The American Mathematical Monthly

ISSN: 0002-9890 (Print) 1930-0972 (Online) Journal homepage: http://www.tandfonline.com/loi/uamm20

What Happens When the Division Algorithm “Almost” Works

Scott T. Chapman

To cite this article: Scott T. Chapman (2018) What Happens When the Division Algorithm “Almost” Works, The American Mathematical Monthly, 125:7, 643-647, DOI: 10.1080/00029890.2018.1470414

To link to this article: https://doi.org/10.1080/00029890.2018.1470414

Published online: 03 Aug 2018.

What Happens When the Division Algorithm "Almost" Works

Scott T. Chapman

Abstract. Let K be any field. The division algorithm plays a key role in studying the basic algebraic structure of $K[X]$. While the division algorithm implies that all the ideals of $K[X]$ are principal, we show that subrings of $K[X]$ satisfying a slightly weaker version of the division algorithm produce ideals that while not principal, are still finitely generated. Our construction leads to an example for each positive integer n of an integral domain with the n, but not the $n-1$, generator property.

Dedicated to the Memory of Nick Vaughan

Central in a first abstract algebra course is the notion of the division algorithm. Indeed, a first abstraction for students studying ring theory is moving from the standard division algorithm over $\mathbb{Z}$ (the integers) to a similar statement for a polynomial ring over a field. The result below can be found in any standard abstract algebra text (such as [4] or [6]).

The Division Algorithm. *Let K be a field and $K[X]$ the polynomial ring over K. If $f(X)$ and $g(X)$ are in $K[X]$ with $g(X) \neq 0$, then there exist unique polynomials $q(X)$ and $r(X)$ in $K[X]$ such that*

$$f(X) = g(X)q(X) + r(X)$$

and either $r(X) = 0$ or $\deg r(X) < \deg g(X)$.

A simple application of the division algorithm shows that ideals in $K[X]$ are principal (i.e., generated by one element). While many introductory textbooks give an example to show that not all ideals are principal (a popular one is $I = (2, X)$ in $\mathbb{Z}[X]$), most books do not go into great detail describing ideal generation problems. In this note, we consider a natural class of subrings of $K[X]$, namely those subrings R with $K \subseteq R \subseteq K[X]$. We show that if such R satisfy a weaker form of the division algorithm, then we can not only bound the number of generators of an ideal I of R, but also offer examples of ideals that can be generated by n, but not $n-1$ elements. We describe this weaker algorithm below.

Definition – The Almost Division Algorithm. A subring R of $K[X]$, with $K \subseteq R$, has an *almost division algorithm of index m* (where $m \in \mathbb{N}$) if it satisfies the following property. If $f(X)$ and $g(X)$ are in R with $g(X) \neq 0$, then there exist polynomials $h(X)$ and $r(X)$ in R such that

$$f(X) = h(X)g(X) + r(X)$$

where

(d1) $r(X) = 0$,

(d2) $\deg r(X) < \deg g(X)$, or

(d3) $\deg r(X) = \deg g(X) + i$ for $1 \leq i \leq m$.

doi.org/10.1080/00029890.2018.1470414

MSC: Primary 13B25

A more general approach to rings and semirings satisfying an almost division algorithm can be found in [11] and [12].

Before proceeding, we note that various arguments can be used to show that the K-subalgebra R of $K[X]$ is finitely generated and Noetherian (see for instance [13]). An in-depth look at computing generating sets for a particular R can be found in [1]. Also, we deal exclusively here with the one variable case, as with multiple variables (such as $K \subseteq R \subseteq K[X, Y]$), the subring R may not be Noetherian. The almost division algorithm leads directly to a proof of the following.

Theorem 1. *Let R be a subring of $K[X]$ with an almost division algorithm of index m and I a proper ideal of R. There exist polynomials $f_1(X), f_2(X), \ldots, f_{m+1}(X)$ such that*

$$I = (f_1(X), f_2(X), \ldots, f_{m+1}(X)).$$

Thus, R has the $m + 1$ generator property on ideals.

Proof. Let I be a proper ideal of R. If d is the minimal degree of a polynomial in I, then for each i with $0 \leq i \leq m$, choose a polynomial $t_{d+i}(X) \in I$ with $\deg t_{d+i}(X) = d + i$. (If I does not contain a polynomial of such degree, then set $t_{d+i}(X) = 0$.) Setting

$$J = (t_d(X), t_{d+1}(X), \ldots, t_{d+m}(X)),$$

we will prove that $I = J$. Clearly $J \subseteq I$. We prove the reverse containment.

