Hilbert's Nullstellensatz

Harry Gulliver

Throughout this document, all rings are assumed to be commutative and unital unless otherwise stated and all ring morphisms are assumed to be unital ($\phi(1) = 1$). Some sections are in red; these are the harder proofs and more general statements of some results, included for the interested reader; they can be safely skipped. Though I have made every effort to ensure there are no typos, no doubt some have slipped through - my apologies!

1 Some Background Ring Theory

DEFINITION: *Ideals; Prime & Maximal Ideals*

Let R be a ring. An *ideal* in R is a subset $I \subseteq R$ such that I is a subgroup of the additive group $(R, +)$ and "absorbs multiplication" - meaning that for any $r \in R$ and any $i \in I$, $ri \in I$. Compare with the zero element, which absorbs multiplication in a similar way - indeed, $\{0\}$ is always an ideal in any ring. We write $I \trianglelefteq R$ for I an ideal in R. An ideal I is called *prime* if $I \neq R$ and whenever $xy \in I$ we have either $x \in I$ or $y \in I$ (or both); compare with the definition of a prime element, where p is prime if whenever $p|xy$, $p|x$ or $p|y$. An ideal is called *maximal* if $I \neq R$ and there is no ideal J with $I \subsetneq J \subsetneq R$.

EXAMPLES:

1. Let R be any ring. Then R and $\{0\}$ are both ideals. We normally write (0) for $\{0\}$ in this context and call it the zero ideal.

2. R is an integral domain if and only if (0) is a prime ideal.

3. Let $r \in R$; define $(r) = \{rx|x \in R\}$, the set of all multiples of r. This is easily seen to be an ideal and is called the *principal ideal generated by r*. This explains the notation for the zero ideal, which is the principal ideal generated by zero. A ring in which every ideal has this form is called a *principal ideal domain*

4. Generalising the last example, let $r_1, \ldots, r_n \in R$ and define $(r_1, \ldots, r_n) = \{\sum_{i=1}^{n} r_i x_i | x_i \in R\}$, the set of all sums of multiples of the r_i. This is also an ideal, called the ideal generated by $r_1, \ldots r_n$. A ring in which every ideal has this form is called *Noetherian.*

5. The ring of integers, $\mathbb{Z}$, is easily seen to be a principal ideal domain (take the smallest positive element in an ideal and show that this generates it). An ideal (n) is prime if and only if n is a prime number or 0 and is maximal if and only if n is a prime number.

6. Let $\phi : R \to S$ be a ring morphism and $\ker(\phi) = \phi^{-1}(0)$; then $\ker(\phi)$ is an ideal in R.

Lemma:

Let $I \subseteq R$ be an ideal. Then $I = R$ if and only if $I \cap R^\times \neq \varnothing$. That is, if and only if there is an invertible element in I.

Proof:

If $I = R$, then $1 \in I$ and so I contains an invertible element. Conversely, if $x \in I$ is invertible, then $1 = x^{-1}x \in I$, by the multiplicative property of ideals; but then for any $r \in R$, $r = r \times 1 \in I$, again by the multiplicative property. So $R \subseteq I$ and the reverse inclusion holds by definition. ■

Corollary:

A ring R is a field if and only if its only ideals are (0) and R itself.

Proof:

Every non-zero element of a field is invertible, so any non-zero ideal of a field contains an invertible element and hence is equal to the whole field. Conversely, let $r \in R$ be any non-zero element and consider the ideal (r) generated by r. This must be all of R, so $1 \in (r)$, hence $1 = rx$ for some $x \in R$ and so r is invertible. ■

Lemma:

Let $I \subseteq R$. Then I is an ideal if and only if I is non-empty, closed under addition and has the multiplicative property.

Proof:

We need to check that I is a subgroup of $(R, +)$. We know that it is closed under addition and non-empty, so there exists some $x \in I$. Then $0 = 0 \times x \in I$ and for any $y \in I$, $-y = (-1) \times y \in I$, by the multiplicative property. So I satisfies the other two subgroup conditions automatically. ■

