ON POLYNOMIAL RINGS WITH A GOLDBACH PROPERTY

PAUL POLLACK

Abstract. David Hayes observed in 1965 that when $R = \mathbf{Z}$, every element of $R[T]$ of degree $n \geq 1$ is a sum of two irreducibles in $R[T]$ of degree n. We show that this result continues to hold for any Noetherian domain R with infinitely many maximal ideals.

It appears that David Hayes [5] was the first to observe the following polynomial analogue of the celebrated Goldbach conjecture: If $R = \mathbf{Z}$, then

($\star$) $\boxed{\text{every element of } R[T] \text{ of degree } n \geq 1 \text{ can be written as the sum of two irreducibles of degree } n.}$

His proof is a clever application of Eisenstein's irreducibility criterion. Hayes's theorem and its proof were rediscovered by Rattan and Stewart [10] (see also [1] for some cognate results). Recently Saidak [11] and Kozek [7] have considered quantitative variants of Hayes's theorem. The latter shows that in a precise asymptotic sense, for a given monic polynomial $A(T) \in \mathbf{Z}[T]$ of degree $n \geq 2$, almost all (100%) of its representations as a sum of two monic polynomials are such that both summands are irreducible.

In this note we consider a generalization in a different direction. Namely, we investigate which integral domains R have the property ($\star$). In [5], Hayes points out that his proof shows that ($\star$) holds whenever R is a principal ideal domain with infinitely many maximal ideals, and so in particular for the polynomial ring $F[x]$ with F an arbitrary field. Here we show how to relax the requirement that R be a PID to the much weaker condition that the ideals of R are finitely generated.

Theorem 1. *Suppose that R is an integral domain which is Noetherian and has infinitely many maximal ideals. Then R has property ($\star$).*

The condition that R be Noetherian cannot be removed. To illustrate, let R be the ring of all algebraic integers, i.e., the collection of all complex numbers which are roots of some monic polynomial with integer coefficients. It is known that over R, there are no irreducible polynomials of degree $n > 1$; in fact, as is nicely explained in (e.g.) [8], every nonconstant polynomial in $R[x]$ can be written as a product of linear factors. However, there are certainly infinitely many maximal ideals of R: Indeed, for every (positive) prime p of $\mathbf{Z}$, Zorn's lemma implies the existence of a maximal ideal of R containing (p) (see [2, p. 254]), and distinct primes p correspond to distinct maximal ideals. The condition that R contain infinitely many maximal ideals also cannot be dispensed with (e.g., take R to be your favorite algebraically closed field), but can perhaps be relaxed beyond what is obvious from the proof below; it would be interesting to investigate this further.

The proof of Theorem 1 is a nice application of the commutative ring theory seen in an introductory graduate algebra course. As a corollary of the proof (but not Theorem 1 as stated), we have the following:

Theorem 2. *If S is any integral domain, then $R = S[x]$ has property ($\star$).*

In their proof of ($\star$) for $R = \mathbf{Z}$, Hayes as well as Rattan and Stewart appear to use 'irreducible' to mean 'irreducible over $\mathbf{Q}$'; so, e.g., $2T$ is considered irreducible. Throughout this paper, we use 'irreducible' in its usual ring-theoretic sense: An element of $R[T]$ is *irreducible* if it is not a unit and cannot be factored as a product of two nonunits. So (strictly speaking) even in the case $R = \mathbf{Z}$, our result is stronger than that asserted by previous authors.

1. The basic argument.

We begin by stating our version of Eisenstein's criterion.

Lemma 3 (Eisenstein's criterion). *Let P be a prime ideal of the integral domain R. Suppose $A(T) = a_n T^n + \cdots + a_1 T + a_0 \in R[T]$ is a nonconstant polynomial whose coefficients satisfy the following three conditions:*

(i) *$a_0, a_1, \ldots, a_{n-1}$ are all contained in P,*
(ii) *a_0 is not contained in P^2,*
(iii) *a_n is not contained in P.*

Moreover, suppose that A is a primitive *polynomial, in the sense that*

(iv) *the coefficients a_i generate the unit ideal, i.e., $(a_0, \ldots, a_n) = R$.*

Then A is irreducible over R.

