

A division algorithm

Fred Richman
Florida Atlantic University
Boca Raton, FL 33431
`richman@fau.edu`

Abstract

A divisibility test of Arend Heyting, for polynomials over a field in an intuitionistic setting, may be thought of as a kind of division algorithm. We show that such a division algorithm holds for divisibility by polynomials of content 1 over any commutative ring in which nilpotent elements are zero. In addition, for an arbitrary commutative ring R , we characterize those polynomials g such that the R -module endomorphism of $R[X]$ given by multiplication by g has a left inverse.

1 Introduction

In [3], Arend Heyting talks about polynomials over what has become known as a *Heyting field* [5]. This is a commutative ring with an **apartness relation**, $x \neq y$, that satisfies the following properties

- Not $x \neq x$. (consistent)
- If $x \neq y$, then $y \neq x$. (symmetric)
- If $x \neq z$, then either $x \neq y$ or $y \neq z$. (cotransitive)
- If not $x \neq y$, then $x = y$. (tight)
- If $x \neq y$, then $x + z \neq y + z$. (shift invariant)
- $x \neq 0$ if and only if x is invertible. (field)

If $a = a_0 + a_1X + \cdots + a_nX^n$ is a polynomial with coefficients in a Heyting field, then $a \neq 0$ means $a_i \neq 0$ for some i .

The model that Heyting had in mind was the real numbers, with apartness being a positive form of inequality: two real numbers are apart if we can find a positive rational number that bounds them away from one another. Thus tightness is a form of the *archimedean* property—no infinitesimals—that is the basis for Archimedes’ famous proofs by double contradiction. The first three properties are the duals of the axioms for an equivalence relation. We can use the field property to *define* the relation $x \neq 0$ algebraically, and then define $x \neq y$ to be $x - y \neq 0$ in accordance with shift invariance. Thus we can eliminate the apartness entirely, and just keep the algebraic versions of the first four properties.

The algebraic interpretation of consistency is that zero is not a unit, that is, the ring is nontrivial. Symmetry is automatic while cotransitivity says that the ring is local: if $x + y$ is invertible, then either x or y is invertible. Tightness says that any nonunit is zero, so it is this property that gives us a field in the traditional sense. In the presence of the law of excluded middle, tightness also implies that any nonzero element is a unit. Heyting does not assume that law, so being a unit may be stronger than being nonzero, which is the whole point of introducing the apartness. I’m not concerned with this issue here as I am going to drop the tightness condition.

Many intuitionistic theorems about Heyting fields require neither tightness nor consistency, so they are really theorems about local rings. However, one consequence of tightness and consistency which will play a role in what follows is that nilpotent elements are zero (the ring is reduced). Indeed, suppose $x^n = 0$ and we want to show that $x = 0$. By tightness, it suffices to derive a contradiction from $x \neq 0$. But if $x \neq 0$, then x is a unit, so x^n is a unit, so $x^n \neq 0$. By consistency, this is a contradiction, so $x = 0$.

There is a sort of converse to this implication from tight (if x is not invertible, then $x = 0$) to nilpotents are zero. Pass to the ring $S^{-1}R$ where $S = \{1, x, x^2, \dots\}$. The ring $S^{-1}R$ is the universal construction of a ring in which x is invertible, and $S^{-1}R$ is trivial ($1 = 0$) exactly when x is nilpotent in R . To apply tightness in practice, one assumes that x is invertible and derives a contradiction. Often this derivation shows directly that $1 = 0$ in the ring R . Instead of *assuming* that x is invertible, we can pass to $S^{-1}R$ where x is invertible. The derivation will now show that $1 = 0$ in $S^{-1}R$. Thus we have a strategy for reading proofs that assume tightness as proofs that assume only that nilpotent elements are zero.

The strategy works for the proof in [3] of the following theorem which motivated this paper. So we may replace “Heyting field” here by “local ring with no nilpotents.”