Definition: *Quotient Rings*

Let R be a ring and I an ideal in R. Then I is a subgroup of $(R, +)$, which is an abelian group, so I is a normal subgroup. Hence we can form the quotient group $R/I = \{r + I | r \in R\}$, with addition given by $(r + I) + (s + I) = (r + s) + I$. Define a multiplication on R/I by $(r + I)(s + I) = (rs) + I$. This is well-defined, since if $r_1 + I = r_2 + I$ and $s_1 + I = s_2 + I$, then for some $i_r, i_s \in I$, $r_1 = r_2 + i_r$ and $s_1 = s_2 + i_s$, so:

$$\begin{aligned}(r_1 + I)(s_1 + I) &= (r_1 s_1) + I \\ &= (r_2 + i_r)(s_2 + i_s) + I \\ &= (r_2 s_2 + i_r s_2 + r_2 i_s + i_r i_s) + I \\ &= (r_2 s_2) + I \\ &= (r_2 + I)(s_2 + I)\end{aligned}$$

using the multiplicative property and additive closure of ideals to see that $i_r s_2 + r_2 i_s + i_r i_s \in I$. It is easy to check that this multiplication makes R/I into a ring, which we call the *quotient ring of R by I*.

Let $\phi : R \to R/I$ be the canonical group homomorphism, so $\phi(r) = r + I$. It is easy to see that ϕ is in fact a ring morphism with kernel I. Moreover, we have the following:

Theorem: *The First Isomorphism Theorem*

Let $\phi : R \to S$ be a ring morphism. Then ϕ naturally induces an isomorphism:

$$R/\ker(\phi) \xrightarrow{\sim} \phi(R)$$

given by $r + \ker(\phi) \mapsto \phi(r)$.

Proof:

Routine and almost identical to the proof of the group-theoretic version, so omitted. Indeed, versions of this theorem exist in all sorts of contexts and are all proved in basically the same way.

Theorem: *The Correspondence Theorem*

Let R be a ring, I an ideal in R and $\phi : R \to R/I$ the canonical map. Then ϕ induces a bijection between the set of ideals in R which contain I and the set of ideals in R/I. Moreover, an ideal $J \trianglelefteq R$ with $I \subseteq J$ is prime (resp. maximal) if and only if the corresponding ideal $\phi(J) \trianglelefteq R/I$ is prime (resp. maximal).

Proof:

Let $J \trianglelefteq R$ be an ideal with $I \subseteq J$. Then for $X, Y \in \phi(J)$, there exist $x, y \in J$ with $\phi(x) = X$ and $\phi(y) = Y$; then $X + Y = \phi(x + y) \in \phi(J)$ and for any $A \in R/I$ there exists $a \in R$ with $\phi(a) = A$ (as ϕ is surjective), so $AX = \phi(ax) \in \phi(J)$; hence $\phi(J)$ is indeed an ideal. Similarly, if $K \trianglelefteq R/I$, then for any $x, y \in \phi^{-1}(K)$, there exist $X, Y \in K$ with $\phi(x) = X$ and $\phi(y) = Y$; then $\phi(x + y) = X + Y \in K$, so $x + y \in \phi^{-1}(K)$, and for any $a \in R$, there exists $A = \phi(a)$ in R/I, so $\phi(ax) = AX \in K$, so $ax \in \phi^{-1}(K)$. Moreover, $0 \in K$, so $\phi^{-1}(0) \subseteq \phi^{-1}(K)$, but $\phi^{-1}(0) = \ker(\phi) = I$, so we do indeed have $I \subseteq \phi^{-1}(K)$.

For any ideal $J \trianglelefteq R$, with $I \subseteq J$, $\phi^{-1}\phi(J) = \{r \in R | \phi(r) \in \phi(J)\} = \{r \in R | \exists j \in J : \phi(r) = \phi(j)\}$. But if $\phi(r) = \phi(j)$, then $\phi(r - j) = 0$, so $r - j \in I \subseteq J$, hence $r \in J$. So in fact $\phi^{-1}\phi(J) \subseteq J$; the reverse inclusion is clear. Conversely, for any ideal $K \trianglelefteq R/I$, it is clear that $\phi\phi^{-1}(K) \subseteq K$, while the reverse inclusion follows from surjectivity - given any $k \in K$, there exists $r \in R$ with $\phi(r) = k$, so $r \in \phi^{-1}(K)$ and hence $k = \phi(r) \in \phi\phi^{-1}(K)$.