Proof (sketch). The proof follows the familiar argument for Eisenstein's criterion where one passes to the domain R/P; see, e.g., [2, p. 611]. Conditions (i)-(iii) guarantee that A has no decomposition of the form $G(T)H(T)$ where $G(T)$ and $H(T)$ are nonconstant. Finally, condition (iv) implies that every constant polynomial dividing A is a unit in R (and so in $R[T]$). $\square$

Hayes's argument in [5] utilizes a familiar result from the foundations of number theory: If m and n are relatively prime integers, then there is a solution in integers x and y to the equation $mx + ny = 1$. One can view this as a result about the solvability of simultaneous linear congruences: Given x and y with $mx + ny = 1$, the integer $a = mx$ solves the simultaneous congruences $a \equiv 0 \pmod{m}$ and $a \equiv 1 \pmod{n}$. Conversely, given a solution a to these congruences, we obtain an integral solution of $mx + ny = 1$ by setting $a = mx$ and solving for x and y.

When are we guaranteed the existence of a solution to a system of simultaneous congruences? One answer is given by the Chinese Remainder Theorem, a ring-theoretic version of which we quote here (for a proof, see, e.g., [2, p. 265]). Recall that two ideals I and J of a commutative ring R are said to be *comaximal* if $I + J = R$.

Chinese Remainder Theorem for commutative rings. *Let R be a commutative ring containing ideals $I_1, \ldots, I_k$. Suppose that for every pair of i and j with $i \neq j$, the ideals I_i and I_j are comaximal. Then the map*

$$\begin{aligned} R &\to R/I_1 \times \cdots \times R/I_k \\ r &\mapsto (r \bmod I_1, \ldots, r \bmod I_k) \end{aligned}$$

is a surjective homomorphism with kernel $I_1 \cap \cdots \cap I_k$. Moreover, $I_1 \cap \cdots \cap I_k = I_1 I_2 \cdots I_k$, so that

$$R/(I_1 \cdots I_k) = R/(I_1 \cap \cdots \cap I_k) \cong R/I_1 \times \cdots \times R/I_k.$$

To apply this result, one needs to know that certain pairs of ideals are comaximal. An easy observation is that if I is a maximal ideal and J is an ideal not contained in I, then I and J are comaximal. (Otherwise $I \subsetneq I+J \subsetneq R$, contradicting the maximality of I.) Apart from this, the only property of comaximality we need is its preservation upon taking powers:

Lemma 4. *Suppose that I and J are comaximal ideals. Then for any positive integers m and n, the ideals I^m and J^n are comaximal.*

Proof. Since I and J are comaximal, one can pick $a \in I$ and $b \in J$ with $a+b=1$. By the binomial theorem,

$$(a+b)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} a^k b^{m+n-k}.$$

If $k \geq m$, the kth term of the sum is divisible by a^m, and so belongs to I^m. If $k < m$, then $m+n-k > n$, and so the kth term is divisible by b^n and therefore belongs to J^n. Hence $1 = (a+b)^{m+n}$ belongs to $I^m + J^n$. Consequently, I^m and J^n are comaximal. □

We now prove, by Hayes's method, a somewhat technical general result from which we will deduce both Theorems 1 and 2.

Theorem 5. *Suppose that R is an integral domain possessing distinct maximal ideals P and Q for which the following hold:*

(i) *$P^2 \neq P$ and $Q^2 \neq Q$,*
(ii) *$\#R/P > 2$ and $\#R/Q > 2$.*

Then R has property $(\star)$.

Proof. Let $A(T) = \sum_{j=0}^{n} a_j T^j \in R[T]$ be given, where A has degree $n \geq 1$.