Theorem 1 (Heyting) *Let R be a Heyting field. Let a and b be polynomials with coefficients in R such that $a \neq 0$. Then we can compute elements e_1, \dots, e_m of R , polynomials in the coefficients of a and b , so that $b = qa$ for some q if and only if $e_i = 0$ for all i .*

For example, if a is a monic polynomial, then we can use the division algorithm to write $b = qa + r$ where $\deg r < \deg a$. The coefficients of r serve as the elements e_1, \dots, e_m in the theorem. Thus Theorem 1 may be thought of as an extension of the division algorithm.

The division algorithm for a monic polynomial a can be thought of in terms of the map λ taking b to q . This map is an R -endomorphism of $R[X]$ which is a left inverse for multiplication by a . Given such a left inverse λ , we can get Heyting’s elements e_1, \dots, e_m as the coefficients of $b - \lambda(f)a$. In general, a left inverse is too much to expect (see Theorem 6) so, with Heyting, we construct *local* left inverses (Theorem 4). This can be done for an arbitrary commutative ring if a has content 1. However, for local inverses to suffice, we must be able to bound the degree of q in terms of the degree of b , and this is where the condition that nilpotent elements of R are zero comes into play.

2 Local left inverses

Let R be a commutative ring, $R[X]$ the polynomial ring over R in the indeterminate X , and

$$R[X]_n = \{c_0 + c_1X + \dots + c_nX^n : c_i \in R \text{ for } i = 0, \dots, n\}$$

the (free) R -submodule of $R[X]$ consisting of the polynomials of degree at most n . If $a \in R[X]_n$, then multiplication by a induces an R -homomorphism $T_m : R[X]_m \rightarrow R[X]_{m+n}$ for each m . When does T_m have a left inverse? For R a Heyting field, Heyting showed that T_m has a left inverse if $a \neq 0$. His proof goes through for local rings.

We will show, for an arbitrary commutative ring R , that it is enough for the coefficients of a to generate R as an ideal (a has content 1), which in the

local case simply says that some coefficient of a is a unit (that is, $a \neq 0$). The key fact is the following lemma.

Lemma 2 *Let q be an $(m + 1)$ -form in $\mathbf{Z}[X_0, \dots, X_n]$. Then there exist m -forms p_0, \dots, p_{m+n} in $\mathbf{Z}[X_0, \dots, X_n]$ such that $\sum_{k=0}^n p_k X_k = q$ and $\sum_{k=0}^n p_{k+j} X_k = 0$ for $0 < j \leq m$.*

Proof. Consider the map Φ from $(m + n + 1)$ -tuples of m -forms to $(m + 1)$ -tuples of n -forms such that $\Phi(p_0, \dots, p_{m+n}) = (v_0, \dots, v_m)$ where $v_j = \sum_{k=0}^n p_{k+j} X_k$. We want to show that $(q, 0, \dots, 0)$ is in the image of Φ for any $(m + 1)$ -form q . By linearity we may assume that q is a monomial. The proof is by induction on $m + n$. If either $m = 0$ or $n = 0$, choose X_i dividing q , let $p_i = q/X_i$ and let $p_k = 0$ if $k \neq i$. So we may assume that $m, n > 0$.

First suppose that X_n divides q , so $q = X_n q'$. By induction, because $m > 0$, there exist $(m - 1)$ -forms p'_0, \dots, p'_{m+n-1} such that $\sum_{k=0}^n p'_{k+j} X_k = 0$ if $0 < j \leq m - 1$, and $\sum_{k=0}^n p'_k X_k = q'$. Set $p_k = X_n p'_k$ for $k < m + n$ and $p_{m+n} = -\sum_{k=0}^{n-1} p'_{k+m} X_k$. Then

$$\sum_{k=0}^n p_{k+j} X_k = \begin{cases} X_n \sum_{k=0}^n p'_k X_k = X_n q' = q & \text{if } j = 0 \\ X_n \sum_{k=0}^n p'_{k+j} X_k = 0 & \text{if } 0 < j < m \\ X_n \sum_{k=0}^{n-1} p'_{k+m} X_k + p_{n+m} X_n = 0 & \text{if } j = m \end{cases}$$