To prove that the correspondence preserves primality of ideals, let $P \trianglelefteq R$ be a prime ideal with $I \subseteq P$. Then to show that $\phi(P)$ is prime in R/I, take a product $XY \in \phi(P)$; by surjectivity, $X = \phi(x)$ and $Y = \phi(y)$ for some $x, y \in R$, so $\phi(xy) \in \phi(P)$. But then $\phi(xy) = \phi(p)$ for some $p \in P$, so $xy + i \in P$ for $i = p - xy \in I$; but $I \subseteq P$, so $i \in P$ and hence $xy \in P$. P is prime, so $x \in P$ or $y \in P$; but then $\phi(x) \in \phi(P)$ or $\phi(y) \in \phi(P)$. Conversely, if $P \trianglelefteq R/I$ is prime, then consider $xy \in \phi^{-1}(P)$. This implies that $\phi(x)\phi(y) \in P$, hence $\phi(x) \in P$ or $\phi(y) \in P$, so $x \in \phi^{-1}(P)$ or $y \in \phi^{-1}(P)$.

Finally, to prove that the correspondence preserves maximality, it suffices to note that it preserves the ordering of subsets by inclusion. ■

Corollary: *Characterisation of Maximal Ideals*

An ideal $I \trianglelefteq R$ is maximal if and only if R/I is a field.

Proof:

If I is maximal, then there are no ideals strictly between I and R, so by the Correspondence Theorem, there are no idelas of R/I strictly between (0) and R/I; but this is equivalent to R/I being a field, by an earlier result. ■

Lemma: *Characterisation of Prime Ideals*

An ideal $I \trianglelefteq R$ is prime if and only if R/I is an integral domain.

Proof:

If I is prime, suppose $(x+I)(y+I) = 0+I$ in R/I; then $xy+I = I$, so $xy \in I$; but then $x \in I$ or $y \in I$, so $x+I = 0+I$ or $y+I = 0+I$ and so R/I is an integral domain. Conversely, suppose $xy \in I$; then $(x+I)(y+I) = 0+I$, so $x+I = 0+I$ or $y+I = 0+I$, hence $x \in I$ or $y \in I$. ■

Corollary:

All maximal ideals are prime.

Proof:

Let $M \trianglelefteq R$ be maximal. Then R/I is a field; in particular, it is an integral domain, so M is prime. ■

Theorem: *The Nilradical*

An element $x \in R$ is nilpotent (*i.e.*, $x^k = 0$ for some positive integer k) if and only if x is in every prime ideal. Thus, the set of all nilpotent elements is precisely the intersection of all prime ideals; it is called the *nilradical*.

Proof:

Suppose x is nilpotent and let P be a prime ideal. We have that $x^k = 0 \in P$ for some k, so $x \times x^{k-1} \in P$; by the definition of a prime ideal, either $x \in P$ or $x^{k-1} \in P$. But in the latter case we then have $x \times x^{k-2} \in P$, so proceeding by induction we must eventually have $x \in P$.

The converse is much harder and requires a formulation of the Axiom of Choice called Zorn's Lemma. Some preliminaries:

A relation on a set is called a *partial ordering* if it is reflexive ($x \sim x \ \forall x$), transitive ($x \sim y \sim z \Rightarrow x \sim z$) and antisymmetric ($x \sim y$ and $y \sim x \Rightarrow x = y$). Examples of partial orderings are the relation $\leq$ on the real numbers (this is something stronger - a total ordering - as given any elements x and y, either $x \leq y$ or $y \leq x$) and the relation $\subseteq$ on any set of sets - in particular, on the set of ideals in a ring, or some subset thereof (note that this is generally not a total ordering - there can be two sets with neither one a subset of the other).

A set with a partial ordering $\sim$ on it is called a partially ordered set, or *poset*. If S is a subset of a poset P, an *upper bound* for S is an element u of P with $x \sim u$ for all $x \in S$. A *chain* in a poset is a totally ordered subset. A maximal element of a poset P is one such that there is no larger element in P - *i.e.*, $m \in P$ is maximal if whenever $m \sim x$ for $x \in P$, then $m = x$. Maximal ideals are precisely the maximal elements of the set of proper ideals, partially ordered by inclusion. Note that the definition of maximal element does not imply that $x \sim m$ for all $x \in P$ - maximal means "smaller than nothing", it does not mean "bigger than everything". In particular, maximal elements need not be unique.

Zorn's Lemma states that if S is a non-empty poset in which every chain has an upper bound in S, then S has (at least one) maximal element. This is logically equivalent to the Axiom of Choice (more precisely, set theory with the AoC is equivalent to set theory with Zorn), so Zorn's Lemma is really something we assume, rather than prove (despite the name).

