PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 34, Number 1, July 1972

# AN EISENSTEIN CRITERION FOR NONCOMMUTATIVE POLYNOMIALS

J. KOVACIC[1]

ABSTRACT. An analogue of the Eisenstein irreducibility criterion is developed for linear differential operators, or, more generally, noncommutative polynomials, and is applied to a few simple examples.

**Introduction.** The question of the irreducibility of an ordinary linear differential operator is of interest in the Picard-Vessiot theory (see Kolchin [1, §22]). Indeed, the operator is irreducible if and only if the Galois group is linearly irreducible. In this note we develop an "Eisenstein criterion" to help answer this question.

Because a linear differential operator is a special type of noncommutative polynomial, it is more natural to phrase the result in this more general context. The result, and indeed the proof with only slight changes in notation, is valid for partial differential operators, or more generally, noncommutative polynomials in several variables. Because the hypothesis that the ring be principal is unnatural in this setting, and because the reader may make the necessary changes if he so desires, we confine our attention to the ordinary case.

1. **The irreducibility criterion.** By a differential ring $\mathscr{R}$ we shall mean a ring (associative, commutative, with unit) together with two commuting operators $\sigma$ and $\delta$ such that $\sigma$ is an automorphism of $\mathscr{R}$, $\delta$ is additive, and $\delta(ab)=\sigma a\cdot\delta b+\delta a\cdot b$ for every $a$, $b$ in $\mathscr{R}$. $\mathscr{R}[\delta]$ will denote the noncommutative ring of differential operators with coefficients in $\mathscr{R}$, so that $\mathscr{R}[\delta]$ is the set of $\sum_{i=0}^{n} a_i\delta^i$, with $a_i\in\mathscr{R}$, $n\in N$, and right multiplication is defined by $\delta\cdot a=\sigma a\cdot\delta+\delta a$.

Evidently if $\sigma=\mathrm{id}$, then $\mathscr{R}$ is an ordinary differential ring with derivation operator $\delta$. By a differential ideal of $\mathscr{R}$ we mean an ideal which is closed under the two operators $\sigma$ and $\delta$. The smallest differential ideal which contains the set $\Sigma\subset\mathscr{R}$ is denoted by $[\Sigma]$.

Received by the editors October 7, 1971.

*AMS* 1970 *subject classifications*. Primary 12H05, 12E05; Secondary 13B25, 16A02.

*Key words and phrases*. Eisenstein criterion, irreducibility criterion, noncommutative polynomials, differential rings, differential operator.

[1] Supported by NSF grant GP-28242.

Let $\mathscr{R}$ be a differential principal integral domain and let $L \in \mathscr{R}[\delta]$. It is apparent that $L$ is primitive over $\mathscr{R}$ if and only if the ideal generated by the coefficients of $L$ is $\mathscr{R}$. Analogously, we make the following definition.

DEFINITION. Let $\mathscr{R}$ be a differential principal integral domain and let $L \in \mathscr{R}[\delta]$. $L$ is said to be *differentially primitive* over $\mathscr{R}$ if the differential ideal generated by the coefficients of $L$ is $\mathscr{R}$.

For any $L \in \mathscr{R}[\delta]$, there exist $c_L \in \mathscr{R}$ and $L^* \in \mathscr{R}[\delta]$ with $L = c_L L^*$ such that $L^*$ is primitive over $\mathscr{R}$. Evidently $c_L$ and $L^*$ are unique up to multiplication on the left by a unit in $\mathscr{R}$.

PROPOSITION 1. *Let $\mathscr{R}$ be a differential ring and $\mathfrak{p}$ a prime differential ideal in $\mathscr{R}$. Assume that the local ring $\mathscr{R}_{\mathfrak{p}}$ is a principal integral domain. If $L \in \mathscr{R}_{\mathfrak{p}}[\delta]$ is differentially primitive over $\mathscr{R}_{\mathfrak{p}}$, then $L$ is primitive over $\mathscr{R}_{\mathfrak{p}}$.*

PROOF. Let $L = c_L L^*$, with $c_L \in \mathscr{R}_{\mathfrak{p}}$ and $L^*$ primitive over $\mathscr{R}_{\mathfrak{p}}$. If $c_L \notin \mathfrak{p}\mathscr{R}_{\mathfrak{p}}$, then $c_L$ is a unit in $\mathscr{R}_{\mathfrak{p}}$ and hence $L$ is primitive over $\mathscr{R}_{\mathfrak{p}}$. However, if $c_L \in \mathfrak{p}\mathscr{R}_{\mathfrak{p}}$ then the differential ideal generated by the coefficients of $L = c_L L^*$ is contained in $[c_L] \subset \mathfrak{p}\mathscr{R}_{\mathfrak{p}}$, which contradicts the assumption that $L$ is differentially primitive over $\mathscr{R}_{\mathfrak{p}}$. This proves the proposition.

