# THE EQUATION $x' \equiv xd - dx = b$

N. JACOBSON

Let $\mathfrak{A}$ be an associative algebra with a possibly infinite basis over a field $\Phi$. Then if $d$ is a fixed element in $\mathfrak{A}$, it is well known that the mapping $x \rightarrow x' \equiv [x, d] = xd - dx$ is a derivation[1] in $\mathfrak{A}$; that is,

$$(x + y)' = x' + y', \qquad (x\alpha)' = x'\alpha, \qquad (xy)' = x'y + xy'$$

for all $x$, $y$ in $\mathfrak{A}$ and all $\alpha$ in $\Phi$. The constants relative to such a derivation are the elements of $\mathfrak{A}$ that commute with $d$. We shall call an element $b$ a *d-integral* if $b = a'$ for some element $a$ in $\mathfrak{A}$, that is, if the equation $x' = xd - dx = b$ has a solution in $\mathfrak{A}$. Clearly if $a$ is a solution of this equation then the totality of solutions is the set $\{a + c\}$ where $c$ ranges over the set of $d$-constants. In a recent paper appearing in this Bulletin, R. E. Johnson obtained a necessary and sufficient condition that an element $b$ be a $d$-integral under the assumption that $\mathfrak{A}$ is a separable algebraic division ring.[2] In this note we allow $\mathfrak{A}$ to be an arbitrary algebra but we make the assumption that $d$ is an algebraic element in the sense that it satisfies a polynomial equation with coefficients in $\Phi$. We obtain a necessary condition, which is equivalent to Johnson's condition when $\mathfrak{A}$ is a division ring, that $b$ be a $d$-integral. If the minimum polynomial $\mu(\lambda)$ of $d$ is relatively prime to its derivative $\mu'(\lambda)$, then it is easy to see that the condition is also sufficient and one may give an explicit formula for a solution of the equation $x' = b$. If we assume that $\mathfrak{A}$ is a simple algebra satisfying the descending chain condition for left ideals then we can show that our condition is also sufficient when $\mu(\lambda)$ is a product of distinct irreducible factors in $\Phi[\lambda]$ and in certain other cases. Here, however, we do not display a solution but merely prove its existence. Our results include, of course, Johnson's result for algebraic division rings, since the minimum polynomial of an element in such a ring is irreducible. No assumption about separability is required.

In order to obtain a condition for the solvability of the equation $x' = b$ we consider the matrices

$$u = \begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix}, \qquad v = \begin{pmatrix} d & b \\ 0 & d \end{pmatrix} \tag{1}$$

Received by the editors May 19, 1944.

[1] Cf. the author's paper *Abstract derivation and Lie algebras*, Trans. Amer. Math. Soc. vol. 42 (1937) pp. 206–224.

[2] *On the equation* $\chi\alpha = \gamma\chi + \beta$ *over an algebraic division ring*, Bull. Amer. Math. Soc. vol. 50 (1944) pp. 202–208.

in the matrix algebra $\mathfrak{A}_2$ of two-rowed matrices with elements in $\mathfrak{A}$. If $x$ is any element in $\mathfrak{A}$

$$\begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^{-1}$$

and the equation $x' = xd - dx = b$ is equivalent to the matrix equation

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} d & b \\ 0 & d \end{pmatrix}. \tag{2}$$

Thus if $b$ is a $d$-integral the matrices (1) are similar in $\mathfrak{A}_2$. We suppose now that $d$ is an algebraic element and let

$$\phi(\lambda) = \lambda^m + \alpha_1\lambda^{m-1} + \cdots \tag{3}$$

be the minimum polynomial of $d$ over $\Phi$. Then it is clear that $\phi(u) = 0$. Hence a necessary condition that $b$ be a $d$-integral is that $\phi(v) = 0$. Now

$$v^r = \begin{pmatrix} d^r & B_r \\ 0 & d^r \end{pmatrix}$$

where $B_r = \sum_{k=0}^{r-1} d^k b d^{r-k-1}$. Hence the condition that $\phi(v) = 0$ is that

