Commun. Korean Math. Soc. **23** (2008), No. 4, pp. 499–509

# SOME REMARKS ON EISENSTEIN'S CRITERION

Sung Sik Woo

Abstract. In [4] we showed that a polynomial over a Noetherian ring is divisible by some other polynomial by looking at the matrix formed by the coefficients of the polynomials which we called the resultant matrix. Using the result, we will find conditions for a polynomial over a commutative ring to be irreducible. This can be viewed as a generalization of the Eisenstein's irreducibility criterion.

## 1. Introduction

Let $A$ be a commutative Noetherian ring with 1. Given two polynomials $f, g \in A[X]$ we showed exactly when $g$ divides $f$ by using the matrix $R(f, g)$ formed by the coefficients of $f$ and $g$ [4]. The polynomial $f$ will be irreducible when there is no such polynomial $g$ of degree $\geq 1$ which divides $f$. We will show that Eisenstein's irreducibility criterion can be deduced from our result and we will show how Eisenstein's criterion can be generalized in this method.

In Section 2, we recall the notion of resultant matrix and Fitting invariant. And we deduce an immediate corollary of Fitting's Lemma and recall the main result of [4]. In Section 3, we show how Eisenstein's criterion can be deduced from our result and then we generalize Eisenstein criterion by using the resultant matrix $R(f, g)$ in Section 4.

All rings are commutative with the identity 1.

## 2. Resultant and Fitting invariant

In this section we recall the result of [4] which we will use later. We adapted the notion of resultant from Ch.IV Sec. 6 of [1] for our purpose. To fix our notations let $A$ be a commutative ring and $F_1$, $F_2$ be $A$-free modules with bases $\beta = \{v_1, v_2, \ldots, v_n\}$ and $\gamma = \{w_1, w_2, \ldots, w_m\}$ of $F_1$ and $F_2$ respectively. Let $\phi : F_1 \to F_2$ be an $A$-linear map. Then the matrix $X = (x_{ij}) \in M(n \times m, A)$ of $\phi$ with respect to the bases $\beta$ and $\gamma$ is defined by the equality

$$\phi(v_i) = \sum_{j=1}^{m} x_{ij} w_j \ (i = 1, 2, \ldots, n).$$

Received May 26, 2008; Revised September 2, 2008.

2000 *Mathematics Subject Classification.* 13B25, 11R09, 11C20.

*Key words and phrases.* irreducibile polynomial over a commutative ring.

Here we denote the matrices of size $n\times m$ with coefficients in $A$ by $M(n\times m, A)$. If $\psi : F_2 \to F_3$ is another $A$-linear map of free modules with matrix $Y$, then the matrix corresponding to $\psi\circ\phi$ will be $XY$. Let $A$ be a commutative ring. For positive integers $n, m$ let $f, g \in A[X]$ be the polynomials

$$\begin{aligned} f(X) &= a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \\ g(X) &= b_mX^m + b_{m-1}X^{m-1} + \cdots + b_0. \end{aligned}$$

Let $S_n$ be the $A$-submodule of $A[X]$ consisting of polynomials of degree $< n$. Choose bases $B_1$ (resp. $B_2$) of $S_m \times S_n$ (resp. $S_{n+m}$ ) by

$$\begin{aligned} B_1 &= \{(X^{m-1}, 0), \dots, (X, 0), (1, 0), (0, X^{n-1}), \dots, (0, X), (0, 1)\} \\ B_2 &= \{X^{n+m-1}, \dots, X, 1\}. \end{aligned}$$

Define an $A$-linear map $\phi : S_n \times S_m \to S_{n+m}$ by

$$\phi(u, v) = uf + vg.$$

Let us denote $R(f, g)$ the matrix of $\phi$ with respect to $B_1$ and $B_2$,

$$R(f,g) = \begin{pmatrix} a_n & a_{n-1} & \cdots & 0 & a_0 & 0 & \cdots & 0 \\ 0 & a_n & a_{n-1} & \cdots & a_1 & a_0 & \cdots & 0 \\ \dots & \dots & \ddots & \dots & \dots & \dots & \dots & 0 \\ 0 & \cdots & 0 & a_n & a_{n-1} & \cdots & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_1 & b_0 & 0 & 0 & 0 \\ 0 & b_m & b_{m-1} & \cdots & b_1 & b_0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \cdots & \cdots & b_m & b_{m-1} & \cdots & \cdots & b_0 \end{pmatrix}.$$

The matrix $R(f, g)$ will be called the *resultant matrix* and the determinant of the resultant matrix $R(f, g)$ is called the *resultant* $\operatorname{res}(f, g)$ of $f$ and $g$.