In general, however, a differential operator may be differentially primitive without being primitive. As an example, consider the differential ring $\mathscr{C}[x]$, where $\sigma = \mathrm{id}$, $\mathscr{C}$ is a field of constants and $\delta x = 1$. Then $L = x\delta^2 + x^2\delta - x$ is differentially primitive but not primitive over $\mathscr{C}[x]$. Moreover, we find that the Gauss Lemma does not hold, since $x\delta^2 + x^2\delta - x = (\delta + x)(x\delta - 1)$, both factors of which are primitive over $\mathscr{C}[x]$. We do however have the following proposition.

PROPOSITION 2. *Let $\mathscr{R}$ be a differential principal integral domain with the property that every proper differential ideal is contained in a prime differential ideal. Let $M$, $N \in \mathscr{R}[\delta]$ be differentially primitive over $\mathscr{R}$. Then $L = MN$ is differentially primitive over $\mathscr{R}$.*

REMARK. The condition on $\mathscr{R}$ is automatically satisfied in the case that $\sigma = \mathrm{id}$ and $\mathscr{R}$ contains the field of rational numbers.

PROOF. Let $M = \sum_{i=0}^{m} a_i \delta^i$, $N = \sum_{j=0}^{n} b_j \delta^j$. Then

$$L = \sum_{i=0}^{m} \sum_{j=0}^{n} \sum_{k=0}^{i} \binom{i}{k} a_i \sigma^k \delta^{i-k} b_j \delta^{j+k} = \sum_{l=0}^{m+n} c_l \delta^l.$$

We assume that $L$ is not differentially primitive and force a contradiction. Let $\mathfrak{p}$ be a prime differential ideal of $\mathscr{R}$ which contains the coefficients $c_0, \cdots, c_{m+n}$ of $L$. Since $M$ and $N$ are differentially primitive, there exist maximal indices $r$, $s$ $(0 \leqq r \leqq m, 0 \leqq s \leqq n)$ with $a_r \notin \mathfrak{p}$ and $b_s \notin \mathfrak{p}$. We observe that

$$c_{r+s} = \sum_{i>r}\ \sum_{j+k=r+s}\binom{i}{k}a_i\sigma^k\delta^{i-k}b_j + \sum_{i\leqq r}\ \sum_{j+k=r+s}\binom{i}{k}a_i\sigma^k\delta^{i-k}b_j.$$

In the second summation $r+s=j+k\leqq j+i\leqq j+r$, so that $s\leqq j$ and equality holds only if $i=k=r$. Thus $0\equiv a_r\sigma^r b_s \pmod{\mathfrak{p}}$. Since $\mathfrak{p}$ is prime and $a_r\notin\mathfrak{p}$, $\sigma^r b_s\in\mathfrak{p}$, and therefore $b_s\in\mathfrak{p}$. This contradiction proves the proposition.

We now wish to compare factorization of a differential operator over a differential integral domain $\mathscr{R}$ and its quotient field $\mathscr{F}$. Because the Gauss Lemma is not valid, we cannot assert that an operator in $\mathscr{R}[\delta]$ which factors over $\mathscr{F}$ factors over $\mathscr{R}$; indeed, if $\mathscr{R}=\mathscr{C}[x]$, where $\sigma=\mathrm{id}$, $\mathscr{C}$ is a field of constants and $\delta x=1$, then $\delta^2+x\delta-1=(x^{-1}\delta+1)(x\delta-1)$ has no factorization over $\mathscr{R}$.

