Paper accepted by American Mathematical Monthly in 2013

An Eigenvalue Theorem for Systems of Polynomial Equations

Yuly Billig and John D. Dixon

Abstract

We give a new short proof of a theorem relating solutions of a system of polynomial equations to the eigenvalues of the multiplication operators on the quotient ring, in the case when the quotient ring is finite-dimensional.

Everyone is familiar with the representation of a curve in the plane using an algebraic equation such as $X^2 + Y^2 = 1$. Algebraic geometers have learned that it is more convenient to represent these curves in the equivalent form of solutions (or zeros) of polynomials. In the case above, the circle is simply the set of (λ, μ) which are zeros of $X^2 + Y^2 - 1$. Similarly the simultaneous zeros of several polynomials represent the points of intersection of all of the corresponding curves. The solution of a system of polynomial equations is a natural extension of the problem of solving linear equations, and arises, for example, in the Lagrange multiplier method when the constraints and the function to be optimized are algebraic. Our particular aim is to prove the theorem below (Theorem 4) which gives a description of the common zeros of a system of polynomials. It is interesting in itself because it combines various important concepts and results from a standard undergraduate curriculum: ideals, quotient rings, homomorphism theorems, commuting linear operators and their common eigenvectors. Although the theorem is not new (see [2], [4] and [3]) and is quite elementary, we cannot find it in undergraduate text books.

If $\mathbb{K}$ is any field and $f_1, \ldots, f_n$ are polynomials in the ring $\mathbb{K}[X, Y]$, then it is convenient to consider the ideal $J = \langle f_1, \ldots, f_n \rangle$ generated by these polynomials. The set of common zeros in $\mathbb{K}^2$ of $f_1, \ldots, f_n$ is clearly the same as the set of common zeros for all the polynomials in J so we can forget about the particular polynomials chosen to generate J and simply think about the ideal J itself. We shall refer to these zeros briefly as the *zeros of* J. An important advantage of approaching the problem of the set of common zeros of polynomials (= intersection of curves) in this way is that we can take advantage of the structure of the ring $\mathbb{K}[X, Y]$ rather than simply dealing with a subset of $\mathbb{K}^2$. At the same time, we should not lose sight of the geometric interpretation of the theorems which arise.

In what follows, we shall restrict ourselves to the case of two variables, but at the end of this note we shall point out how all the results can be generalized to the case of m variables $X_1, \ldots, X_m$.

To fix notation, consider a finite list of polynomials $f_1, \ldots, f_n$ in $A := \mathbb{K}[X, Y]$. Let J be the ideal in A which they generate and let $S \subseteq \mathbb{K}^2$ be the set of all solutions to $f_1(X, Y) = 0, \ldots, f_n(X, Y) = 0$. We shall consider the relationship between S, J and the quotient ring $R := A/J$. Note that the rings A and R are vector spaces over $\mathbb{K}$. Whereas A is infinite-dimensional as a vector space, its quotient R could have finite dimension over $\mathbb{K}$. We are looking for a description of S in the case where R is finite dimensional.

The special case where $J = A$ ($\dim_{\mathbb{K}} R = 0$) occurs exactly when $1 \in J$ and in this case $S = \emptyset$. However, S may be empty even when J is a proper ideal. In what follows you might find it helpful to keep in mind the following example: $f_1 = X + Y - 3$ and $f_2 = X^2 + Y^2 - 1$ with $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$. In this case one can check that we have $S = \emptyset$ when $\mathbb{K} = \mathbb{R}$ (this is obvious from the geometry of the two curves) whilst $|S| = 2$ when $\mathbb{K} = \mathbb{C}$. On the other hand, one can show that for every field $\dim_{\mathbb{K}} R = 2$ (for example, show $1 + J$, $X + J$ is a basis for R).

Proposition 1. *We have* $\dim_{\mathbb{K}} R < \infty$ *if and only if* J *contains nonzero polynomials* $p(X)$ *and* $q(Y)$ *(each depending on a single variable).*

Proof. If R is finite-dimensional then the set of monomials $\{X^i | i \geq 0\}$ is linearly dependent in the quotient ring and thus there exists a non-zero polynomial $p(X) \in J$. Likewise, there is a non-zero polynomial $q(Y) \in J$. To prove the converse, note that a polynomial $p(X) \in J$ may be viewed as a reduction rule in the quotient ring R and and this allows one to reduce any power of X to a linear combination of $\{X^i\}$ with $i < \deg(p)$. Then R is spanned by a finite set $\{X^i Y^j | i < \deg(p), j < \deg(q)\}$ and is finite-dimensional. □

Corollary 2. *If* $\dim_{\mathbb{K}} R < \infty$ *then* S *is finite.*

Proof. Let $p(X), q(Y)$ be non-zero polynomials in J. Denote by P the set of roots of $p(X)$ and by Q the set of roots of $q(Y)$. Since every polynomial in the ideal J vanishes at every point in S, we conclude that S is contained in the finite set $P \times Q \subset \mathbb{K}^2$. □

The converse of the corollary is false in general. For example, if $\mathbb{K} = \mathbb{R}$ and we take $J = \langle X^2 + 1 \rangle$, then $S = \emptyset$ (there are no possible values for the first coordinate of a zero of J). On the other hand, $\dim_{\mathbb{R}} R$ is infinite by the proposition since J contains no nonzero polynomial $q(Y)$ depending only on Y. A similar example can be constructed whenever $\mathbb{K}$ is not algebraically closed, but it turns out that this is the only obstruction.