Next we recall the notion of Fitting invariant [3, Ch. 20] and obtain an immediate corollary for future use.

**Definition 2.1.** Let $F$ and $G$ be free modules over a commutative ring $A$ and let $\phi : F \to G$ be an $A$-linear map. Then we define $I_j\phi$ be the image of the map

$$\wedge^j F \otimes \wedge^j G^* \to A.$$

When $\phi$ is expressed as a matrix with respect to some bases for $F$ and $G$ then $I_j(\phi)$ is the ideal generated by all minors of size $j$. By convention we define $I_0\phi = A$.

Note that we have a chain of ideals

$$A = I_0\phi \supseteq I_1\phi \supseteq I_2\phi \supseteq \cdots \supseteq I_r$$

because a minor of size $j$ is a linear combination of minors of size $(j-1)$.

Let $M$ be a finitely generated $A$-module and let

$$F \xrightarrow{\phi} G \to M \to 0$$

$$F' \xrightarrow{\phi'} G' \to M \to 0$$

be two free presentations of $M$ with $G, G'$ free of rank $r, r'$ respectively. Then Fitting's Lemma asserts that

**Lemma 2.2** (Fitting's Lemma [3, Ch. 20.2])**.** *$I_{r-i}\phi = I_{r'-i}\phi'$.*

Using the independence on presentations of $M$ we can define:

**Definition 2.3.** We define the *i-th Fitting invariant* of $M$ to be the ideal

$$\mathrm{Fitt}_i(M) = I_{r-i},$$

where $I_{r-i}$ is the common value $I_{r-i}\phi = I_{r'-i}\phi'$ in Fitting's Lemma.

For convenience we will also write $\mathrm{Fitt}_i(\phi)$ for $\mathrm{Fitt}_i(M)$ when $\phi$ is a linear map or a matrix giving the cokernel $M$. We get a corollary to Fitting's Lemma [4, Corollary 3.4].

**Corollary 2.4.** *Let $A$ be a commutative ring and let $X \in M(n \times m, A)$, $Y \in M(m, A)$ and $Z \in M(n, A)$. If $Y, Z$ are invertible matrices, then* $\mathrm{Fitt}_i(X)$ $= \mathrm{Fitt}_i(YX)= \mathrm{Fitt}_i(XZ)$. □

Now we state a main result of [4, Theorem 4.4] in the form we will use.

**Theorem 2.5.** *Let $A$ be a Noetherian commutative ring and $f, g \in A[X]$ be monic polynomials of degree $n$ and $m$ respectively with $n > m$. Then $g(X)$ divides $f(X)$ if and only if the condition*

(R) *the minors of $R(f, g)$ of size bigger than $n$ vanishes*

*satisfies*

*Remark.* In (iv), of [4, Theorem 4.4] the condition "the minors of $R(f, g)$ of size $n$ generate the unit ideal" is redundant since the $n \times n$ matrix in the low left corner of $R(f, g)$ has determinant $b_m^n$ and we assumed $f$ and $g$ to be monic. Also monic polynomials can be replaced by the polynomials with a unit leading coefficients.

## 3. Irreducibility of polynomials

We first carefully define our terms to make things clear. An element $a$ in a ring $A$ is said to be *irreducible* if $a = bc$, then either $b$ or $c$ is a unit. It is well known that a polynomial $f(X) = \sum_{i=0}^{n} a_i X^i$ is a unit if and only if $a_0$ is a unit and $a_i$ $(0 < i \leq n)$ are nilpotent. We will say that $g$ divides $f$ (written $g|f$) if there is a polynomial $h(X) = \sum_{i=0}^{l} c_i X^i$ such that $f = gh$. Therefore if $a_n$ is a unit, then $f(X)$ is irreducible whenever there is no polynomial $g(X) = \sum_{i=0}^{m} b_i X^i$ with $m > 0$ such that $g|f$.

An element $a \in A$ is a *nilpotent* element if there is a positive integer $n$ such that $a^n = 0$. The smallest such $n$ will be called the *nilpotency* of $a$. If $a$ is non-nilpotent, then we will say that the nilpotency of $a$ is $\infty$. And we adopt the convention that $\infty$ larger than any integer.

Let $\phi : A \to B$ be a ring homomorphism. For a polynomial $f(X) = \sum_{i=0}^{n} a_i X^i$ in $A[X]$ we will write $\phi(f(X)) = \sum_{i=0}^{n} \phi(a_i) X^i \in B[X]$. Often we will abbreviate $\phi(a_i)$ by $\bar{a}_i$.

We will make use of the following observation.

