THE IDEAL OF POLYNOMIALS VANISHING ON A COMMUTATIVE RING

Robert Gilmer

Abstract. We determine equivalent conditions on a commutative Artinian ring S in order that the ideal of $S[t]$ consisting of polynomials that vanish on S should be principal. Our results correct an error in a paper of Niven and Warren.

Let R be a commutative unitary ring. If $f(t) = \sum_{j=0}^{n} a_j t^j \in R[t]$, then f induces a polynomial function T_f of R into R defined by $T_f(r) = \sum_{j=0}^{n} a_j r^j$. The map $f \rightarrow T_f$ is a surjective homomorphism of $R[t]$ onto the ring $\mathcal{P}(R)$ of all polynomial functions of R into R. Following Narkiewicz [N, p.1], we denote by I_R the kernel of this map. Thus $I_R = \{f \in R[t] \mid T_f = 0\}$; I_R is called the *ideal of polynomials that vanish on* R. In [NW], Niven and Warren determine a set of generators for I_R in the case where $R = \mathbb{Z}/m\mathbb{Z}$ is the ring of integers modulo m, and for this ring they use the notation $\mathcal{I}(m)$ instead of I_R. Exercise 1, page 10, of [N] states that $\mathcal{I}(m)$ is principal if and only if m is prime; this repeats the content of Theorem 4 of [NW]. However, that result is false, with the correct statement being that $\mathcal{I}(m)$ is principal if and only if m is square-free. This note corrects the error in [NW] by showing that, for a finite ring R, the ideal I_R is principal if and only if R is reduced or, equivalently, if and only if R is a direct sum of fields. We begin with a basic lemma.

Lemma 1. *If e is an idempotent of the commutative unitary ring R, the epimorphism $\phi : R[x] \rightarrow Re[x]$ defined by $\phi(f(x)) = ef(x)$ maps I_R onto I_{Re}.*

Proof. The inclusion $\phi(I_R) \subseteq I_{Re}$ is clear. To prove the converse we show that $I_{Re} \subseteq I_R$; this suffices since ϕ induces the identity map on $Re[x]$. Thus, take $g \in I_{Re}$. Since $g(0) = 0$, $g = ex \cdot h$ for some $h \in Re[x]$, and hence g vanishes on $R(1-e)$. Because g vanishes on Re and $R = Re \oplus R(1-e)$, it follows that $g \in I_R$. $\square$

Corollary 2. *If $R = R_1 \oplus ... \oplus R_n$ is the direct sum of ideals $R_1, ..., R_n$ of R, then $R[x] = \sum_{j=1}^{n} \oplus R_j[x]$ and $I_R = \sum_{j=1}^{n} \oplus I_{R_j}$. Therefore I_R is principal as an ideal of $R[x]$ if and only if each I_{R_j} is principal as an ideal of $R_j[x]$.*

If S is an Artinian ring, it is well-known that S is a finite direct sum of zero-dimensional local rings [ZS, Thm.3, p. 205]. Hence Corollary 2 shows that in determining conditions under which I_S is principal, it suffices to consider the case

1991 *Mathematics Subject Classification.* Primary 13B25; Secondary 13E10.
Key words and phrases. Vanishing polynomials, Artinian rings.

Typeset by $\mathcal{A}_\mathcal{M}\mathcal{S}$-TEX

where S is local. Our solution of this problem in Corollary 5 uses the following result due to Ernst Snapper.

Theorem 3. (Snapper, [S, p. 680]) *Suppose R is a commutative unitary ring and $f(t) \in R[t]$ is not a zero divisor in $R[t]$. If d is the minimum of the degrees of the nonzero elements of the principal ideal $(f(t))$ of $R[t]$, then there exists $a \in R$ such that $af(t)$ has degree d.*

Theorem 4. *If (R, M) is a zero-dimensional local ring, then I_R is principal if and only if either R/M is infinite or R is a finite field.*