Suppose first that $n=1$, so that $A(T) = a_1 T + a_0$. If $a_1 \neq 1$, then $A(T) = ((a_1-1)T + 1) + (T + a_0 - 1)$ is a decomposition of the desired form. If $n=1$ and $a_1 = 1$, then by a change of variables, we can assume $A(T) = T$. Then picking $r \in R$ with $r \notin \{0,1\}$, we have the decomposition $T = (rT+1) + ((1-r)T - 1)$.

Suppose now that $n \geq 2$. We will find degree-n polynomials $B = \sum_{i=0}^{n} b_i T^i$ and $C = \sum_{i=0}^{n} c_i T^i$ satisfying $A = B + C$, where B and C satisfy the conditions of Eisenstein's criterion (Lemma 3). It is enough to describe how to choose the b_i, since clearly $c_i = a_i - b_i$. Using hypothesis (i), fix $p \in P \setminus P^2$ and $q \in Q \setminus Q^2$. Using the Chinese Remainder Theorem and Lemma 4, pick the coefficients b_i to satisfy the congruences

$$b_i \equiv 0 \pmod{P}, \quad c_i \equiv 0 \pmod{Q} \quad \text{for } i = 1, 2, \dots, n-1,$$

$$b_0 \equiv p \pmod{P^2}, \quad c_0 \equiv q \pmod{Q^2},$$

$$b_n \not\equiv 0 \pmod{P}, \quad c_n \not\equiv 0 \pmod{Q}.$$

(Here a congruence on c_i is to be interpreted as a congruence on b_i, via the relation $b_i + c_i = a_i$.) Then B satisfies conditions (i)–(iii) of Lemma 3 with respect to P, and C satisfies these conditions with respect to Q.

To ensure that (iv) is satisfied, we amend the construction somewhat. In addition to the constraints imposed on the b_i above, we add that

$$c_n \not\equiv 0 \pmod{P} \quad \text{and} \quad b_n \not\equiv 0 \pmod{Q};$$

since $\#R/P > 2$ and $\#R/Q > 2$, this is permissible. Fix $b_2, \ldots, b_n$ satisfying all of the congruence conditions specified above. Now choose b_0 to satisfy all the above and the additional congruence

$$b_0 \equiv 1 \pmod{b_n}. \tag{1}$$

To see that this is possible, notice that we now have congruence conditions on b_0 with respect to the moduli P^2, Q^2 and (b_n); since we have specified above that b_n is in neither P nor Q, these three moduli are pairwise comaximal (again, we appeal to Lemma 4). Similarly, we can choose b_1 satisfying all the congruences given above as well as

$$c_1 \equiv 1 \pmod{c_n}. \tag{2}$$

From (1) we have that b_0 and b_n generate the unit ideal, and from (2) we get the same for c_1 and c_n. In particular, we have secured condition (iv) of Lemma 3. □

2. Proof of Theorem 1.

In this section we show that any Noetherian domain with infinitely many maximal ideals satisfies the hypotheses of Theorem 5 and thus has property ($\star$). The first lemma shows that if R is a Noetherian domain, then condition (i) of Theorem 5 is satisfied for all nonzero P and Q.

Lemma 6. *If R is a Noetherian domain and M is a nonzero maximal ideal, then $M^2 \neq M$.*

Proof. Since R is Noetherian and $M \neq 0$, we can choose nonzero generators $g_1, \ldots, g_k$ for M, where k is a positive integer. Suppose that $M^2 = M$. Since each $g_i \in M = M^2$, we can write

$$g_i = \sum_{j=1}^{k} m_{ij} g_j \quad \text{for} \quad 1 \leq i \leq k, \quad \text{where each} \quad m_{ij} \in M.$$

The matrix $(m_{ij}) - \mathrm{Id}$ kills the column vector $[g_1, \ldots, g_k]^T$. But the determinant of this matrix is congruent to $\pm 1 \pmod{M}$; in particular, it is nonvanishing, so that the matrix is invertible over the quotient field of R. So we have an invertible matrix killing a nonzero vector, an absurdity. □

The next lemma shows that if R is a Noetherian domain with infinitely many maximal ideals M, then infinitely many of these M have $\#R/M > 2$.