Now, to prove that an element lying in all prime ideals is nilpotent, we prove the contrapositive: that for any non-nilpotent element x, there exists some prime ideal not containing x. To do this, let S be the set of all ideals which contain no powers of x: $S = \{I \trianglelefteq R | \forall n x^n \notin I\}$. S naturally carries a partial ordering by inclusion and is non-empty, as the non-nilpotency assumption implies that $(0) \in S$. Take any chain in S -

i.e., any sequence of nested ideals, none of which contain any powers of x; call the chain $C = (I_n)_{n \in N}$ where N is some indexing set. Let $U = \bigcup_{n \in N} I_n$ be the union of this chain. Then U is an upper bound for C. Note that the union of ideals is not usually an ideal (though the intersection always is), but it is in the case that the ideals being unioned are nested. To see this, let $x, y \in U$. Then $x \in I_n$ and $y \in I_m$ for some $n, m \in N$; then either $I_n \subseteq I_m$ or the converse, since C is totally ordered; suppose $I_n \subseteq I_m$; then $x, y \in I_m$ and so $x + y \in I_m \subseteq U$. Now let $r \in R$ be any element; then $x \in I_n$, so $rx \in I_n \subseteq U$; so we have proved that U is an ideal.

Moreover, $U \in S$, since every element of U is contained in one of the I_n, none of which contains any power of x, so U contains no powers of x. Finally, it is true by definition that $I_n \subseteq U$ for all $n \in N$. So U is an upper bound for C in S. Hence, by Zorn's Lemma, S has a maximal element M. M is an ideal which does not contain x (or indeed any power of x), so it suffices to prove that M is prime.

Suppose for a contradiction that M is not prime; then there exist elements $a, b \in R$ such that neither a nor b is an element of M, but $ab \in M$. Consider $J := \{c \in R | ac \in M\}$; this is readily seen to be an ideal, it contains M (as for $m \in M$, $rm \in M$ for any $r \in R$, in particular for $r = a$) and $J \neq M$, since $b \in J$. But M was maximal in S, so we must have $J \notin S$; then, for some n, $x^n \in J$. Now consider $K := \{c \in R | cx^n \in M\}$; by the same argments as above, *mutatis mutandis*, K is an ideal properly containing M, so $K \notin S$ and $x^m \in K$ for some m. But then by the definition of K, $x^{n+m} \in M$, which is the desired contradiction. ■

2 Jacobson Rings

Definition: *Jacobson Rings*

A commutative ring is called *Jacobson* if every prime ideal is an intersection of maximal ideals.

The true definition goes as follows: for an R-module M, define the *annihilator* of M as $\operatorname{ann}_R(M) = \{r \in R | rm = 0 \forall m \in M\}$; this is easily seen to be an ideal and we call an ideal *primitive* if it is the annihilator of a simple R-module (one with no proper, non-trivial submodules). Then a Jacobson ring is one in which every prime ideal is an intersection of primitive ideals. In commutative rings, maximal and primitive ideals turn out to coincide, whence the above definition.

Lemma: *Watters' Lemma*

If R is a Jacobson ring, then so is $R[X]$.

Proof:

Lengthy, so omitted. If interested, read Watters' 1975 paper *Polynomial Extensions of Jacobson Rings* from the Journal of Algebra (vol. 36, issue 2, pp. 302-308); this is available through the library.

Lemma: *Quotients of Commutative Jacobson Rings*

Let R be a Jacobson ring and $I \trianglelefteq R$ an ideal. Then R/I is also Jacobson.

Proof:

Let $\phi : R \to R/I$ be the canonical projection and take any prime ideal $P \trianglelefteq R/I$. By the Correspondence Theorem, $\phi^{-1}(P)$ is a prime ideal in R, with $I \subseteq \phi^{-1}(P)$. Then

$\phi^{-1}(P) = \bigcap_{\alpha \in A} M_\alpha$ for some maximal ideals M_α, with A some indexing set. As $I \subseteq \phi^{-1}(P)$, we must have $I \subseteq M_\alpha$ for all α. Then $P = \phi\left(\bigcap_{\alpha \in A} M_\alpha\right)$.