Note that p_k is divisible by X_n if $k < m + n$. So if q is divisible by X_n , then $(q, 0, \dots, 0) = \Phi(p_0, \dots, p_{m+n})$ where p_k is divisible by X_n if $k < m + n$. It follows that $\Phi(0, \dots, 0, p_0, \dots, p_{m+n-i}) = (v_0, \dots, v_m)$ where v_{i+1}, \dots, v_m are zero, v_0, \dots, v_{i-1} are divisible by X_n and $v_i = q$. By taking linear combinations of these, we see that any vector (v_0, \dots, v_m) is in the image of Φ if each v_i is divisible by X_n .

Now suppose that X_n does not divide q , so $q \in \mathbf{Z}[X_0, \dots, X_{n-1}]$. By induction, because $n > 0$, there exist m -forms p_0, \dots, p_{m+n-1} in $\mathbf{Z}[X_0, \dots, X_{n-1}]$ such that $\sum_{k=0}^{n-1} p_k X_k = q$ and $\sum_{k=0}^{n-1} p_{k+j} X_k = 0$ for $0 < j \leq m$. For any value of p_{m+n} we have $\Phi(p_0, \dots, p_{m+n}) = (v_0, \dots, v_m)$ where $v_0 = q$ and v_1, \dots, v_m are divisible by X_n . So adding a vector constructed in the previous paragraph gives us $(q, 0, \dots, 0)$. ■

Theorem 3 Let $a_0, a_1, \dots, a_n, s_0, s_1, \dots, s_n$ be indeterminates and m a non-negative integer. Then there exist integral forms b_0, b_1, \dots, b_{m+n} of degree m in the a 's and degree 1 in the s 's such that

$$\sum_{i=0}^n b_{i+j} a_i = \begin{cases} \sum_{i=0}^n s_i a_i^{m+1} & \text{if } j = 0 \\ 0 & \text{if } 0 < j \leq m \end{cases}$$

Proof. By linearity it suffices, for each $k = 0, \dots, n$, to construct forms b_0, b_1, \dots, b_{m+n} such that

$$\sum_{i=0}^n b_{i+j} a_i = \begin{cases} s_k a_k^{m+1} & \text{if } j = 0 \\ 0 & \text{if } 0 < j \leq m \end{cases}$$

Lemma 2 gives integral m -forms $b'_0, b'_1, \dots, b'_{m+n}$ in $\mathbf{Z}[a_0, \dots, a_n]$ such that

$$\sum_{i=0}^n b'_{i+j} a_i = \begin{cases} a_k^{m+1} & \text{if } j = 0 \\ 0 & \text{if } 0 < j \leq m \end{cases}$$

Set $b_i = s_k b'_i$ for $i = 0, \dots, m+n$. ■

Theorem 4 If $a \in R[X]_n$, then the map $T_m : R[X]_m \rightarrow R[X]_{m+n}$, induced by multiplication by a , has a left inverse if and only if the coefficients of a generate R as an ideal.

Proof. If λ is a left inverse of T_m , then $\lambda(a) = \lambda(T_m(1)) = 1 \in R[X]_m$. So following λ by evaluation at 0 gives a linear functional on $R[X]_{m+n}$ whose value on a is equal to 1. Thus some linear combination of the coefficients of a is equal to 1.