$$B_m + \alpha_1 B_{m-1} + \cdots + \alpha_{m-1}B_1 = 0. \tag{4}$$

As we have shown elsewhere[3]

$$B_r = C_{r,1}d^{r-1}b + C_{r,2}d^{r-2}b' + \cdots + b^{(r-1)}$$

where $b^{(k)} = (b^{(k-1)})'$. Hence if we define

$$\phi_h(\lambda) = C_{m,h}\lambda^{m-h} + C_{m-1,h}\alpha_1\lambda^{m-h-1} + \cdots \equiv \phi^{(h)}(\lambda)/h!$$

we may write (4) in the more useful form

$$\phi_1(d)b + \phi_2(d)b' + \cdots + \phi_m(d)b^{(m-1)} = 0. \tag{5}$$

We suppose now that $\phi_1(\lambda) \equiv \phi'(\lambda)$ is relatively prime to $\phi(\lambda)$.[4] Then $\phi_1(d)$ is a regular element in $\mathfrak{A}$. Hence if $b$ is an element such that (5) holds,

$$b = -\phi_1(d)^{-1}\phi_2(d)b' - \cdots - \phi_1(d)^{-1}\phi_m(d)b^{(m-1)} = x'$$

where

$$x = -\phi_1(d)^{-1}\phi_2(d)b - \cdots - \phi_1(d)^{-1}\phi_m(d)b^{(m-2)}. \tag{6}$$

---

[3] Loc. cit. footnote 1, p. 209.

[4] This condition will be satisfied if $d$ generates a separable algebraic field over $\Phi$.

This proves the following theorem.

THEOREM 1. *Let $\mathfrak{A}$ be an arbitrary algebra and let d be an algebraic element of $\mathfrak{A}$ having a minimum polynomial $\phi(\lambda)$ relatively prime to its derivative. Then* (5) *is a necessary and sufficient condition in order that the element b be a d-integral. When the condition holds, $b=x'$ where x is given by* (6).

We suppose now that $\mathfrak{A}$ is a simple algebra with an identity satisfying the descending chain condition for left (right) ideals. Then $\mathfrak{A}=\mathfrak{D}_h$, a matrix algebra of $h$ rows over the (not necessarily finite) division algebra $\mathfrak{D}$ and conversely any algebra of this form satisfies our condition. As before let $d$ be an algebraic element of $\mathfrak{A}$ and let $\phi(\lambda)$ be its minimum polynomial. Let $b$ be an element of $\mathfrak{A}$ such that (5) holds. Then (4) holds and hence the minimum polynomial of $v$ as well as of $u$ is $\phi(\lambda)$. Since $d, b\in\mathfrak{A}=\mathfrak{D}_h$ the matrices $u$ and $v\in\mathfrak{D}_{2h}$ and these may be regarded as the matrices of linear transformations in a $2h$-dimensional vector space $\mathfrak{R}$ over $\mathfrak{D}$. Let $T$ be the linear transformation corresponding to $v$. Then according to the form of $v$ we have an $h$-dimensional subspace $\mathfrak{S}$ of $\mathfrak{R}$ invariant under $T$ such that the matrix of $T$ in $\mathfrak{S}$ is $d$ and the matrix of $T$ in the difference space $\mathfrak{R}-\mathfrak{S}$ is also $d$.

We suppose now that $\phi(\lambda)$ is a product of irreducible factors in $\Phi[\lambda]$. In this case the linear transformation is completely reducible.[5] Hence there exists a subspace $\mathfrak{S}'$ invariant under $T$ such that $\mathfrak{R}=\mathfrak{S}+\mathfrak{S}'$, $\mathfrak{S}\cap\mathfrak{S}'=0$ and such that the matrix of $T$ in $\mathfrak{S}'$ is also $d$. Let $x_1, \cdots, x_h, x_{h+1}, \cdots, x_{2h}$ be the original basis of $\mathfrak{R}$ relative to which $T$ has the matrix $v$ so that $x_1, \cdots, x_h$ is a basis for $\mathfrak{S}$. Corresponding to the decomposition $\mathfrak{R}=\mathfrak{S}+\mathfrak{S}'$ we have the basis $x_1, \cdots, x_h, x'_{h+1}, \cdots, x'_{2h}$. The matrix relating this basis to the original one has the form