Now, if $y \in P = \phi\left(\bigcap_{\alpha \in A} M_\alpha\right)$, then there exists $x \in \bigcap_{\alpha \in A} M_\alpha$ with $\phi(x) = y$, so $x \in M_\alpha$ for all α and hence $y = \phi(x) \in \phi(M_\alpha)$ for all α and hence $y \in \bigcap_{\alpha \in A} \phi(M_\alpha)$. Conversely, if $y \in \bigcap_{\alpha \in A} \phi(M_\alpha)$, then for each α there exists some $x_\alpha \in M_\alpha$ with $\phi(x_\alpha) = y$. But $x_\alpha - x_\beta \in I$ for any $\alpha, \beta \in A$ and $I \in M_\alpha$ for all α, so in fact $x_\beta \in M_\alpha$ for all $\alpha, \beta \in A$ (what we have shown is that each M_α contains something which maps to y, but then must contain everything which maps to y, since they all contain the kernel). So in fact we have some $x \in M_\alpha$ for all α such that $\phi(x) = y$; hence $y \in \phi\left(\bigcap_{\alpha \in A} M_\alpha\right)$. Thus, $P = \bigcap_{\alpha \in A} \phi(M_\alpha)$.

But each M_α is maximal, so each $\phi(M_\alpha)$ is maximal and so P is an intersection of maximal ideals. ■

Examples: *Jacobson Rings*

1. Every field is Jacobson, since the only prime ideal is (0), and this is also maximal.

2. Every polynomial ring over a field (in any number of variables) is Jacobson, by induction on Watters' Lemma.

3. Every quotient of a polynomial ring over a field is Jacobson.

Lemma: *The Nilradical & Jacobson Radical in a Jacobson Ring*

Let R be a commutative, Jacobson ring. Then the intersection of all prime ideals is equal to the intersection of all maximal ideals. Note that the intersection of all prime ideals is called the nilradical (it is the set of all nilpotent elements) and the intersection of all maximal ideals is called the Jacobson radical (in a non-commutative ring, the Jacobson radical is the intersection of all primitive ideals).

Proof:

Every maximal ideal is prime, so the intersection of all prime ideals is the intersection of all maximal ideals intersected with the intersection of all non-maximal prime ideals; in particular, it is a subset of the intersection of all maximal ideals. Conversely, in a Jacobson ring, every prime ideal is an intersection of maximal ideals, so the intersection of all prime ideals is an intersection of some maximal ideals, hence is a superset of the intersection of all maximal ideals. So the nilradical and Jacobson radical are each included in the other, hence they are equal. ■

3 Zariski's Lemma & the Nullstellensatz

Definition: *Finitely Generated Algebras*

Let F be a field. An (associative, unital) *F-algebra* is an F-vector space with a multiplication operation which, coupled with its addition operation, makes it into a ring. That is, an F-algebra A is a set with three operations: $+ : A \times A \to A$, $\times : A \times A \to A$ and $. : F \times A \to A$ such that $(A, +, \times)$ is a ring (associative and unital, but not necessarily commutative) and $(A, +, .)$ is a vector space. We also require that for any scalar λ and any algebra elements a and b, $\lambda(ab) = (\lambda a)b = a(\lambda b)$. We say that A is *finitely generated* if there exists some finite set $\{a_1, \ldots, a_n\} \subseteq A$ such that every element in A can be expressed as a polynomial in the a_i (that is, every element can be written as a finite sum of scalar multiples of finite products of the a_i). Note that, unlike with bases of vector spaces, there might not exist a generating set such that the expressions are unique; for instance, the quotient algebra $F[X]/(X^2)$).

Examples: *Algebras*

1. $F[t_1, \dots, t_n]$, the polynomial ring over F in n variables, is a commutative F-algebra; it has finite generating set $\{1, t_1, \dots, t_n\}$.

2. Any quotient ring of an F-algebra A is an F-algebra. For any ideal $I \trianglelefteq A$ is also a vector subspace, since for all scalars λ and for all $i \in I$, $\lambda i = (\lambda 1)i \in I$ by the multiplicative property; hence A/I is a vector space, and it is also a ring. Moreover, if $\{a_1, \dots, a_n\}$ is a generating set for A, then $\{a_1 + I, \dots, a_n + I\}$ generates A/I, using the same polynomial expressions.

Lemma: *Zariski's Lemma*

Let F be an algebraically closed field and A a finitely generated F-algebra, which is also a field in its own right. Then $A = F$.