Conversely, suppose that the coefficients of a generate R as an ideal. Let $a = a_0 + a_1 X + \dots + a_n X^n$. Then we can find $s_i \in R$ such that $s_0 a_0^{m+1} + \dots + s_n a_n^{m+1} = 1$. By Theorem 3 there exist $b_0, b_1, \dots, b_{m+n} \in R$ so that

$$\sum_{i=0}^n b_{i+j} a_i = \begin{cases} 1 & \text{if } j = 0 \\ 0 & \text{if } 0 < j \leq m \end{cases}$$

The map T_m is described by the $m + n + 1$ by $m + 1$ matrix

$$\begin{pmatrix} a_0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ a_1 & a_0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ a_2 & a_1 & a_0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & 0 \\ a_n & a_{n-1} & a_{n-2} & \cdots & a_0 & 0 & 0 & \cdots & 0 \\ 0 & a_n & a_{n-1} & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ 0 & 0 & a_n & \cdots & a_2 & a_1 & a_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a_n & a_{n-1} & a_{n-2} & \cdots & a_0 \\ 0 & 0 & 0 & \cdots & 0 & a_n & a_{n-1} & \cdots & a_1 \\ 0 & 0 & 0 & \cdots & 0 & 0 & a_n & \cdots & a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & a_n \end{pmatrix}$$

The problem is to find a left inverse for this matrix. If we multiply on the left by the $m + 1$ by $m + n + 1$ matrix

$$\begin{pmatrix} b_0 & b_1 & b_2 & \cdots & b_m & \cdots & b_{m+n} \\ 0 & b_0 & b_1 & \cdots & b_{m-1} & \cdots & b_{m+n-1} \\ 0 & 0 & b_0 & \cdots & b_{m-2} & \cdots & b_{m+n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & b_0 & \cdots & b_n \end{pmatrix}$$

we get a lower triangular $m + 1$ by $m + 1$ matrix with 1's down the diagonal. This matrix has a left inverse, hence so does the original matrix. ■

We obtain the desired generalization of Heyting's theorem as a corollary.

Corollary 5 *Suppose that nilpotent elements of R are zero and the coefficients of $a \in R[X]_n$ generate R as an ideal. Then for each m there exists an R -homomorphism $\lambda : R[X]_{m+n} \rightarrow R[X]_m$ such that $b \in R[X]_m \subset R[X]_{m+n}$ is a multiple of a if and only if $b = \lambda(f)a$.*

Proof. Let λ be a left inverse of the map $R[X]_m \rightarrow R[X]_{m+n}$ induced by multiplication by a . The “if” part is trivial, so suppose $b = qa$. It suffices to show that $q \in R[X]_m$. Suppose $q = q_0 + q_1X + \cdots + q_dX^d$ with $d \geq m$.

Induct on $d - m$. If $d = m$, then $q \in R[X]_m$ and we are done. If $d > m$, let $S = \{1, q_d, q_d^2, \dots\}$. Clearly q is regular of degree d over $S^{-1}R$. Therefore $a = 0$ over $S^{-1}R$, because $\deg qa = \deg b \leq m < d$. As the coefficients of a generate R , the ring $S^{-1}R$ is trivial. Thus q_d is nilpotent in R , therefore zero, and we are done by induction. ■

We need *some* hypothesis in this corollary to eliminate the case $a = 1 - uX$, where u is nilpotent of large order, in which case $b = 1$ is a multiple of a but not by an element of $R[X]_m$.

3 Global left inverses

Theorem 4 says that some linear combination of the coefficients of a is equal to 1 if and only if the map $T : R[X] \rightarrow R[X]$, given by multiplication by a , has local left inverses: that is, the restriction of T to a map $R[X]_m \rightarrow R[X]_{m+n}$ has a left inverse for each m . When does T itself have a left inverse? Equivalently, when is a regular and $R[X]a$ an R -summand of $R[X]$? If the leading coefficient of a is invertible, then the division algorithm provides a left inverse. If a itself is invertible, like $1 - uX$ where u is nilpotent, then multiplication by a^{-1} provides a left inverse. We first treat the case where nilpotent elements of R are zero.