PROPOSITION 3. *Let $\mathscr{R}$ be a differential principal integral domain and let $\mathscr{F}$ be its quotient field. Let $L\in\mathscr{R}[\delta]$ be an operator which is reducible over $\mathscr{F}$. Then there exist elements $p$, $q$ of $\mathscr{R}$, with $pq\neq 0$, such that $qL=pMN$, where $M$ and $N$ are in $\mathscr{R}[\delta]$ and are primitive over $\mathscr{R}$.*

PROOF. Let $L=M'N'$, with $M'$, $N'\in\mathscr{F}[\delta]$. Say $M'=\sum_{i=0}^{m}a_i\delta^i$. Choose $f\in\mathscr{F}$ such that $N=fN'$ is in $\mathscr{R}[\delta]$ and is primitive over $\mathscr{R}$. Choose $p$, $q\in\mathscr{R}$, $pq\neq 0$, such that

$$M = \frac{q}{p}\sum_{k=0}^{m}\ \sum_{i=k}^{m}\binom{i}{k}a_i\sigma^k\delta^{i-k}\frac{1}{f}\,\delta^k$$

is in $\mathscr{R}[\delta]$ and is primitive over $\mathscr{R}$. Then an easy computation shows that $pMN=qL$.

COROLLARY. *Let $\mathscr{R}$ be a differential integral domain with quotient field $\mathscr{F}$. Let $\mathfrak{p}$ be a prime differential ideal of $\mathscr{R}$. Assume that the local ring $\mathscr{R}_{\mathfrak{p}}$ is principal. If $L\in\mathscr{R}_{\mathfrak{p}}[\delta]$ is reducible over $\mathscr{F}$, then $L$ is reducible over $\mathscr{R}_{\mathfrak{p}}$.*

PROOF. Suppose that $L$ is reducible over $\mathscr{F}$. By the proposition, there exist $p$, $q\in\mathscr{R}_{\mathfrak{p}}$, $pq\neq 0$, $M$, $N\in\mathscr{R}_{\mathfrak{p}}[\delta]$, primitive over $\mathscr{R}_{\mathfrak{p}}$ such that $qL=pMN$. Let $L=c_L L^*$, where $L^*$ is primitive over $\mathscr{R}_{\mathfrak{p}}$. Because every proper differential ideal of $\mathscr{R}_{\mathfrak{p}}$ is contained in $\mathfrak{p}\mathscr{R}_{\mathfrak{p}}$, which is a prime differential ideal, Proposition 2 implies that $MN$ is differentially primitive. Whence, by Proposition 1, $MN$ is primitive over $\mathscr{R}_{\mathfrak{p}}$, so there exists a unit $u\in\mathscr{R}_{\mathfrak{p}}$ such that $p=qc_Lu$. We have $L=q^{-1}pMN=(c_LuM)N$. This proves the corollary.

THEOREM. *Let $\mathscr{R}$ be a differential integral domain with quotient field $\mathscr{F}$, and let $\mathfrak{p}$ be a prime differential ideal in $\mathscr{R}$. Assume that the local ring $\mathscr{R}_{\mathfrak{p}}$ is* *principal. Let $L=\sum_{i=0}^{l} c_i\delta^i \in \mathscr{R}[\delta]$ be such that $c_i \in \mathfrak{p}$ for $i=1,\cdots,l$, $c_0 \notin \mathfrak{p}$ and $c_l \notin \mathfrak{p}^2$. Then $L$ is irreducible over $\mathscr{F}$.*

PROOF. We suppose that $L$ is reducible over $\mathscr{F}$ and force a contradiction. By the preceding corollary, we may assume that $L=MN$, where $M$, $N \in \mathscr{R}_{\mathfrak{p}}[\delta]$. Let $M=\sum_{i=0}^{m} a_i\delta^i$, $N=\sum_{i=0}^{n} b_i\delta^i$ $(m>0, n>0)$. Then $l=m+n$,

$$L=\sum_{i=0}^{m}\sum_{j=0}^{n}\sum_{k=0}^{i}\binom{i}{k}a_i\sigma^k\delta^{i-k}b_j\delta^{j+k},$$

and $c_{m+n}=a_m\sigma^m b_n$.

*Case* 1. $a_m \in \mathfrak{p}\mathscr{R}_{\mathfrak{p}}$, $\sigma^m b_n \notin \mathfrak{p}\mathscr{R}_{\mathfrak{p}}$. Let $r$ $(0\leqq r\leqq m)$ be the minimal index such that $a_i \in \mathfrak{p}\mathscr{R}_{\mathfrak{p}}$ for every $i\geqq r$. Since $c_0=\sum_{i=0}^{m} a_i\delta^i b_0$ is not in $\mathfrak{p}$, we have that $r>0$. Thus $c_{n+r-1} \in \mathfrak{p}$. However,

$$c_{n+r-1}=\sum_{i=0}^{m}\sum_{j+k=n+r-1}\binom{i}{k}a_i\sigma^k\delta^{i-k}b_j.$$

Since $n+r-1=j+k\leqq j+i\leqq n+i$, we have $i\geqq r-1$ and equality holds only if $j=n$ and $k=i$. Hence $0\equiv a_{r-1}\sigma^{r-1}b_n \pmod{\mathfrak{p}\mathscr{R}_{\mathfrak{p}}}$, so that $\sigma^{r-1}b_n$ and therefore $\sigma^m b_n$ is in $\mathfrak{p}\mathscr{R}_{\mathfrak{p}}$. This contradiction proves the theorem in Case 1.