**Lemma 3.1.** *Let $\phi : A \to B$ be a ring homomorphism and let $f(X) = \sum_{i=0}^{n} a_i X^i$ be a polynomial in $A[X]$. Suppose $\phi(a_n)$ is a unit and $\phi(f(X)) = \sum_{i=0}^{n} \phi(a_i) X^i \in B[X]$ is irreducible then so is $f(X)$ in $A[X]$.*

*Proof.* Assume $f = gh$ with $g(X) = \sum_{i=0}^{m} b_i X^i$ and $h(X) = \sum_{i=0}^{l} c_i X^i$ with $m, l > 0$. Then $\phi(b_m)$ and $\phi(c_l)$ are units. In particular, $\deg(g) = \deg(\phi(g))$ and $\deg(h) = \deg(\phi(h))$. Hence $\phi(f) = \phi(g)\phi(h)$ is a proper factorization in $B[X]$. □

**Corollary 3.2.** *Let $\phi : A \to B$ be a ring homomorphism where $B$ is Noetherian. Let $f(X) = \sum_{i=0}^{n} a_i X^i$ be a polynomial in $A[X]$. For any $g(X) = \sum_{i=0}^{m} b_i X^i$ $(m < n)$ in $B[X]$ such that $b_m$ is a unit and $b_0|\phi(a_0)$ does not satisfies the condition* (R) *of Theorem 2.5 then $f(X)$ is irreducible in $A[X]$.*

*Proof.* Follows immediately from Theorem 2.5 and the lemma above. □

We will show how Eisenstein criterion can be deduced from our result. (see for example, [Lang, *Algebra*, Addison Wesley, 3rd ed, 1993].) A *unique factorization domain* (UFD for short. Lang used the term 'factorial ring') is an integral domain in which every element has a 'unique' factorization into irreducible elements. An irreducible element of a UFD generates a prime ideal and is called a *prime element.*

**Theorem 3.3** (Eisenstein criterion)**.** *Let $A$ be a UFD with its quotient field $K$. Let $f(X) = a_n X^n + \cdots + a_0$ be a polynomial of degree $n \geq 1$ in $A[X]$. Let $p$ be a prime in $A$ and assume*

$$p \nmid a_n, \quad p|a_i \ (i = 0, 1, \ldots, n-1), \quad p^2 \nmid a_0.$$

*Then $f(X)$ is irreducible in $K[X]$. If $a_n$ is a unit, then $f(X)$ is irreducible in $A[X]$.*

Since Theorem 2.5 required the ring $A$ to be Noetherian whereas the Eisenstein criterion did not, we need to reduce the statement of Eisenstein criterion for a Noetherian ring. For this we will use the following lemma. For its proof we will use the results in [2].

**Lemma 3.4.** *Let $A$ be a UFD and $\mathfrak{p}_0, \mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the prime ideals generated by the primes $p_i$ $(i = 0, 1, \ldots, n)$ of $A$. Let $S$ be the multiplicative $S = \cup_{i=0}^{n} \mathfrak{p}_i$. Then $S^{-1}A$ is a Noetherian UFD. A fortiori, $S^{-1}A$ is a PID.*

*Proof.* First we know that [2, Theorem 1, p. 502] $A$ is a Krull domain. Therefore so is $S^{-1}A$. And $S^{-1}A$ is a semilocal ring with the maximal ideals $S^{-1}\mathfrak{p}_i$. Hence $S^{-1}A$ is a Dedekind domain. By [2, Theorem 1, p. 494], we see that $S^{-1}A$ is Noetherian.

It is well known that a semilocal Dedekind domain is a PID. See for example see [Serge Lang, *Algebraic number theory*, Addison-Wesley, 1970, Proposition 15, p. 21]. □

Using this we can prove Eisenstein criterion by the way of Theorem 2.5.

*Proof of Eisenstein criterion.* Let $p_0, p_1, \dots, p_n$ be the set of all prime divisors of the coefficients of $f(X)$ and let $p = p_0$. Let $\mathfrak{p}_i = (p_i)$ be the prime ideals generated by $p_i$ $(i = 0, 1, \dots, n)$ and let $S = \cup_{i=0}^{n} \mathfrak{p}_i$. Let $B = S^{-1}A/\mathfrak{p}_0$ (which is a field) and let $\phi$ be the composition of the maps $A \to S^{-1}A \to B = S^{-1}A/\mathfrak{p}_0$. We will denote the image $\phi(a)$ of $a$ under $\phi$ by $\bar{a}$.