Let $f(X)$ be an arbitrary nonzero element of I. Since S has an almost division algorithm of index m,

$$f(X) = h(X)t_d(X) + r(X)$$

where $r(X)$ satisfies (d1), (d2), or (d3). Option (d2) cannot hold, as otherwise $r(X) \in I$ contradicts the minimality of d. If (d1) holds, then $f(X) \in J$.

Now suppose (d3) holds. Then $\deg r(X) = d + i$ for some $1 \leq i \leq m$. Now $\deg t_{d+i}(X) = \deg r(X)$ and so there is a $k \in K$ with $r(X) = kt_{d+i}(X) + r_1(X)$ where either (d1) or (d2) holds. If (d1) holds, then $f(X) = h(X)t_d(X) + kt_{d+i}(X) \in J$. If (d2) holds, then $r_1(X) \in I$ with $d \leq \deg r_1(X) < d + i$. Repeat this process on $r_1(X)$ with the polynomial $t_{\deg r_1(X)}$ and obtain the remainder term $r_2(X)$. Since the degrees of the remainder terms are strictly descending ($\deg r(X) > \deg r_1(X) > \deg r_2(X) > \cdots$), this process must terminate and we have inductively constructed a finite sequence $\{r_0(X) = r(X), r_1(X), \ldots, r_N(X)\}$ of remainders. Notice that $f(X) = h(X)t_d(X) + \sum k_n t_{\deg r_n(X)}(X)$ where each $k_n \in K$ and hence $f(X) \in I$. Thus $I \subset J$ and the proof is complete. ■

We apply Theorem 1 to a well-studied class of subrings of $K[X]$. We will need the notion of a numerical semigroup to complete our work. Let $\mathbb{N}_0$ represent the non-negative integers. An additive submonoid S of $\mathbb{N}_0$ is called a numerical monoid. Using elementary number theory, it is easy to show that there is a finite set of positive integers $n_1, \ldots, n_k$ such that if $s \in S$, then $s = x_1n_1 + \cdots + x_kn_k$ where each x_i is a nonnegative integer. To represent that $n_1, \ldots, n_k$ is a generating set for S, we use the notation

$$S = \langle n_1, \ldots, n_k \rangle = \{x_1n_1 + \cdots + x_kn_k \mid x_i \in \mathbb{N}_0\}.$$

If the generators $n_1, \ldots, n_k$ are relatively prime, then S is called *primitive*. We shall need the following three facts concerning numerical semigroups. The proofs of all three can be found in [14] (part (a) is Proposition 1.2, (b) is Theorem 1.7, and (c) is a by-product of Lemma 1.1).

Proposition 2. *Let $S = \langle n_1, \ldots, n_k \rangle$ be a numerical semigroup.*

(a) S is isomorphic to a primitive numerical semigroup S'.

(b) S has a unique minimal cardinality generating set.

(c) If S is a primitive numerical semigroup, then there is a largest element $\mathcal{F}(S) \notin S$ with the property that any $s > \mathcal{F}(S)$ is in S.

Due to (a), we assume that S is primitive throughout the remainder of this work. The value $\mathcal{F}(S)$ is known as the Frobenius number of S and its computation remains a matter of current mathematical research. If $S = \langle a, b \rangle$, then it is well known that $\mathcal{F}(S) = ab - a - b$ (see [15]), but for more than 2 generators, no general formula is known (see [14, Section 1.3] for more on Frobenius numbers).

Now, if K is a field and S a numerical semigroup, then set

$$K[X; S] = \{f(X) \mid f(X) \in K[X] \text{ and } f(X) = \sum_{\sigma \in S} a_i X^{\sigma}\},$$

where it is understood that the sum above is finite. The rings $K[X; S]$ are known as *semigroup rings*, and [5] is a good general reference on the subject. Under our hypotheses, the rings $K[X; S]$ consist of all polynomials with exponents coming from the numerical monoid S. We illustrate this with some examples.

Example 3. Let $S = \langle 3, 7, 11 \rangle$. A quick calculation shows that

$$S = \{0, 3, 6, 7, 9, 10, 11, \ldots\}$$

and $\mathcal{F}(S) = 8$. Hence, a typical element in $K[X; \langle 3, 7, 11 \rangle]$ is of the form

$$f(X) = a_0 + a_3 X^3 + a_6 X^6 + a_7 X^7 + \sum_{i=9}^{k} a_i X^i$$

for some $k \geq 9$ with each a_i in K.