Theorem 6 *Suppose that nilpotent elements of R are zero. If the map $T : R[X] \rightarrow R[X]$ given by multiplication by $a \in R[X]$ has a left inverse, then $R = R_1 \times \dots \times R_k$ and, for each i , the leading coefficient of a over R_i is invertible.*

Proof. Suppose $a \in R[X]_n$ and let a_n be the coefficient of X^n in a . Note that a_n might be zero. Let $I = \{r \in R : ra_n^k = 0 \text{ for some } k\}$. We will show that $1 \in Ra_n + I$.

By hypothesis, $R[X] = R[X]a \oplus P$ as an R -module. Let $\bar{R} = R/I$ noting that \bar{a}_n is cancellable in \bar{R} . Then $\bar{R}[X] = \bar{R}[X]\bar{a} \oplus \bar{P}$. If $b \in R[X]$, then the extended division algorithm [4, Theorem 2.14] says that $a_n^k b \in R[X]a + R[X]_{n-1}$ for some k . Let P_0 be the projection of $R[X]_{n-1}$ into P . Then P_0 is finitely generated, hence contained in $R[X]_i$ for some i . As \bar{a}_n is cancellable, it follows that $\bar{P} \subset \bar{R}[X]_i$. But \bar{P} is a summand of $\bar{R}[X]$, so \bar{P} itself is finitely generated. Now $\bar{P} \cong \bar{R}[X]/\bar{R}[X]\bar{a}$, so, as \bar{P} is finitely generated, $\bar{R}[X] \subset \bar{R}[X]\bar{a} + \bar{R}[X]_m$ for some m . In particular, $X^{m+1} = q\bar{a} + r$ in $\bar{R}[X]$,

where $r \in \overline{R}[X]_m$. So \bar{a} is a factor of a monic polynomial, whence \bar{a}_n is invertible, that is, $1 \in Ra_n + I$.

Write $1 = ra_n + s$ where $a_n^k s = 0$. Then $a_n^k = ra_n^{k+1}$ so Ra_n^k is generated by the idempotent $r^k a_n^k$. It follows that R factors as a product $R_1 \times R_2$ with a_n^k invertible in R_1 and zero in R_2 . As nilpotents in R are zero, a_n is invertible in R_1 and zero in R_2 . Thus a is of the desired form over R_1 and is in $R_2[X]_{n-1}$ over R_2 , so we are done by induction on n . ■

Note that the converse of Theorem 6 follows from the remarks about the division algorithm for polynomials a with invertible leading coefficient. The question remains of what happens if R has nilpotent elements.

Lemma 7 *Let I be an ideal of a commutative ring R and $a \in R[X]$. Suppose a_n is invertible and $a_i \in I$ for $i > n$. Then there is $g \in R[X]$ such that $g \equiv 1 \pmod{I}$ and $(ag)_i \in I^2$ for $i > n$. (Note that $(ag)_n$ is invertible.)*

Proof. Induct on m such that $a_i \in I^2$ for $i > m$. If $m = n$, take $g = 1$. If $m > n$, set $b = 1 - a_n^{-1}a_m X^{m-n} \equiv 1 \pmod{I}$. Then

$$(ab)_i = a_i - a_n^{-1}a_m a_{i-m+n}$$

where $a_j = 0$ for $j < 0$. Then $(ab)_m = 0$ and $(ab)_i \in I^2$ if $i > m$ because $i - m + n > n$ if $i > m$. By induction there exists $h \equiv 1 \pmod{I}$ so that $(abh)_i \in I^2$ for $i > n$. Set $g = bh$. ■

Theorem 8 *Let R be a commutative ring with nilradical N , and $a \in R[X]$. Then the following are equivalent:*

1. $a = cd$ where $c \equiv 1 \pmod{N}$ and d has an invertible leading coefficient.
2. $a = cd$ where c is invertible in $R[X]$ and d is monic.
3. a has an invertible leading coefficient modulo N .