Suppose $g(X) = \sum_{i=0}^{m} b_i X^i \in A[X]$ $(m > 0)$ is a divisor of $f$; let $f = gh$ with $h(X) = \sum_{i=0}^{k} c_i X^i$. Then since $p^2 \nmid a_0 = b_0 c_0$ we have either $p \nmid b_0$ or $p \nmid c_0$. Hence we may assume without loss of generality that $p \nmid b_0$. (Otherwise reverse the role of $g$ and $h$.) Therefore the canonical image $\bar{b}_0$ of $b_0$ in $B/(p)$ is also nonzero. Further, since $p$ divides $a_i$ $(i = 0, 1, \dots, n-1)$ we see that $\bar{a}_i = 0$ $(i = 0, 1, \dots, n-1)$.

Thus the resultant matrix $R(\phi(f), \phi(g))$ is of the form

$$R(\phi(f), \phi(g)) = \begin{pmatrix} \bar{a}_n & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & \bar{a}_n & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \ddots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \cdots & 0 & \bar{a}_n & 0 & \cdots & \cdots & 0 \\ \bar{b}_m & \bar{b}_{m-1} & \cdots & \bar{b}_1 & \bar{b}_0 & 0 & 0 & 0 \\ 0 & \bar{b}_m & \bar{b}_{m-1} & \cdots & \bar{b}_1 & \bar{b}_0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & \bar{b}_m & \bar{b}_{m-1} & \cdots & \cdots & \bar{b}_0 \end{pmatrix}.$$

Since we assumed $g|f$ we see that $\phi(g)$ divides $\phi(f)$. Hence the condition (R) of Theorem 2.5 for $R(\phi(f), \phi(g))$ has to be satisfied namely the minors of size bigger than $n$ has to vanish. However the determinant of $R(\phi(f), \phi(g))$ is $\bar{a}_n^m \bar{b}_0^n$ which is nonzero. This is a contradiction. □

## 4. Generalized Eisenstein criterion

**Theorem 4.1.** *Let $A$ be a commutative ring and $B$ be a Noetherian ring. Let $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$ be a polynomial of degree $n \geq 1$ in $A[X]$. Let $\phi : A \to B$ be a ring homomorphism such that*

(i) *$\phi(a_n)$ is a unit,*

(ii) *$\phi(a_i) = 0$ $(i = 0, 1, \dots, n-1)$,*

(iii) *if $a_0 = b_0 c_0$, then either $\phi(b_0)$ or $\phi(c_0)$ is of nilpotency $> n$.*

*Then $f(X)$ is irreducible in $A[X]$.*

*Proof.* Suppose $g(X) = \sum_{i=0}^{m} b_i X^i \in A[X]$ is a divisor of $f$. And let $f = gh$ with $h(X) = \sum_{i=0}^{l} c_i X^i \in A[X]$. Then $b_0 c_0 = a_0$ and, by (iii), either $\phi(b_0)$ or $\phi(c_0)$ is of nilpotency $> n$. We may assume $\phi(b_0)$ is of nilpotency $> n$. (Otherwise reverse the role of $g$ and $h$.)

Since $\phi(f) = \phi(g)\phi(h)$, the minors of resultant matrix $R(\phi(f), \phi(g))$ of size bigger than $n$ must vanish by Theorem 2.5. By (ii) we have

$$R(\phi(f), \phi(g)) = \begin{pmatrix} \bar{a}_n & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & \bar{a}_n & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \ddots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \cdots & 0 & \bar{a}_n & 0 & \cdots & \cdots & 0 \\ \bar{b}_m & \bar{b}_{m-1} & \cdots & \bar{b}_1 & \bar{b}_0 & 0 & 0 & 0 \\ 0 & \bar{b}_m & \bar{b}_{m-1} & \cdots & \bar{b}_1 & \bar{b}_0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & \bar{b}_m & \bar{b}_{m-1} & \cdots & \cdots & \bar{b}_0 \end{pmatrix},$$

where bar denotes the image under $\phi$. The determinant of the resultant matrix $R(\phi(f), \phi(g))$ is $\bar{a}_n^k \bar{b}_0^n$. Since we assumed $\bar{a}_n$ is a unit and $\bar{b}_0$ is of nilpotency $> n$ we see that $\det(R(\phi(f), \phi(g))) \neq 0$. This contradicts to the requirement that the minors of size bigger than $n$ must vanish. □

*Remark.* Using Theorem 4.1, we can prove Eisenstein criterion. In fact, if we choose $\phi$ and $B$ as in the proof of Theorem 3.3, then all the conditions of Theorem 4.1 are satisfied.

The following result may be proved by the same method as the original proof of Eisenstein criterion. However we prove this by using the main result of [4]. The following rather well known result [3, Exercise 18.11] may be proved by the same method as the original proof of Eisenstein criterion. However we prove this by using the main result of [4].