Example 4. Let $S = \langle 2, 3 \rangle$. Thus $S = \{0, 2, 3, 4, 5, \ldots\}$ and a typical element of $K[X; \langle 2, 3 \rangle]$ is of the form $f(X) = a_0 + \displaystyle\sum_{i=2}^{k} a_i X^i$ for some $k \geq 2$ with each a_i in K. Thus, $K[X; \langle 2, 3 \rangle]$ consists of all polynomials from $K[X]$ which lack an X term. A version of Theorem 5 below specifically for $K[X; \langle 2, 3 \rangle]$ can be found in [16].

We can generalize the last example as follows. Let $n > 1$ be a positive integer and set $S = \langle n, n+1, \ldots, 2n-1 \rangle$. Notice that S consists of 0 along with all positive integers greater than or equal to n. Thus, a typical element in $K[X; \langle n, n+1, \ldots, 2n-1 \rangle]$ is of the form $f(X) = a_0 + \sum_{i=n}^{k} a_i X^i$ where $k \geq n$ and again each a_i is in K.

As the last examples make clear, if $S = \langle n_1, \ldots, n_k \rangle$ is a numerical semigroup, then the semigroup ring $K[X; S]$ is equivalent to the extension of K by the monomial terms $X^{n_1}, \ldots, X^{n_k}$ (i.e., $K[X; S] \cong K[X^{n_1}, \ldots, X^{n_k}]$).

Theorem 5. *If K is a field and S a numerical semigroup, then $K[X; S]$ has an almost division algorithm of index $\mathcal{F}(S)$.*

Proof. Let $f(X)$ and $g(X)$ be in $K[X; S]$ with $g(X) \neq 0$; we will divide $f(X)$ by $g(X)$ and verify that either (d1), (d2), or (d3) holds. If $\deg f(X) < \deg g(X)$, then the result is trivial. Hence, we assume $\deg f(X) \geq \deg g(X)$. By the regular division algorithm in $K[X]$, there exist $h(X)$ and $r(X)$ in $K[X]$ with

$$f(X) = h(X)g(X) + r(X)$$

where $r(X) = 0$ or $\deg r(X) < \deg g(X)$. If $h(X) \in K[X; S]$, then $r(X) \in K[X; S]$ and we are done. If not, then write

$$h(X) = \sum_{\gamma \notin S} a_\gamma X^\gamma + \sum_{\sigma \in S} a_\sigma X^\sigma.$$

Setting $h^*(X) = \sum_{\gamma \notin S} a_\gamma X^\gamma$ yields that $h^{**}(X) = h(X) - h^*(X)$ is in $K[X; S]$. If $r^*(X) = h^*(X)g(X) + r(X)$, then we have

$$\begin{aligned} f(X) &= h(X)g(X) + r(X) \\ &= [h(X) - h^*(X)]g(X) + [h^*(X)g(X) + r(X)] \\ &= h^{**}(X)g(X) + r^*(X). \end{aligned}$$

Since $f(X) - h^{**}(X)g(X) \in K[X; S]$, it follows that so too is $r^*(X)$. Since $\deg g(X) < \deg r^*(X) \leq \deg g(X) + \mathcal{F}(S)$, the proof is complete. ■

By a slight adjustment of $h^*(X)$ in the proof above, we see that the representation (d3) in the almost division algorithm may not be unique. For instance, returning to Example 4, if $S = \langle 2, 3 \rangle$, $f(X) = X^3$, and $g(X) = X^2$, then $X^3 = 0 \cdot X^2 + X^3$ and $X^3 = (-1) \cdot X^2 + (X^3 + X^2)$. The next corollary follows directly from Theorems 1 and 5.

Corollary 6. *If K is a field and S a numerical semigroup, then the ideals of $K[X; S]$ require at most $\mathcal{F}(S) + 1$ generators.*

A Noetherian integral domain in which the ideals can be n-generated is said to have the *n-generator property*. If an integral domain D has the n-generator property for some $n \in \mathbb{N}$, then it has it has the m-generator property for some minimal value $m \in \mathbb{N}$. Dedekind domains (a very natural class of rings that are ubiquitous in algebraic number theory and algebraic geometry) are generally not principal ideal domains, but they always have the 2-generator property (a proof of this can be found in [**7**, Theorem 17]). While Corollary 6 shows that $K[X; S]$ has the $\mathcal{F}(S) + 1$ generator property, this value may not be minimal, and in fact is not sharp for all S. Using semigroup ideals, a precise minimal value can be found (the interested reader can construct examples for which our bound is not sharp by using [**2**, Corollary 7] or [**10**]). Further reading on rings with the n-generator property can be found in [**3**], [**8**], and [**9**].

We close by showing that the value of Corollary 6 is sharp for the numerical semigroups introduced in Example 4.