$$\begin{pmatrix} 1 & p \\ 0 & q \end{pmatrix},$$

where $p, q\in\mathfrak{D}_h$ and the matrix of $T$ relative to the basis $x_1, \cdots, x_h, x'_{h+1}, \cdots, x'_{2h}$ is $u$. Hence we have the equation

$$\begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} 1 & p \\ 0 & q \end{pmatrix}^{-1}\begin{pmatrix} d & b \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & p \\ 0 & q \end{pmatrix}.$$

This implies that $dq=qd$ and that $bq=pd-dp$. Since the matrix

[5] See the author's paper *Pseudo-linear transformations*, Ann. of Math. vol. 38 (1937) p. 498.

$$\begin{pmatrix} 1 & p \\ 0 & q \end{pmatrix}$$

is regular, $q$ is regular and hence we have the relation $b = xd - dx$ where $x = pq^{-1}$.

THEOREM 2. *Let $\mathfrak{A} = \mathfrak{D}_h$ where $\mathfrak{D}$ is a division algebra over $\Phi$ and let $d$ be an algebraic element of $\mathfrak{A}$. Then if the minimum polynomial $\phi(\lambda)$ of $d$ is a product of distinct irreducible factors in $\Phi[\lambda]$, the condition* (5) *is necessary and sufficient in order that the element $b$ of $\mathfrak{A}$ be a $d$-integral.*

We next let $\mathfrak{A} = \Phi_h$, the matrix algebra of $h$ rows over $\Phi$. Let $d$ be a non-derogatory matrix in $\Phi_h$. Thus $d$ has only one invariant factor $\phi(\lambda) \neq 1$ and $\phi(\lambda)$ is the minimum polynomial of $d$. Let $b$ be a matrix such that (5) holds and consider the matrix $v$ as before. The minimum polynomial of $v$ is $\phi(\lambda)$. If $T$ is the linear transformation in the $2h$-dimensional space over $\Phi$ associated with the matrix $v$ then $\mathfrak{R}$ contains an invariant subspace $\mathfrak{S}$ whose matrix is $d$. Since $d$ is non-derogatory, $\mathfrak{S}$ is a cyclic subspace and its order is the minimum polynomial of $T$ in $\mathfrak{R}$. Now it is known that this implies that $\mathfrak{R} = \mathfrak{S} + \mathfrak{S}'$, $\mathfrak{S} \cap \mathfrak{S}' = 0$ where $\mathfrak{S}'$ is also invariant relative to $T$.[6] A repetition of the argument used to prove Theorem 2 will now yield the following theorem.

THEOREM 3. *Let $d$ be a non-derogatory matrix in the matrix algebra $\Phi_h$ and let $\phi(\lambda)$ be its minimum polynomial. Then the condition* (5) *is necessary and sufficient that the matrix $b$ be a $d$-integral.*

We give finally an example in which the condition (5) is not sufficient to insure that an element be a $d$-integral. Let

$$d = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad b = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then the minimum polynomial of $d$ is $\phi(\lambda) = \lambda^2$. Since $bd = db = 0$, $b$ satisfies (5). On the other hand, the invariant factors of the matrices $u$ and $v$ here are respectively $\lambda^2, \lambda^2, \lambda, \lambda$ and $\lambda^2, \lambda^2, \lambda^2$. It follows that these matrices are not similar and hence $b$ is not a $d$-integral.

THE JOHNS HOPKINS UNIVERSITY

[6] See van der Waerden's *Moderne Algebra*, vol. 2, pp. 129–130. The proof given there of this theorem for ordinary finite groups is also valid for vector spaces relative to a single linear transformation.