**Corollary 4.2.** *Let $A$ be a Noetherian ring and let $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$ be a polynomial of degree $n \geq 1$ in $A[X]$. Let $\mathfrak{p}$ be a prime ideal of $A$ and assume*

$$a_n \notin \mathfrak{p}, \quad a_i \in \mathfrak{p} \ (i = 0, 1, \ldots, n-1), \quad a_0 \notin \mathfrak{p} \setminus \mathfrak{p}^2.$$

*Then $f(X)$ is irreducible in $A[X]$.*

*Proof.* We let $B = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ and let $\phi$ be the composition $A \to A_{\mathfrak{p}} \to A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$. Then the conditions of Theorem 4.1 are satisfied. Hence $f(X)$ is irreducible in $A[X]$. □

In order to further generalize Eisenstein criterion we will use the following fact which should be well known.

**Lemma 4.3.** *Let $M_1, M_4$ be square matrices and $M_1$ is invertible. Then we have*

$$\begin{pmatrix} M_1 & M_2 \\ M_3 & M_4 \end{pmatrix} = \begin{pmatrix} I & 0 \\ M_3M_1^{-1} & I \end{pmatrix} \begin{pmatrix} M_1 & 0 \\ 0 & M_4 - M_3M_1^{-1}M_2 \end{pmatrix} \begin{pmatrix} I & M_1^{-1}M_2 \\ 0 & I \end{pmatrix}.$$

*In particular we have*

$$\det \begin{pmatrix} M_1 & M_2 \\ M_3 & M_4 \end{pmatrix} = \det(M_1) \cdot \det(M_4 - M_3M_1^{-1}M_2).$$

*Proof.* One can check (i) easily and (ii) follows from (i). □

The following theorem can be viewed as a generalization of Eisenstein criterion.

**Theorem 4.4.** *Let $A$ be a commutative ring and $B$ be a Noetherian ring and let $\phi : A \to B$ be a ring homomorphism. Let $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$ be a polynomial of degree $n \geq 1$ in $A[X]$. Let $k$ be an integer such that $0 \leq k < n$. Assume*

(i) $\phi(a_n)$ *is a unit,*

(ii) $\phi(a_i) = 0$ $(i = 0, 1, \ldots, k)$.

*Then $f(X)$ has no divisor $g(X) \in A[X]$ of degree $\geq n - k$ with $\phi(g(0))$ of nilpotency $> k + 1$.*

*Proof.* Suppose $g(X) = \sum_{i=0}^{m} b_iX^i$ $(m \geq n - k)$ is a divisor of $f$ such that the nilpotency of $\phi(b_0)$ is $> k + 1$. First we have that $R(\phi(f), \phi(g))$ is of the form

$$R(\phi(f), \phi(g)) = \begin{pmatrix} \bar{a}_n & \cdots & \bar{a}_{k+1} & 0 & 0 & 0 & \cdots & \cdots & 0 \\ 0 & \bar{a}_n & \cdots & \bar{a}_{k+1} & 0 & 0 & \cdots & \cdots & 0 \\ \cdots & \cdots & \ddots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \cdots & 0 & \bar{a}_n & \cdots & \bar{a}_{k+1} & 0 & \cdots & 0 \\ \bar{b}_m & \bar{b}_{m-1} & \cdots & \bar{b}_1 & \bar{b}_0 & 0 & 0 & \cdots & 0 \\ 0 & \bar{b}_m & \bar{b}_{m-1} & \cdots & \bar{b}_1 & \bar{b}_0 & 0 & \cdots & 0 \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \cdots & \cdots & 0 & \bar{b}_m & \bar{b}_{m-1} & \cdots & \cdots & \bar{b}_0 \end{pmatrix}.$$

Since $\phi(g)|\phi(f))$ we must have all minors of $R(\phi(f), \phi(g))$ of size $> n$ vanish. We will show that this is not the case. Let $M_1$ be the $m \times m$ matrix on the upper left corner and $M_4$ be the $n \times n$ matrix on the lower right corner. And let $M_3$ be the $n \times m$ matrix on the lower left corner and finally let $M_2$ be the $m \times n$ matrix on the upper right corner. Hence $R(\phi(f), \phi(g))$ can be written as

$$R(\phi(f), \phi(g)) = \begin{pmatrix} M_1 & M_2 \\ M_3 & M_4 \end{pmatrix}.$$

First suppose $B$ is a field. We want show that $R(\phi(f), \phi(g))$ has rank $> n$. Obviously the rank of $\left(\begin{smallmatrix} M_1 & M_2 \\ M_3 & M_4 \end{smallmatrix}\right)$ is the same as the rank of $\left(\begin{smallmatrix} M_1 & 0 \\ 0 & M_4 - M_3M_1^{-1}M_2 \end{smallmatrix}\right)$