Proposition 3. *If* $\mathbb{K}$ *is algebraically closed, and* S *is finite, then* $\dim_{\mathbb{K}} R < \infty$*.*

Proof. The polynomial ring $\mathbb{K}[X, Y]$ in two variables can be embedded in the ring $\mathbb{K}(X)[Y]$ of polynomials in Y over the field $\mathbb{K}(X)$ of rational functions in X. Note that $\mathbb{K}(X)[Y]$ is a principal ideal domain. Consider the ideal $\overline{J}$ generated by $f_1, \ldots, f_n$ in the ring $\mathbb{K}(X)[Y]$. Every ideal in $\mathbb{K}(X)[Y]$ is principal, so let $g = Y^d + a_{d-1}(X)Y^{d-1} + \ldots + a_0(X)$ be the monic generator of $\overline{J}$. Let us show that $d = 0$ and so $g = 1$. Since $\overline{J} = \langle g \rangle$, we have $f_k = gh_k$, where $h_k = \sum_{j=0}^{m_k} c_{jk}(X)Y^j$, $k = 1, \ldots, n$. There are infinitely many values $\alpha \in \mathbb{K}$ for which the denominators of the rational functions $a_i(X)$, $c_{jk}(X)$ do not vanish. If $d > 0$, then for each such α there exists a root $\beta \in \mathbb{K}$ of the polynomial $Y^d + a_{d-1}(\alpha)Y^{d-1} + \ldots + a_0(\alpha)$. Then each f_k vanishes at (α, β), which would give us infinitely many zeros of J. Thus, the monic polynomial g is the constant polynomial 1. Since $g \in \overline{J}$, we can write $1 = f_1u_1 + \ldots + f_nu_n$ for some $u_j \in \mathbb{K}(X)[Y]$. Multiplying both sides of this equality by the denominators of all coefficients of u_j, for $j = 1, \ldots, n$, we construct a non-zero polynomial $p(X)$ which belongs to J. Analogously, J contains a non-zero polynomial $q(Y)$. By Proposition 1, R is finite-dimensional. □

We now study the properties of the quotient ring R in the case that $\dim_{\mathbb{K}} R < \infty$. We define two (commuting) linear transformations T_X and T_Y of R into itself by: $T_X(u(X, Y) + J) := Xu(X, Y) + J$ and $T_Y(u(X, Y) + J) := Yu(X, Y) + J$ (because J is an ideal, XJ, $YJ \subseteq J$, and so T_X and T_Y are well defined).

Our main result describes the zeros of J in terms of the eigenvalues and common eigenvectors of T_X and T_Y.

Theorem 4. *([4]) Suppose that* $\dim_{\mathbb{K}} R < \infty$*. Then* (λ, μ) *is a zero of* J *if and only if there is a nonzero vector* $v \in R$ *such that* $T_Xv = \lambda v$ *and* $T_Yv = \mu v$*.*