Proof. If R is a finite field with q elements, it is well-known that $I_R = (t^q - t)$. If R/M is infinite, we show that $I_R = (0)$ (cf. [J,Th.9]). Thus, let $f(t) = \sum_{j=0}^{n} f_j t^j \in I_R$ and choose elements $a_1, a_2, ..., a_{n+1}$ in distinct residue classes of M in R. Since $f(a_1) = 0$, $f(t)$ is divisible by $(t - a_1)$ in $R[t]$. For $1 \le k < n+1$, if $f(t)$ is divisible by $(t-a_1)...(t-a_k)$ in $R[t]$, say $f(t) = (t-a_1)...(t-a_k)g(t)$, then $0 = f(a_{k+1}) = (a_{k+1} - a_1)...(a_{k+1} - a_k)g(a_{k+1})$, where each $a_{k+1} - a_i$ is a unit of R. We conclude that $g(a_{k+1}) = 0, g(t)$ is divisible by $t - a_{k+1}$, and hence $f(t)$ is divisible by $(t-a_1)...(t-a_{k+1})$ in $R[t]$. By induction it follows that $f(t)$ is divisible by $(t-a_1)...(t-a_{n+1})$, and hence $f(t) = 0$. Thus $I_R = (0)$ if R/M is infinite.

To prove the converse it suffices to show that I_R is not principal if R/M is finite and $M \neq (0)$. We use a proof by contradiction. Assume $I_R = (g(t))$, let $q = |R/M|$, and choose $e > 1$ so that $(0) = M^e < M$. Since $(t^q - t)^e \in I_R$, the polynomial $g(t)$ has a unit coefficient. If b is a nonzero element of $\mathrm{Ann}(M)$, then $b(t^q - t) \in I_R$, and the proof in the preceeding paragraph shows that I_R contains no nonzero element of degree less than q. Hence Theorem 3 shows that $ag(t) = \sum_{i=0}^{q} c_i t^i$ has degree q for some $a \in R$. We show that each c_i belongs to $\mathrm{Ann}(M)$. Thus, let u_0 be an arbitrary element of M and choose $u_1 = 0, u_2, ..., u_q$ to be a set of representatives of the residue classes of M in R. Viewing $c_0, c_1, ..., c_q$ as a solution in R of the homogenous system

$$\sum_{j=0}^{q} x_j u_i^j = 0 \qquad 0 \le i \le q$$

of equations, it follows that $c_j d = 0$ for $0 \le j \le q$, where $d = \prod_{i<j}(u_i - u_j)$ is the Vandermonde determinant associated with $u_0, u_1, ..., u_q$. Since d is a unit multiple of u_0, it follows that $c_j u_0 = 0$ for each j, and hence each c_j is in $\mathrm{Ann}(M)$, as asserted. Because g has a unit coefficient, a is also in $\mathrm{Ann}(M)$. Now $ag - c_q(t^q - t) \in I_R$, and because I_R contains no nonzero polynomial of degree less than q, $ag = c_q(t^q - t)$. We conclude that exactly two of the coefficients of g are units — those of t^q and of t. Moreover, since $g(0) = 0$, we have $g(t) = ut^q + vt + t^2 h(t)$ for some units u, v of R and polynomial $h(t) \in R[t]$. Thus $g(a) = va \neq 0$, a contradiction to the fact that $g(t) \in I_R$. Therefore I_R is not principal, as asserted.□

Since a zero-dimensional local ring (R, M) is finite if and only if R/M is finite, part(a) of Corollary 5 is a consequence of Theorem 4.

Corollary 5. *Let S be an Artinian ring.*

(a) *I_S is principal if and only if S is a direct sum of finite fields and of infinite zero-dimensional local rings.*

(b) *If S is finite, then I_S is principal if and only if S is reduced or, equivalently, if and only if S is a direct sum of finite fields.*

References

[J] G. Jacob, *Anneau de fonctions polynomes d'un anneau commutatif unitaire*, Commun. Algebra **8** (1990), 793–811.

[N] W. Narkiewicz, *Polynomial Mappings*, Lecture Notes in Math. **1600** (1995), Springer, Berlin Heidelberg.

[NW] I. Niven and D. Warren, *A generalization of Fermat's Theorem*, Proc. Amer. Math. Soc. **8** (1957), 306–313.

[S] E. Snapper, *Completely primary rings I.*, Annals of Math. **52** (1950), 666–693.

[ZS] O. Zariski and P. Samuel, *Commutative Algebra*, vol. I, Springer, Berlin Heidelberg, 1986.

Department of Mathematics, Florida State University, Tallahassee, FL 32306-3027

E-mail address: gilmer@math.fsu.edu