by Lemma 4.3. Let's look at the lower left corner $M_3M_1^{-1}M_2$ which is of the form

$$\begin{pmatrix} \bar{b}_m & \bar{b}_{m-1} & \cdots & \bar{b}_1 \\ 0 & \bar{b}_m & \cdots & b_2 \\ \cdots & \cdots & \cdots & \\ 0 & 0 & 0 & b_m \\ 0 & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \\ \cdots & \cdots & \cdots & \\ \cdots & \cdots & \cdots & \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \bar{a}_n & \cdots & \bar{a}_{k+1} & 0 & \cdots & 0 \\ 0 & \bar{a}_n & \cdots & a_{k+1} & \cdots & 0 \\ & \cdots & & \cdots & & \\ & \cdots & & \cdots & & \\ & \cdots & & \cdots & & \\ 0 & 0 & 0 & & & a_n \end{pmatrix}^{-1} \begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 & 0 \\ & \cdots & & & \cdots & \\ 0 & 0 & \cdots & \cdots & 0 & 0 \\ \bar{a}_{k+1} & 0 & 0 & 0 & 0 & 0 \\ \bar{a}_{k+2} & \bar{a}_{k+1} & 0 & 0 & 0 & 0 \\ & & \ddots & & & \\ * & * & & & & \\ * & \cdots & \bar{a}_{k+2} & \bar{a}_{k+1} & \cdots & 0 \end{pmatrix},$$

where $*$ denotes the entries in which we are not interested. We know that $M_1^{-1}$ is again an upper triangular matrix and $M_3M_1^{-1}$ is an $n \times m$ matrix whose possible nonzero entries are in the first $m$ rows. On the other hand, $M_2$ is an $m \times n$ matrix with possible nonzero entries in the lower $(n-k-1) \times (n-k-1)$ matrix. Thus the only nonzero entries of $M_3M_1^{-1}M_2$ are in the first $(n-k-1)$ columns.

Now delete the first $(n-k-1)$ columns and rows from $M_4 - M_3M_1^{-1}M_2$ then we obtain a $(k+1) \times (k+1)$ matrix whose determinant is $\bar{b}_0^{k+1}$ which is nonzero. Hence the rank of $M_4 - M_3M_1^{-1}M_2$ is bigger than or equal to $k+1$. On the other hand, we know that $M_1$ is an $m \times m$ invertible matrix. Hence the rank of $\left(\begin{smallmatrix} M_1 & 0 \\ 0 & M_4 - M_3M_1^{-1}M_2 \end{smallmatrix}\right)$ is bigger than or equal to $m+k+1$ which is $> n$. Thus the rank of $R(\phi(f), \phi(g))$ is $> n$. As we contended.

Now suppose $B$ is a commutative ring. Then the rank of a matrix does not make sense. It turns out that the notion of Fitting invariant instead of rank works for our situation. We will show that the $(m+k+1)$-th Fitting invariant of $R(\phi(f), \phi(g))$ is nonzero. (Then we are done since $m+k+1 > n$.)

By Corollary 2.4, we have $I_{m+k+1}\left(\begin{smallmatrix} M_1 & M_2 \\ M_3 & M_4 \end{smallmatrix}\right) = I_{m+k+1}\left(\begin{smallmatrix} M_1 & 0 \\ 0 & M_4 - M_3M_1^{-1}M_2 \end{smallmatrix}\right)$. Since $I_{m+k+1}(*)$ is generated by all $(m+k+1) \times (m+k+1)$ minors it suffices to show that there is a nonzero minor of size $(m+k+1)$. As above the $(m+k+1) \times (m+k+1)$ matrix obtained by deleting the $(m+1), (m+2), \ldots, (m+k-n+1)$-th rows and columns from $\left(\begin{smallmatrix} M_1 & 0 \\ 0 & M_4 - M_3M_1^{-1}M_2 \end{smallmatrix}\right)$ has determinant $\bar{a}_n^m \bar{b}_0^{k+1}$ which is nonzero since $\bar{a}_n$ is a unit and $\bar{b}_0$ is of nilpotency $> k+1$. □

*Remark.* Again Eisenstein criterion can be deduced from Theorem 4.4 with $k = n-1$. In fact, if $g$ is a divisor say $f = gh$, then we may assume $p \nmid g(0)$. (For otherwise reverse the role of $g$ and $h$.) Choose $B = A/(p)$ (if $A$ is not Noetherian, then we may have to localize as we did before) and $\phi$ to be the natural map $A \to B$. Now the theorem asserts that $f$ has no factor of degree $\geq 1$.