*Case* 2. $a_m \notin \mathfrak{p}\mathscr{R}_{\mathfrak{p}}$, $\sigma^m b_n \in \mathfrak{p}\mathscr{R}_{\mathfrak{p}}$. Let $s$ $(0\leqq s\leqq n)$ be the minimal index such that $\sigma^m b_j \in \mathfrak{p}\mathscr{R}_{\mathfrak{p}}$ for every $j\geqq s$. Since $\sigma^m c_0=\sum_{i=0}^{m}\sigma^m a_i\sigma^m\delta^i b_0$ is not in $\mathfrak{p}$, $s$ is bigger than zero. Thus $c_{m+s-1}\in\mathfrak{p}$. However

$$c_{m+s-1}=\sum_{i=0}^{m}\sum_{j+k=m+s-1}\binom{i}{k}a_i\sigma^k\delta^{i-k}b_j.$$

Since $m+s-1=j+k\leqq j+i\leqq j+m$, we have $j\geqq s-1$ and equality holds only if $k=i=m$. Hence $0\equiv a_m\sigma^m b_{s-1} \pmod{\mathfrak{p}\mathscr{R}_{\mathfrak{p}}}$. This contradicts the assumption that $a_m\notin\mathfrak{p}\mathscr{R}_{\mathfrak{p}}$ and proves the theorem.

2. **Examples.** Throughout this section $\sigma=\text{id}$, $\mathscr{C}$ is a field of constants and $x$ is such that $\delta x=1$.

PROPOSITION 4. *Let $L=\delta^2+P$, where $P\in\mathscr{C}[x]$ is of odd degree. Then $L$ is irreducible over $\mathscr{C}(x)$.*

PROOF. Let the degree of $P$ be $2k+1$. Define a new derivation operator $\delta'$ on $\mathscr{C}(x)$ by the formula $\delta' x=x^{-k}\delta$. Let $\mathscr{R}=\mathscr{C}[x^{-1}]$ and $\mathfrak{p}=(x^{-1})$. Because $\delta'(x^{-1})=-x^{-(k+2)}$, $\mathscr{R}$ is a differential ring and $\mathfrak{p}$ is a prime differential ideal with respect to $\delta'$. Evidently $L$ is irreducible over $\mathscr{C}(x)$ if and only if $L'=x^{-(2k+1)}L=x^{-1}(\delta')^2+kx^{-(k+2)}\delta'+x^{-(2k+1)}P$ is irreducible over the quotient field of $\mathscr{R}$. The conditions of the theorem are clearly satisfied, therefore $L'$ is irreducible over the quotient field of $\mathscr{R}$. This proves the proposition.

PROPOSITION 5. *Let $L=x^n\delta^2+P$, where $P\in\mathscr{C}[x]$ has degree $n-1$. Then $L$ is irreducible over $\mathscr{C}(x)$.*

PROOF. The proof is similar to that of Proposition 4 with $\delta'=x\delta$, $\mathscr{R}=\mathscr{C}[x^{-1}]$, $\mathfrak{p}=(x^{-1})$ and $L'=x^{-(n-1)}L$.

PROPOSITION 6. *Let $L=x^n\delta^2+P$, where $P\in\mathscr{C}[x]$. Assume that $n$ is odd and is greater than or equal to 3, and that $P(0)\neq0$. Then $L$ is irreducible over $\mathscr{C}(x)$.*

PROOF. The proof is similar to that of Proposition 4, with $\delta'=x^{(n-1)/2}\delta$, $\mathscr{R}=\mathscr{C}[x]$, $\mathfrak{p}=(x)$, and $L'=L$.

## REFERENCE

1. E. R. Kolchin, *Algebraic matric groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations*, Ann. of Math. (2) **49** (1948), 1-42. MR **9**, 561.

DEPARTMENT OF MATHEMATICS, FORDHAM UNIVERSITY, NEW YORK, NEW YORK 10458