A NEW PROOF OF HILBERT'S NULLSTELLENSATZ

OSCAR ZARISKI

Introduction. A number of proofs of Hilbert's Nullstellensatz can be found in the literature. One, based on elimination theory and due to A. Rabinowitsch, is reproduced in van der Waerden's *Moderne Algebra*, vol. 2, p. 11. In a later chapter van der Waerden gives another proof which is based on the method of specialization in fields of algebraic functions (pp. 59–61). The finishing touches to this proof (p. 65) presuppose the decomposition theorem for polynomial ideals. In his Ergebnisse monograph *Idealtheorie*, p. 46, Krull gives an ideal-theoretic proof which, while it is based on the simple remark by Rabinowitsch, is of an advanced nature, since the proof makes use of the full dimension theory of algebraic varieties developed in §17, pp. 41–43. The main "Dimensionssatz" of p. 43 is based on a result which is proved only in §48, pp. 129–134. Moreover, the concept of integral dependence and the "Normalization theorem" of Emmy Noether are used in Krull's proof.

In the present note we give first of all a short proof of Hilbert's Nullstellensatz which makes use only of the rudiments of field theory and ideal theory. Actually we give two new proofs of the Nullstellensatz. A lemma used in the second proof enables us to establish a result on finite integral domains which we were not able to find in the literature. This result is as follows:

If \( R = K[\xi_1, \xi_2, \ldots, \xi_n] \) is a finite integral domain over a field \( K \) and if \( \overline{K} \) is the algebraic closure of \( K \) in \( R \), then \( K \) contains all the fields which are contained in \( R \).

1. First proof of the Nullstellensatz. Let \( \mathfrak{P}_n \) denote the polynomial ring \( K[x_1, x_2, \ldots, x_n] \) in \( n \) indeterminates \( x_i \), over a given ground field \( K \). By a point \( \alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \) we mean an ordered \( n \)-tuple of algebraic quantities \( \alpha_i \) over \( K \). Our convention will be that conjugate \( n \)-tuples over \( K \) represent the same point over \( K \). Let \( S_n \) denote the (linear) space of all points. By a zero \( \alpha \) of a field \( \mathfrak{A} \) in \( \mathfrak{P}_n \) we mean a point \( \alpha \) such that \( f(\alpha) = 0 \) for every polynomial \( f(x) = f(x_1, x_2, \ldots, x_n) \) in \( \mathfrak{A} \). The totality of zeros of \( \mathfrak{A} \) is the algebraic variety in \( S_n \) determined by the ideal \( \mathfrak{A} \) and shall be denoted by \( \mathfrak{U}(\mathfrak{A}) \).

If \( W \) is an algebraic variety in \( S_n \), we shall denote by \( \mathfrak{I}(W) \) the ideal in \( \mathfrak{P}_n \) consisting of all polynomials which vanish on \( W \) (that is, at every point of \( W \)). The Hilbert Nullstellensatz asserts the following:

Received by the editors November 4, 1946.

362
H1: If $\mathfrak{A}$ is an ideal in $\mathfrak{B}_n$, then $3(\mathcal{U}(\mathfrak{A}))$ is the radical of $\mathfrak{A}$.

It has been shown by Rabinowitsch that the following special case of Hilbert's Nullstellensatz is equivalent to the full Nullstellensatz:

H2: If $\mathcal{U}(\mathfrak{A})$ is an empty set then $\mathfrak{A}$ is the unit ideal.

For the convenience of the reader we reproduce here the original proof of Rabinowitsch. Let $x_{n+1}$ be an extra indeterminate and let $\mathfrak{B}_{n+1}$ be the polynomial ring $K[x_1, x_2, \cdots, x_{n+1}]$. If $f(x)$ is any polynomial in $\mathfrak{B}_n$ which vanishes on $\mathcal{U}(\mathfrak{A})$ and if we set $g = 1 + x_{n+1}f$, then the ideal $\mathfrak{A}$ generated in $\mathfrak{B}_{n+1}$ by $\mathfrak{A}$ and $g$ is such that $\mathcal{U}(\mathfrak{A})$ is empty. Hence by the special case H2 of the Nullstellensatz it follows that $\mathfrak{B} = (1)$. There exists therefore an identity of the form

$$\sum_i A_i h_i + gh = 1, \quad A_i \in \mathfrak{A}; h_i, h \in \mathfrak{B}_{n+1}.$$ 

On replacing $x_{n+1}$ in this identity by $-1/f$ and clearing the denominators we find a relation of the form $\sum A_i B_i = \rho$, where $B_i \in \mathfrak{B}_n$ and $\rho$ is a non-negative integer. Hence $f$ belongs to the radical of $\mathfrak{A}$, and since the inclusion: radical of $\mathfrak{A} \subseteq 3(\mathcal{U}(\mathfrak{A}))$ is trivial, this establishes the Nullstellensatz.

Let $R_n$ denote any finite integral domain over $K$ which can be obtained from $K$ by an $n$-fold ring extension: $R_n = K[\xi_1, \xi_2, \cdots, \xi_n]$. To prove H2 we first show that $R_n$ is an immediate consequence of the following statement:

H3: If a finite integral domain $R_n$ (over $K$) is a field then it is an algebraic extension of the field $K$.