**Corollary 4.5.** *Let $A$ be a commutative ring and $B$ be a Noetherian ring. Let $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$ be a polynomial of degree $n \geq 1$ in $A[X]$. Let $\phi : A \to B$ be a ring homomorphism. Let $k$ be an integer such that $0 \leq k < n$. Assume*

(i) *$\phi(a_n)$ is a unit,*
(ii) $\phi(a_i) = 0$ $(i = 0, 1, \dots, k)$,
(iii) *if $a_0 = b_0 c_0$, then $\phi(b_0)$ and $\phi(c_0)$ are of nilpotency $> k+1$.*
*Then $f(X)$ has no divisor $g(X) \in A[X]$ of degree $\geq n-k$.*

*Proof.* In the proof of the theorem the condition we needed was that the constant term of the divisor $g$ is of nilpotency $> k+1$ which was used to show the $(m+k+1) \times (m+k+1)$ minor $\bar{a}_n^m \bar{b}_0^{k+1}$ is nonzero. Now this is guaranteed by the condition (iii). □

Next we will show that the condition (ii) of Theorem 4.4 can be replaced by a weaker condition that "$\phi(a_i)$ is nilpotent for $i = 0, 1, \dots, k$."

**Theorem 4.6.** *Let $A$ be a commutative ring and $B$ be a Noetherian ring. Let $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$ be a polynomial of degree $n \geq 1$ in $A[X]$. Let $\phi : A \to B$ be a ring homomorphism. Let $k$ be an integer such that $0 \leq k < n$. Assume*
(i) *$\phi(a_n)$ is a unit,*
(ii) *$\phi(a_i)$ is nilpotent for $i = 0, 1, \dots, k$.*
*Then $f(X)$ has no divisor $g(X) \in A[X]$ of degree $\geq n-k$ with $g(0)$ a non-nilpotent element.*

*Proof.* Suppose $g(X) = \sum_{i=0}^m b_i X^i$ $(m \geq n-k)$ is a divisor of $f$ with $\phi(b_0)$ is not nilpotent. First we have that $R(\phi(f), \phi(g))$ is of the form

$$R(\phi(f),\phi(g)) = \begin{pmatrix} \bar{a}_n & \cdots & \bar{a}_{k+1} & n_k & \cdots & n_0 & \cdots & \cdots & 0 \\ 0 & \bar{a}_n & \cdots & \bar{a}_{k+1} & n_k & \cdots & \cdots & \cdots & 0 \\ \cdots & \cdots & \ddots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \cdots & 0 & \bar{a}_n & \cdots & \bar{a}_{k+1} & n_k & \cdots & n_0 \\ \bar{b}_m & \bar{b}_{m-1} & \cdots & \bar{b}_1 & \bar{b}_0 & 0 & 0 & \cdots & 0 \\ 0 & \bar{b}_m & \bar{b}_{m-1} & \cdots & \bar{b}_1 & \bar{b}_0 & 0 & \cdots & 0 \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \cdots & \cdots & 0 & \bar{b}_m & \bar{b}_{m-1} & \cdots & \cdots & \bar{b}_0 \end{pmatrix},$$

where the bar denotes the image under $\phi$. As before write $R(\phi(f), \phi(g))$ as

$$R(\phi(f),\phi(g)) = \begin{pmatrix} M_1 & M_2 \\ M_3 & M_4 \end{pmatrix},$$

where $M_1$ is the $m \times m$ matrix on the upper left corner and $M_4$ be the $n \times n$ matrix on the lower right corner of $R(\phi(f), \phi(g))$. And $M_3$ is the $n \times m$ matrix on the lower left corner and $M_2$ is the $m \times n$ matrix on the upper right corner of $R(\phi(f), \phi(g))$.

Since we assumed $\phi(g)$ divides $\phi(f)$ we must have all minors of $R(\phi(f), \phi(g))$ of size $> n$ vanish. We will show that this is not the case.