Lemma 7. *Let R be a Noetherian ring. Then R has only finitely many maximal ideals M with $\#R/M = 2$.*

Clearly Theorem 1 follows from Theorem 5 and Lemmas 6 and 7.

Proof. Let J be the intersection of all maximal ideals M of R for which $\#R/M = 2$. We will show that $S := R/J$ is finite. Hence there are only finitely many ideals of S, and so by the lattice isomorphism theorem, also only finitely many ideals of R containing J. Since each M contains J, we obtain the lemma.

Let us show that S has the property that each of its prime ideals is maximal, with corresponding residue field $\mathbf{Z}/2\mathbf{Z}$. Suppose $x \in R$. Since $R/M \cong \mathbf{Z}/2\mathbf{Z}$, we have that $x^2 - x \in M$ for all M, and hence $x^2 - x \in \cap M = J$. So in $S = R/J$, every element is idempotent (i.e., S is a *Boolean ring*). It follows that the same is true for every quotient of S. In particular, if P is a prime ideal of S, then S/P is a domain where every element satisfies $x^2 - x = 0$; the field $\mathbf{Z}/2\mathbf{Z}$ is the only such domain.

Since S is Noetherian, every ideal of S contains a product of prime ideals [2, p. 685]. Applying this to the zero ideal, we find that $(0) = P_1^{e_1} P_2^{e_2} \cdots P_k^{e_k}$ for distinct prime ideals $P_1, \dots, P_k$ of S. Since each P_i is maximal, the Chinese Remainder Theorem and Lemma 4 give that $S \cong S/(0) \cong \prod_{i=1}^k S/P_i^{e_i}$. Since each element of S is idempotent, none of the rings $S/P_i^{e_i}$ can have nonzero nilpotent elements. This forces $P_i^{e_i} = P_i$ for each i, yielding that $S \cong \prod_{i=1}^k S/P_i \cong (\mathbf{Z}/2\mathbf{Z})^k$. □

With a bit of effort, one can tweak the proof of Lemma 7 to show that for any Noetherian ring R and any constant B, there are only finitely many ideals I of R with $\#R/I \leq B$. This argument is due to Samuel [12, p. 292].

3. Proof of Theorem 2.

It suffices to verify that $R = S[x]$ satisfies the two conditions of Theorem 5. Fix a maximal ideal M of S and let K denote the field S/M. The ring $K[x]$ contains infinitely many monic irreducibles; one can see this by mimicking the usual Euclidean proof that there are infinitely many primes. Each such irreducible has the form $\overline{I}$, where $I \in S[x]$ is monic, and $\overline{I}$ signifies that the coefficients are reduced modulo M. We have an isomorphism

$$S[x]/(M, I(x)) \cong K[x]/(\overline{I}),$$

which shows that $(M, I(x))$ is a maximal ideal of $S[x]$. Moreover, any two distinct monic irreducibles $\overline{I}$ generate the unit ideal of $K[x]$, and so correspond to distinct maximal ideals $(M, I(x))$ of $S[x]$. Note that the above isomorphism shows that the quotient of $S[x]$ by $(M, I(x))$ has size > 2 provided either that K is infinite or that $\overline{I}$ has degree at least two; in particular, regardless of the size of K, there are always infinitely many choices of I for which the quotient has size > 2.

Now let monic polynomials I_1 and I_2 in $S[x]$ be chosen so that $\overline{I}_1, \overline{I}_2$ are distinct irreducibles over K, and so that $P := (M, I_1(x))$ and $Q := (M, I_2(x))$ have residue fields with more than two elements. To see that $P^2 \neq P$, note that the elements of P are exactly those elements of $S[x]$ whose reductions modulo M are divisible by $\overline{I}_1$ over K. So every element of P^2, after reduction modulo M, is congruent to a multiple of $\overline{I}_1^2$. Since $\overline{I}_1^2$ does not divide $\overline{I}_1$ in $K[x]$, we see that $I_1 \notin P^2$, so that $P^2 \neq P$. Similarly, $Q^2 \neq Q$.