Proposition 7. *Let K be a field, $n > 1$ a positive integer, and $S = \langle n, n+1, \ldots, 2n-1 \rangle$ a numerical semigroup. The integral domain $K[X; S]$ has the n, but not the $n-1$ generator property.*

Proof. Since $\mathcal{F}(S) = n - 1$, Corollary 6 implies that $K[X; S]$ has the n-generator property. We argue that the ideal

$$I = (X^n, X^{n+1}, \ldots, X^{2n-1})$$

requires n generators. The argument will center around the K-vector space V generated by $X^n, \ldots, X^{2n-1}$. Since the elements $X^n, \ldots, X^{2n-1}$ are linearly independent over K, V has dimension n.

Suppose $I = (f_1(X), \ldots, f_k(X))$ where each $f_i(X) \in K[X; S]$ and $k < n$. Since I contains no elements with nonzero constant terms, the constant terms on the $f_i(X)$'s are all zero. For each $i = 1, \ldots, k$ define $f_i'(X)$ by

$$f_i(X) = a_{1,i}X^n + \cdots + a_{n,i}X^{2n-1} + \sum_{j=2n}^{r_i} a_{j,1}X^j = f_i'(X) + \sum_{j=2n}^{r_i} a_{j,1}X^j$$

for $1 \leq i \leq k$ where each $a_{i,j} \in K$. By assumption, for each $0 \leq \upsilon \leq n-1$,

$$X^{n+\upsilon} = C_{1,\upsilon}(X)f_1(X) + \cdots + C_{k,\upsilon}(X)f_k(X)$$

where each $C_{j,\upsilon}(X) \in K[X; S]$. If $c_{j,\upsilon}$ is the constant term for each $C_{j,\upsilon}(X)$, then a simple degree argument yields

$$X^{n+\upsilon} = c_{1,\upsilon}f_1'(X) + \cdots + c_{k,\upsilon}f_k'(X)$$

for each $0 \leq \upsilon \leq n-1$. Thus the K-vector space generated by $f_1'(X), \ldots, f_k'(X)$ contains V, which contradicts that $\dim V = n$. ■

ACKNOWLEDGMENTS. The author would like to thank Susan Colley, Vadim Ponomarenko, and two unknown referees for comments that greatly improved the content and exposition of this note.

REFERENCES

[1] Assi, A., García-Sánchez, P. A., Micale, V. (2017). Bases of subalgebras of $K[[x]]$ and $K[x]$. *J. Symbolic Comput.* 79: 4–22.

[2] Chapman, S. T., Vaughan, N. (1991). A theorem on generating ideals in certain semigroup rings. *Boll. Un. Mat. Ital. A (7)*. 5(1): 41–49.

[3] Clark, P. (2016). A note on rings of finite rank. arxiv.org/pdf/1605.01305.pdf

[4] Gallian, J. (2016). *Contemporary Abstract Algebra*, 9th ed. Boston: Cengage Learning.

[5] Gilmer, R. (1984). *Commutative Semigroup Rings*. Chicago: Univ. of Chicago Press.

[6] Hungerford, T. (2013). *Abstract Algebra: An Introduction*, 3rd ed. Boston: Cengage Learning.

[7] Marcus, D. (1977). *Number Fields*. New York: Springer.

[8] Matson, A. (2009). Rings of finite rank and finitely generated ideals. *J. Commut. Algebra.* 1(3): 537–546.

[9] Matsuda, R. (1979). Torsion free abelian semigroup rings, V. *Bull. Fac. Sci. Ibaraki Univ. Ser. A.* 11: 1–37.

[10] Matsuda, R. (1984). n-Generator property of a polynomial ring. *Bull. Fac. Sci. Ibaraki Univ. Ser. A.* 16: 17–23.

[11] Mehdi-Nezhad, E., Rahimi, A., (2009). Semirings with an almost division algorithm. *Libertas Math.* 29: 129–137.

[12] Rahimi, A. (1993). Rings with an almost division algorithm. *Libertas Math.* 13: 41–46.

[13] Robbiano, L., Sweedler, M. (1990). Subalgebra bases. In: Bruns, W. and Simis, A., eds. *Commutative Algebra (Salvador 1988)*. New York: Springer, pp. 61–87.

[14] Rosales, J. C., García-Sánchez, P. A. (2009). *Numerical Semigroups*. Developments in Mathematics, 20. New York: Springer.

[15] Sylvester, J. (1884). Mathematical questions with their solutions. *Educational Times*. 41: 171–178.

[16] Vaughan, N. (1981). An integral domain with an almost division algorithm. *J. Nat. Sci. Math.* 21(1): 81–83.

Department of Mathematics and Statistics, Sam Houston State University, Box 2206, Huntsville, TX 77341
scott.chapman@shsu.edu