Proof. Suppose (1) holds. As $c \equiv 1 \pmod{N}$ we have $c = 1 - \nu$ where $\nu^k = 0$ for some k . So c is invertible with $1 + \nu + \nu^2 + \cdots + \nu^{k-1}$ as its inverse. If u is the leading coefficient of d , then uc and d/u are the desired polynomials for (2).

Suppose (2) holds. As c is invertible, it follows that c_0 is invertible and that $c \equiv c_0 \pmod{N}$ (see below). Thus $a = cd \equiv c_0 d \pmod{N}$ so the leading coefficient of a modulo N is invertible.

Finally, suppose (3) holds. Let n be the degree of a modulo N . Let I be the ideal generated by the coefficients a_i for $i > n$. Then I is nilpotent. Repeated application of Lemma 7 gives a polynomial $g \equiv 1 \pmod{N}$ in $R[X]$ so that $\deg ag = n$. Let $c = g^{-1}$ and $d = ag$. ■

The usual proof of the key fact in the proof of (2) implies (3) is to note that modulo any prime ideal of R the polynomial c is equal to an invertible constant; the result follows because N is the intersection of all prime ideals of R , and every noninvertible element of R is contained in a prime ideal. However, in a paper that generalizes a theorem of Heyting, we should be careful to see that all our proofs are constructive. To this end, suppose that $cd = 1$. We want to show that $c_i \in N$ for all $i > 0$. Suppose we have shown that $c_i \in N$ for all $i > n$. If $n = 0$ we are done, otherwise pass to the ring $S^{-1}R$ where S consists of the powers of c_n . Now c_n is invertible in $S^{-1}R$, and a similar induction on the coefficients of d shows that they are all nilpotent in $S^{-1}R$, so $S^{-1}R$ is trivial because $cd = 1$. Thus a_n is nilpotent.

In the next two theorems we use subscripts to indicate components in a direct product rather than coefficients.

Theorem 9 *Let R be a commutative ring and $a \in R[X]$. The map $T : R[X] \rightarrow R[X]$ given by multiplication by a has a left inverse if and only if $R = R_1 \times \cdots \times R_k$ and, for $i = 1, \dots, k$, the image of a in $R_i[X]$ can be written as $c_i d_i$ where c_i is invertible in $R_i[X]$ and d_i is monic.*

Proof. Let N be the nilradical of R and let \bar{R} denote R/N . First suppose that T has a left inverse. Then so does the map on $\bar{R}[X]$ given by multiplication by a . By Theorem 6 we can write $\bar{R} = \bar{R}_1 \times \cdots \times \bar{R}_k$ and the leading coefficient of \bar{a} over \bar{R}_i is invertible for each i . Because N is the nilradical of R , this decomposition of \bar{R} comes from a decomposition of $R = R_1 \times \cdots \times R_k$ (see, for example, [1, Chapter III, Proposition 2.10]). Let N_i denote the nilradical of R_i . The image of a in $R_i[X]$ has an invertible leading coefficient modulo N_i , so can be written as $c_i d_i$ where c_i is invertible in $R_i[X]$ and d_i is monic by Theorem 8.

Conversely, suppose the second condition of the theorem is satisfied. Then multiplication by the image of a in $R_i[X]$ has a left inverse because multiplication by c_i and d_i do. Putting these inverses together gives a left inverse for the map T . ■

In the following theorem, the statement $\deg r < \deg a$ means that $rX \in R[X]_n$ whenever $a \in R[X]_n$. This formulation obviates the need for deciding

whether or not certain coefficients are zero. It has the feature that $\deg 0 < \deg 0$.