The proper statement of Zariski's Lemma is: Let F be any field and A a finitely generated F-algebra, which is also a field. Then A is a finite field extension of F (*i.e.*, A is finite-dimensional as an F-vector space). This implies the above statement, as if F is algebraically closed, the only finite extension of F is the trivial one, F itself.

Proof:

Difficult, so omitted. It can be proved quite easily from Noether's Normalisation Theorem, but that is itself a very deep result and hard to prove.

We now come to the problem to which the Nullstellensatz provides the solution. Let F be a field and $f_1, \dots, f_m$ polynomials in n variables over F. Then we define the set $V \subseteq F^n$ by $V = \{x \in F^n | f_i(x) = 0 \forall i\}$. The problem is, given V, to reconstruct $\{f_1, \dots, f_m\}$. This is clearly not generally possible; for instance, $\{y - x, y - 2x, 6y - 12x\}$ and $\{2y - 3x, 2x - y\}$ are different sets that generate the same V. It is clear that any polynomial in $I = (f_1, \dots, f_m)$, the ideal generated by the f_i, will vanish everywhere on V and most of these polynomials will in fact vanish nowhere else but on V (though some will - for instance, $0 \in I$ vanishes everywhere). So the best we can reasonably hope for is to recover I from V. In fact, this too is not quite possible, as $x - y$ and $(x - y)^2$ have the same vanishing locus V, but generate different ideals. However, this turns out to be the last wrinkle (when working over an algebraically closed field, which is a sensible condition to impose when dealing with polynomials and their roots!):

Theorem: *Hilbert's Nullstellensatz*

Let F be an algebraically closed field and $R = F[t_1, \dots, t_n]$ the polynomial ring in n variables over F. Let $I \trianglelefteq R$ be an ideal in R and $V = \mathcal{V}(I) = \{x \in F^n | g(x) = 0 \forall g \in I\}$ be the vanishing locus of I. Then if a polynomial $f \in R$ vanishes everywhere on V, there exists some positive integer k such that $f^k \in I$. Equivalently, $f \in \sqrt{I}$, where $\sqrt{I} = \{r \in R | \exists k \in \mathbb{N} : r^k \in I\}$ is the radical of I.

Proof:

Note that if I contains any non-zero constant polynomial, then $I = R$ and the theorem is trivial, so we may assume that 0 is the only constant polynomial in I. Then quotienting by I may be regarded as imposing relations among the variables t_i without affecting the coefficients; in particular, we may write $g(t_1 + I, \dots, t_m + I)$ in place of $g(t_1, \dots, t_m) + I$

for any polynomial g. For convenience, write $t = (t_1, \dots, t_m)$ and $T = (t_1 + I, \dots, t_m + I)$. It is clear that $f(t)^k \in I$ if and only if $f(T)^k = 0$ in the quotient ring R/I. That is, it suffices to prove that $f(T)$ is a nilpotent element of R/I, *i.e.*, that $f(T)$ is in the nilradical of R/I.

The nilradical is the intersection of all prime ideals; R is a polynomial ring over a field, hence is Jacobson, so R/I is also Jacobson, so the nilradical is in fact equal to the intersection of all maximal ideals. So our strategy is to show that $f(T)$ is contained in every maximal ideal of R/I.

Let $M \trianglelefteq R/I$ be a maximal ideal. Then $(R/I)/M$ is a field. Let x_i be the image of $t_i + I$ when quotienting by M; then $\{1, x_1, \dots, x_n\}$ is a generating set for $(R/I)/M$ as an F-algebra, so $(R/I)/M$ is a field and a finitely generated F-algebra. Hence, by Zariski's Lemma, $(R/I)/M = F$. Hence $x = (x_1, \dots, x_n)$ is an element of F^n and, in fact, of V; for if $g(t)$ is any polynomial in I, then $g(T) = 0$, so $g(x) = 0$ (once g has been sent to zero by quotienting out I, we can't possibly make it non-zero again by quotienting out by M). Therefore $f(x) = 0$, by the assumption that f vanishes on V.

But then $f(T)$ is sent to zero when we quotient out M, so $f(T)$ must be in the kernel of this quotient map, which is precisely M. M was an arbitrary maximal ideal, so we have shown that $f(T)$ is contained in every maximal ideal of R/I; hence it lies in every prime ideal (as R/I is Jacobson) and hence is nilpotent, so $f(T)^k = I$ for some k, hence $f(t)^k \in I$. ■