$ must be constant. But $l \in F_{1}(L)$ implies $l(0)=0$, so in fact $l=0$. Now let $D \in F_{1}(\operatorname{Der}(A)) \cap$ $F_{1}(\operatorname{Der}(L))$, and set $Q_{i}=D\left(q_{i}\right), P_{i}=D\left(p_{i}\right) ;$ note that $Q_{i}, P_{i} \in F_{2}(A)$. Applying $D$ to the canonical commutation relations $\left\{q_{i}, p_{j}\right\}=\delta_{i j}$, $\left\{q_{i}, q_{j}\right\}=\left\{p_{i}, p_{j}\right\}=0$ and using $D \in \operatorname{Der}(L)$ we then obtain

$$
\left\{Q_{i}, p_{j}\right\}+\left\{q_{i}, p_{j}\right\}=\left\{Q_{i}, q_{j}\right\}+\left\{q_{i}, Q_{j}\right\}=\left\{P_{i}, p_{j}\right\}+\left\{p_{i}, P_{j}\right\}=0
$$

hence $\partial P_{j} / \partial p_{i}=-\partial Q_{i} / \partial p_{j}, \partial Q_{i} / \partial p_{j}=\partial Q_{j} / \partial p_{i}$ and $\partial P_{i} / \partial q_{j}=\partial P_{j} / \partial q_{i}$. These equations hold for the homogeneous components of the $Q_{i}, P_{i}$, and as a result the one-form $\sum\left(P_{i} d q_{i}-Q_{i} d p_{i}\right)$ must be closed in the sense that all of the homogeneous components have this property. But then for each homogeneous component of degree $k \geq 2$ we can find a homogeneous polynomial of degree $k+1$, denoted by $l_{k-1}$ in accordance with our previous convention, such that for $l=l_{1}+\cdots$ we have

$$
d l=\sum\left(P_{i} d q_{i}-Q_{i} d p_{i}\right)
$$

But then $D=\operatorname{ad}(l)$ and $l \in F_{1}(L)$.
In Theorem 5.4 we found that $\operatorname{Diff}(2 n) \simeq \operatorname{Aut}(A)$. We now let $\operatorname{Can}(n)$ be the group of formal canonical transformations of $K^{2 n}$ fixing the origin: $\operatorname{Can}(n)=\left\{\varphi \in \operatorname{Diff}(2 n): \varphi^{*}\right.$ preserves Poisson brackets $\}=$ $\left\{\varphi \in \operatorname{Diff}(2 n): \varphi^{*} \in \operatorname{Aut}(L)\right\}$. We readily see that $\varphi \rightarrow \varphi^{*}$ is an anti-isomorphism between $\operatorname{Can}(n)$ and $\operatorname{Aut}(A) \cap \operatorname{Aut}(L)$.
6.2. Theorem. There is a split exact sequence of G-morphisms

$$
\begin{equation*}
0 \rightarrow F_{1}(L) \rightarrow \operatorname{Can}(n) \xrightarrow{\mathrm{Jac}} \mathrm{Sp}(n) \rightarrow e \tag{1}
\end{equation*}
$$

where $F_{1}(L)$ is the Campbell-Hausdorff group of $L$ and the map $F_{1}(L) \rightarrow$ $\operatorname{Can}(n)$ is given by $l \rightarrow \exp (\operatorname{ad}(l)) \cdot x$.

Proof. Apply Theorem 4.5 to $A$ twice: first as a ring and then as a Lie algebra. The result is an exact sequence $0 \rightarrow F_{1}(\operatorname{Der}(A)) \cap F_{1}(\operatorname{Der}(L)) \rightarrow$ $\operatorname{Aut}(A) \cap \operatorname{Aut}(L) \rightarrow \operatorname{Gl}\left(K^{n}\right) \cap \operatorname{Aut}_{0}(L) \rightarrow e$, and the terms are immediately identified with those of (1).

The meaning of Theorem 6.2 is that every formal canonical transformation $u$ of $K^{2 n}$ preserving the origin can be uniquely decomposed as a product $u_{0} \exp (\operatorname{ad} h)$, where $u_{0}=\operatorname{Jac}(u)$ is a symplectic linear map and $h$ is a formal hamiltonian vanishing to order three at 0 .

As an application of this polar decomposition we offer a quick proof of a theorem which, at least when $n=1$, is standard in the dynamical systems literature (compare [9, pp. 30-33]).
6.3. Example. Let $u \in \operatorname{Can}(n)$ be in normal form, i.e. $u u_{0}=u_{0} u$, where $u_{0}=\operatorname{Jac}(u)([9$, p. 31]). Then $u$ has an integral. Indeed, if $u=$ $u_{0} \exp (\operatorname{ad} h)$ then $\exp (\operatorname{ad} h)$ commutes with $u_{0}$. But then $\exp (\operatorname{ad} h)=$ $\exp (\operatorname{ad} h) u_{0} u_{0}^{-1}=u_{0} \exp (\operatorname{ad} h) u_{0}^{-1}=\exp \left(u_{0} \operatorname{ad} h u_{0}^{-1}\right)=\exp \left(\operatorname{ad}\left(u_{0} h\right)\right)$. Since expoad is injective, $u_{0} h=h$. But then $u h=h$ as $h$ is certainly invariant under its own flow.

## References

[1] N. Bourbaki, Commutative Algebra, Hermann, Paris, and Addison-Wesley, Reading, MA., 1973.
[2] C. Bouton, Bull. Amer. Math. Soc., 23 (1916), p. 73.
[3] A. Brjuno, The analytical form of differential equations, Trans. Moscow Math. Soc., 25 (1971), 131-288.
[4] H. Broer, Formal normal form theorems for vector fields and some consequences to bifurcations in the volume preserving case, in Dynamical Systems and Turbulence, Warwick, 1980 (D. A. Rand and L.-S. Young, Eds.), Springer Lecture Notes in Mathematics, Vol. 898, Springer-Verlag, New York, 1981.
[5] P. Dixon and J. Esterle, Michael's problem and the Poincaré-Fatou-Bieberbach phenomenon, Bull. Amer. Math. Soc., 15 (1986), 127-188.
[6] R. Gérard and A. H. M. Levelt, Sur les connexions a singularités régulières dans le cas de plusiers variables, Funcialaj Elevacioj, 19 (1976), 149-173.
[7] G. Hochschild, Basic Theory of Algebraic Groups and Lie Algebras, Springer-Verlag, New York, 1981.
[8] D. Lewis, On formal power series transformations, Duke J. Math., 5(1939), 794-803.
[9] J. Moser, Lectures on Hamiltonian systems, Mem. Amer. Math. Soc., No. 81, Amer. Math. Soc., Providence, RI., 1968.
[10] J. P. Serre, Lie Algebras and Lie Groups, W. A. Benjamin, New York, 1965.
[11] S. Sternberg, Infinite Lie groups and the formal aspects of dynamical systems, J. Math. Mech., 10 (1961), 451-474.
[12] F. Takens, Singularities of vector fields, In: Publ. Math. IHES, 43 (1974), 48-100.
[13] _, , Forced oscillations and bifurcations, in Applications of Global Analysis I, Comm. of the Math. Inst. Rijksuniversiteit Utrecht, 1974.
[14] J. van der Meer, The Hamiltonian Hopf Bifurcation, Springer Lecture Notes in Mathematics, Vol. 1160, Springer-Verlag, New York, 1985.

Received June 17, 1986 and in revised form November 6, 1986.
Hunter College
New York, NY 10021