Theorem 10 *Let R be a commutative ring and $a \in R[X]$. Then the following conditions are equivalent:*

1. *For all $b \in R[X]$ there exist $q, r \in R[X]$ such that $b = qa + r$ and $\deg r < \deg a$.*
2. *There exists $q \in R[X]$ such that qa is monic.*
3. *The map $T_a : R[X] \rightarrow R[X]$ given by multiplication by a has a left inverse.*
4. *$R = R_1 \times \cdots \times R_k$ and, for $i = 1, \dots, k$, the image of a in $R_i[X]$ can be written as $a_i = c_i d_i$ where c_i is invertible in $R_i[X]$ and d_i is monic.*

Proof. Suppose (1) holds and $a \in R[X]_n$. Then $X^n = qa + r$ and $\deg r < n$ so $qa = X^n - r$ is monic.

If (2) holds, then the map $T_{qa} = T_q T_a$ has a left inverse because qa is monic, whence so does T_a .

The previous theorem shows that (3) implies (4).

If (4) holds, then in R_i we can write $b_i = qd_i + r_i$ where $\deg r_i < \deg d_i \leq \deg a_i$. So $b_i = (q_i c_i^{-1})a_i + r_i$ with $\deg r_i < \deg a_i$. Then (1) follows. ■

The implication from (2) to (4) was proved by Gilmer and Heinzer in [2] and constructively by Yengui in [6]. I am indebted to Ihsen Yengui for pointing this out to me.

We don't get uniqueness of q and r in (1) if R has nilpotents or idempotents. Indeed, if $u^2 = 0$ then

$$1 = (uX + 1)(uX - 1) = 0 \cdot (uX - 1) + 1,$$

and if $v^2 = v$, then

$$vX = v(vX + 1 - v) = 1 \cdot (vX + 1 - v) + v - 1.$$

To get uniqueness, we could replace the condition on r in (1) by

- $\deg vr < \deg vca$ whenever $c \in R[X]$ is invertible and $v^2 = v \in R$.

Clearly this implies (1) and it is not hard to see that it is implied by (4).

4 An example and a comment

For $a \in R[X]_n$, let $T : R[X] \rightarrow R[X]$ and $T_m : R[X]_m \rightarrow R[X]_{m+n}$ be multiplication by a as before. One way the coefficients of $a \in R[X]_n$ can generate R is for a to be monic; another is for $a(0) = 1$. In the latter case we can use the division algorithm in reverse to write $b = q_m a + r_m X^{m+n+1}$, with q_m a unique element of $R[X]_{m+n}$. If $b = ah$ with $h \in R[X]_m$, then $r_m = 0$, so sending $b \in R[X]_{m+n}$ to q_m gives a left inverse for T_m , which is guaranteed by Theorem 4. On the other hand, if $b = 1$ and $a = 1 - uX$, then $q_m = 1 + uX + u^2 X^2 + \dots + u^{m+n} X^{m+n}$ and $r_m = u^{m+n+1}$ so this technique will not generally construct a left inverse for T . Indeed, if R is an integral domain and $u \neq 0$ is not invertible, then Theorem 6 precludes a left inverse for T .

Finally, I would like to point out that all the proofs given here are constructive, as befits a paper on a generalization of a theorem of Heyting.

References

- [1] BASS, HYMAN, *Algebraic K-theory*, W. A. Benjamin 1968
- [2] GILMER, ROBERT AND WILLIAM HEINZER, On the divisors of monic polynomials over commutative rings, *Pacific J. Math.*, **78** (1978), 121–123.
- [3] HEYTING, AREND, Untersuchungen über intuitionistische Algebra, *Verhandelingen Akad. Amsterdam*, eerste sectie **18** (1941) 1–36.
- [4] JACOBSON, NATHAN, *Basic Algebra*, W. H. Freeman 1974.
- [5] MINES, RAY, FRED RICHMAN AND WIM RUITENBURG, *A course in constructive algebra*, Springer-Verlag, 1988.
- [6] YENGUI, IHSEN, An algorithm for the divisors of monic polynomials over a commutative ring, *Math. Nachr.*, **260** (2003), 1–7.