4. Concluding remarks.

Theorem 1 does not directly comment on the case when $R = F$ is a field, since in that case (0) is the only maximal ideal. However, if F is the quotient field of a unique factorization domain R satisfying the conditions of Theorem 1, then 'Gauss's lemma' [2, p. 303] shows that $(\star)$ holds. At a much deeper level, we have the investigations into the Hilbert irreducibility theorem (see [13, §4.4]), from which we may deduce that $(\star)$ holds if $R = F$ and F is any infinite finitely generated field.

If we ask what happens when $R = F$ is a finite field, then we are quickly led to interesting open problems. Suppose first that $\#F > 2$. Here one expects that every element of $F[T]$ can be written as a sum of two irreducibles, and that for elements of sufficiently large degree (larger than an absolute constant), the summands can be taken to be of the same degree as F. However, for all anyone knows, proving this may be as difficult as resolving the classical

Goldbach conjecture. Just as in the classical situation, the expected results *are* known for sums of three irreducibles; see [6], [3], and the survey [4]. The situation is similar for $F = \mathbf{Z}/2\mathbf{Z}$, but now congruence obstructions modulo the primes T and $T+1$ of $F[T]$ must be taken into account. For a precise discussion of these issues, see [9].

Acknowledgements

The author is supported by an NSF postdoctoral research fellowship. He would also like to thank Carl Pomerance and the referees for suggestions that helped make this note more readable.

References

[1] C. Betts, Additive and subtractive irreducible monic decompositions in $\mathbf{Z}[x]$, *C. R. Math. Acad. Sci. Soc. R. Can.* **20** (1998) 86–90.
[2] D. S. Dummit and R. M. Foote, *Abstract algebra*, third ed., John Wiley & Sons, Hoboken, NJ, 2004.
[3] G. Effinger and D. R. Hayes, A complete solution to the polynomial 3-primes problem, *Bull. Amer. Math. Soc. (N.S.)* **24** (1991) 363–369.
[4] G. Effinger, K. Hicks, and G. L. Mullen, Integers and polynomials: comparing the close cousins $\mathbf{Z}$ and $\mathbf{F}_q[x]$, *Math. Intelligencer* **27** (2005) 26–34.
[5] D. R. Hayes, A Goldbach theorem for polynomials with integral coefficients, this Monthly **72** (1965) 45–46.
[6] ———, The expression of a polynomial as a sum of three irreducibles, *Acta Arith.* **11** (1966) 461–488.
[7] M. Kozek, An asymptotic formula for Goldbach's conjecture with monic polynomials in $\mathbf{Z}[x]$, this Monthly **117** (2010) 365–369.
[8] A. Magidin and D. McKinnon, Gauss's lemma for number fields, this Monthly **112** (2005).
[9] P. Pollack, The exceptional set in the polynomial Goldbach problem, *Int. J. Number Theory*, to appear. Preprint available from `http://www.math.illinois.edu/~pppollac/`.
[10] A. Rattan and C. Stewart, Goldbach's conjecture for $\mathbf{Z}[x]$, *C. R. Math. Acad. Sci. Soc. R. Can.* **20** (1998) 83–85.
[11] F. Saidak, On Goldbach's conjecture for integer polynomials, this Monthly **113** (2006) 541–545.
[12] P. Samuel, About Euclidean rings, *J. Algebra* **19** (1971) 282–301.
[13] A. Schinzel, *Polynomials with special regard to reducibility*, Encyclopedia of Mathematics and its Applications, vol. 77, Cambridge University Press, Cambridge, 2000.

Department of Mathematics, University of Illinois at Urbana-Champaign, 1409 West Green Street, Urbana, Illinois 61801
E-mail address: `pppollac@illinois.edu`