As in the proof of Theorem 4.4, we will show that the $(m+k+1)$-th Fitting invariant of $R(\phi(f), \phi(g))$ is nonzero. As in the proof of Theorem 4.4, we need to show that $I_{m+k+1}\left(\begin{smallmatrix} M_1 & 0 \\ 0 & M_4-M_3M_1^{-1}M_2 \end{smallmatrix}\right)$ is nonzero. Now $M_3M_1^{-1}$ is of the form

$$\begin{pmatrix} \bar{b}_m & \bar{b}_{m-1} & \cdots & \bar{b}_1 \\ 0 & \bar{b}_m & \cdots & b_2 \\ \cdots & \cdots & \cdots & \\ 0 & 0 & 0 & b_m \\ 0 & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \\ \cdots & \cdots & \cdots & \\ \cdots & \cdots & \cdots & \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \bar{a}_n & \cdots & \bar{a}_{k+1} & n_k & n_{k-1} & \cdots \\ 0 & \bar{a}_n & \cdots & a_{k+1} & n_k & \cdots \\ & \cdots & & \cdots & & \\ & \cdots & & \cdots & & \\ & \cdots & & \cdots & a_n & a_{n-1} \\ 0 & 0 & 0 & & & a_n \end{pmatrix}^{-1}$$

and the possible nonzero entries are in the first $m$ rows.

And $M_2$ is of the form

$$\begin{pmatrix} n_* & \cdots & n_0 & \cdots & 0 & 0 \\ & \cdots & & & \cdots & \\ n_k & n_{k-1} & \cdots & \cdots & 0 & 0 \\ \bar{a}_{k+1} & n_k & \cdots & n_0 & 0 & 0 \\ \bar{a}_{k+2} & \bar{a}_{k+1} & n_k & \cdots & n_0 & 0 \\ * & * & \ddots & & & \\ * & \cdots & \bar{a}_{k+2} & \bar{a}_{k+1} & \cdots & n_0 \end{pmatrix},$$

where $*$ denotes the entries in which we are not interested. Further only possible non-nilpotent entries are in the first $(n-k-1)$ columns. Hence the possible non-nilpotent entries of the product $M_3M_1^{-1}M_2$ are in the first $(n-k-1)$ columns.

Since the sum of two nilpotent elements and a product of a nilpotent element and arbitrary element are again nilpotent we see that $M_4 - M_3M_1^{-1}M_2$ is of the form

$$\begin{pmatrix} \bar{b}_0 & 0 & & & \cdots & 0 \\ \bar{b}_1 & \bar{b}_0 & 0 & & \cdots & 0 \\ & \cdots & & & \cdots & \\ \bar{b}_m & \cdots & \bar{b}_1 & \bar{b}_0 & \cdots & 0 \\ & \cdots & & & \cdots & 0 \\ 0 & \cdots & \bar{b}_m & \bar{b}_{m-1} & \cdots & \bar{b}_0 \end{pmatrix} - \begin{pmatrix} * & \cdots & * & \natural & \cdots & \natural \\ & \cdots & & & \cdots & \\ * & \cdots & * & \natural & \cdots & \natural \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix},$$

where $\natural$'s denotes a nilpotent element. (The only possible nonzero rows of the second matrix are the first $m$ rows.) If we delete the first $(n-k-1)$ columns and rows from $M_4 - M_3M_1^{-1}M_2$ then it is of the form

$$\begin{pmatrix} \bar{b}_0 + \natural & \natural & \cdots & \natural & & \cdots & \natural \\ & \ddots & & & & \cdots & \\ * & \cdots & \bar{b}_0 + \natural & \natural & & \cdots & \natural \\ 0 & \bar{b}_m & * & \bar{b}_0 & 0 & \cdots & 0 \\ & \cdots & & & \ddots & & 0 \\ \cdots & 0 & \bar{b}_m & \cdots & & \bar{b}_0 & 0 \\ 0 & \cdots & 0 & \bar{b}_m & \cdots & & \bar{b}_0 \end{pmatrix}.$$

The determinant of this matrix is of the form $\bar{b}_0^{k+1} + \nu$ where $\nu$ is some nilpotent element. Therefore $\left(\begin{smallmatrix} M_1 & 0 \\ 0 & M_4 - M_3M_1^{-1}M_2 \end{smallmatrix}\right)$ contains a $(m+k+1) \times (m+k+1)$ submatrix whose determinant is of the form $\bar{a}_n^m \bar{b}_0^{k+1} + \nu_0$ for some nilpotent element $\nu_0$. Since $\bar{a}_n$ is a unit and $b_0$ is not nilpotent we see that the determinant is nonzero. □

## References

[1] Bourbaki, *Elements of Mathematics, Algebra II*, Addison-Wesley, 1973.

[2] ———, *Elements of Mathematics, Commutative Algebra*, Addison-Wesley, 1972.

[3] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, New York Berlin, 1995.

[4] S. S. Woo, *Dividing polynomials using the resultant matrix*, Comm. Alg. **35** (2007), 3263–3272.

Department of Mathematics
Ewha Women's University
Seoul 120-750, Korea
*E-mail address*: sswoo@ewha.ac.kr