Proof. By Proposition 1 there exist nonzero single variable polynomials $p(X)$ and $q(Y)$ in J. Suppose $(\lambda, \mu) \in S$. Then $p(\lambda) = 0$ and $q(\mu) = 0$, so $p(X) = (X - \lambda)^r p_1(X)$ and $q(Y) = (Y - \mu)^s q_1(Y)$ for some $r, s > 0$ where $p_1(\lambda) \neq 0$ and $q_1(\mu) \neq 0$. Furthermore, $u(X, Y) := p_1(X)q_1(Y) \notin J$ since it does not vanish on (λ, μ), but $(X - \lambda)^r u(X, Y)$, $(Y - \mu)^s u(X, Y) \in J$. Thus, there exists $v(X, Y) := (X - \lambda)^{r_1}(Y - \mu)^{s_1} u(X, Y)$ with $0 \leq r_1 < r$ and $0 \leq s_1 < s$ such that $v(X, Y) \notin J$ but $(X - \lambda)v(X, Y) \in J$ and $(Y - \mu)v(X, Y) \in J$. Now $v(X, Y) + J$ is the required common eigenvector. Conversely, let $v(X, Y) + J$ be a common eigenvector for T_X and T_Y with eigenvalues λ and μ. We want to show that $(\lambda, \mu) \in S$, that is, that $J \subseteq M := \langle X - \lambda, Y - \mu \rangle$ (M is simply the ideal consisting of all polynomials for which (λ, μ) is a zero). We proceed as follow. For each $p(X, Y) \in A$ we can use the division algorithm to divide by $X - \lambda$ and obtain $p(X, Y) = a(X, Y)(X - \lambda) + r(Y)$ for some polynomials $a(X, Y)$, $r(Y) \in A$. Now we can divide by $Y - \mu$ to obtain $r(Y) = b(Y)(Y - \mu) + s$ where $b(Y)$, $s \in A$ and the remainder s is a constant. Evaluating at (λ, μ) shows that $s = r(\mu) = p(\lambda, \mu)$. Thus, we see that for each $p(X, Y)$ in A there exist $a(X, Y)$, $b(Y) \in A$ such that $p(X, Y) = a(X, Y)(X - \lambda) + b(Y)(Y - \mu) + p(\lambda, \mu)$. Hence $A = M + \mathbb{K}$ and so $\dim_{\mathbb{K}}(A/M) \leq 1$. Thus, if $J \nsubseteq M$, then $A = J + M$ since $J + M$ is a $\mathbb{K}$-subspace of A containing M. But $v(X, Y)M \subseteq J$ since $v(X, Y)(X - \lambda)$ and $v(X, Y)(Y - \mu)$ lie in J by the choice of $v(X, Y)$. Hence $J \nsubseteq M$ implies $v(X, Y) \in v(X, Y)J + v(X, Y)M \subseteq J$ contrary to the fact that an eigenvector is non-zero. □

More generally, if $p(X, Y) \in \mathbb{K}[X, Y]$ and T_p denotes the linear operator on R obtained by multiplication by $p(X, Y)$, then the eigenvalues of T_p are given by $p(\lambda, \mu)$ for $(\lambda, \mu) \in S$.

Corollary 5. $|S| \leq \dim_{\mathbb{K}} R$.

This corollary follows from the fact that the eigenvectors corresponding to distinct eigenvalues are linearly independent.

It is well-known that two commuting operators on a finite-dimensional space over an algebraically closed field have a common eigenvector (provided that the dimension of the vector space is non-zero). As a consequence we get the following

Corollary 6. *If $\mathbb{K}$ is algebraically closed, and $1 \leq \dim_{\mathbb{K}} R < \infty$, then J has at least one zero.*

Remark 7. What happens if we have more than two variables? There are obvious generalizations of the first proposition, the theorem and their corollaries to polynomial rings $\mathbb{K}[X_1, \ldots, X_m]$ in any (finite) number of variables. A little thought shows that they can be proved using natural generalizations of those proofs given above.

It is also true that Proposition 3 generalizes to polynomial rings of m variables (over an algebraically closed field!), but the proof above which depends on the fact that a polynomial ring in one variable over a field is a principal ideal ring does not seem to generalize. A proof of the general proposition instead requires Hilbert's Nullstellensatz which is less elementary. Recently Arrondo [1] has given an elegant proof of the Nullstellensatz which makes that theorem within reach of an undergraduate algebra course.

In order to carry out explicit calculations with Theorem 4, one has to work out a Gröbner basis of the ideal J or a border basis of J [5]. A computational alternative to this theorem is the elimination theory (see e.g., [6]), however Theorem 4 is much more attractive aesthetically. It is a convenient stepping stone towards computational algebra and algebraic geometry.

Acknowledgments. The authors thank Ken Small for his suggestion to write this note.

References

[1] E. Arrondo, Another elementary proof of the Nullstellensatz. Amer. Math. Monthly **113** (2006) 169-171.

[2] W. Auzinger, H. J. Stetter, An elimination algorithm for computation of all zeros of a system of multivariate polynomial equations, in: *Conference in Numerical Analysis*, Internat. Schriftenreihe Numer. Math., Vol. 86, Birkhäuser, Basel, 1988. 11-30.

[3] D. Cox, J. Little, D. O'Shea, *Using Algebraic Geometry.* Graduate Texts in Mathematics, Vol. 185. Springer-Verlag, New York, 1998.

[4] H. J. Stetter, Multivariate polynomial equations as matrix eigenproblems, in *Contributions in Numerical Mathematics*, World Sci. Ser. Appl. Anal., Vol. 2, World Sci. Publ., River Edge, NJ, 1993. 355-371.

[5] M. Kreuzer, L. Robbiano, *Computational Commutative Algebra 2*. Springer-Verlag, Berlin, 2005.

[6] B. L. van der Waerden, *Modern Algebra,* Vol. II, Frederick Ungar Publishing, New York, 1950.

School of Mathematics and Statistics, Carleton University, Ottawa, Canada
billig@math.carleton.ca, jdixon@math.carleton.ca