For if $\mathfrak{A}$ is an ideal in $\mathfrak{B}_n$, different from the unit ideal, then $\mathfrak{A}$ is contained in some maximal ideal of $\mathfrak{B}_n$. If $p$ is such a maximal ideal and if we set $R_n = \mathfrak{B}_n/p = K[\alpha_1, \alpha_2, \cdots, \alpha_n]$, then $R_n$ is a field and, therefore, if we assume $H^3_n$, it follows that the $\alpha_i$ are algebraic over $K$, that is, $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ is a point. This point is a zero of $p$ and hence a fortiori a zero of $\mathfrak{A}$, since $\mathfrak{A} \subseteq p$. We have thus shown that if $\mathfrak{A} \neq (1)$ then $\mathcal{U}(\mathfrak{A})$ is not empty, and this establishes $H_2$.

The proof of Hilbert's Nullstellensatz is thus reduced to proving $H^3_n$. We shall prove $H^3_n$ by induction with respect to $n$, since $H^3_1$ is trivial (if $K[\xi_1]$ is a field, then $1/\xi_1 = f(\xi_1) \in K[\xi_1]$ and hence $\xi_1$ is a root of the polynomial $xf(x) - 1$).

Granted that $H^3_{n-1}$ is true, let $R_n$ be a given finite integral domain $K[\xi_1, \xi_2, \cdots, \xi_n]$ and let it be assumed that $R_n$ is a field. Under this assumption we shall have $R_n = K(\xi_1)[\xi_2, \xi_3, \cdots, \xi_n]$, where $K(\xi_1)$ is the field generated over $K$ by $\xi_1$. Hence if we apply $H^3_{n-1}$ to $R_n$ thought of as an $R_{n-1}$ over the field $K(\xi_1)$, we conclude that $R_n$ is an algebraic extension of $K(\xi_1)$. To complete the proof of $H^3_n$ it remains only to
show that $\xi_1$ is algebraic over $K$.

Each $\xi_i$, $i = 2, 3, \ldots, n$, is a root of a polynomial $f_i(X)$ with coefficients in $K[\xi_1]$. Let $b_i$ be the leading coefficient of $f_i(X)$, $b_i \neq 0$. If $\omega$ is any element of $R_n$, there will exist an integer $p$ (depending on $\omega$) such that the product $\omega \cdot (b_2 b_3 \cdots b_n)^p$ can be expressed as a linear combination, with coefficients in $K[\xi_1]$, of the $m_2 m_3 \cdots m_n$ power products $\xi_2^j \xi_3^l \cdots \xi_n^m$, $0 \leq j, l \leq m_i - 1$, where $m_i$ is the degree of $f_i(X)$.

Let $\nu$ be the relative degree of $R_n$ over $K(\xi_1)$ and let $\omega_1 = 1$, $\omega_2$, $\ldots$, $\omega_n$ be a linear basis of $R_n$ over $K(\xi_1)$. We can find an element $b_1$ in $K[\xi_1]$, $b_1 \neq 0$, such that for each of the above $m_2 m_3 \cdots m_n$ power products $\xi_2^j \xi_3^l \cdots \xi_n^m$ the following is true: in the expression of $b_1 \cdot \xi_2^j \xi_3^l \cdots \xi_n^m$ as a linear combination of the elements $\omega_1$, $\omega_2$, $\ldots$, $\omega_n$, with coefficients in $K(\xi_1)$, the coefficient of $\omega_i$ is in $K[\xi_1]$. It follows that if we set $b = b_1 b_2 \cdots b_n$ then $b$ is an element of $K[\xi_1]$, different from zero, having the following property: for any element $\omega$ in $R_n$ there exists an integer $p$ such that if $\omega b^p = a_1 + a_2 \omega_2 + \cdots + a_n \omega_n$, $a_i \in K(\xi_1)$, then $a_1 \in K[\xi_1]$. Now let $\xi$ be an arbitrary element of $K[\xi_1]$, $\xi \neq 0$, and let us apply this result to $\omega = 1/\xi$. Since 1, $\omega_2$, $\ldots$, $\omega_n$ are independent over $K(\xi_1)$ and since $b^p/\xi \in K(\xi_1)$, it follows then that $b^p/\xi = a_1$, that is, any element $\xi$ of $K[\xi_1]$, $\xi \neq 0$, divides some power of the fixed element $b$ of $K[\xi_1]$. The existence of an element $b \neq 0$ with this property clearly implies that $K[\xi_1]$ cannot be a ring of polynomials in one indeterminate over $K$. Hence $\xi_1$ is algebraic over $K$, and this completes the proof of $H_1$.

2. Second proof. In this section we shall give a second proof of the Nullstellensatz. If we take for $\mathfrak{A}$ a prime ideal then $H_1$ yields the following result:

$H_\mathfrak{A}$: If $\mathfrak{p}$ is a prime ideal in $\mathfrak{U}$, then $\mathfrak{A}(\mathfrak{U}(\mathfrak{p})) = \mathfrak{p}$.

This is the most important consequence of the Nullstellensatz, since it shows that there exists a one-to-one correspondence between the irreducible varieties in $S_n$ and the prime ideals in $\mathfrak{U}_n$. It is therefore desirable to prove $H_\mathfrak{A}$ directly. On the other hand it is easy to deduce from $H_\mathfrak{A}$ the full Nullstellensatz. In fact, $H_\mathfrak{A}$ implies that if $\mathfrak{p} \neq (1)$ then $\mathfrak{U}(\mathfrak{p})$ is not empty. Since any ideal $\mathfrak{A}$ in $\mathfrak{U}_n$ which is different from the unit ideal is contained in some prime ideal $\mathfrak{p} \neq (1)$ (for instance in a maximal ideal), we see that from $H_\mathfrak{A}$ follows $H_2$, that is, the full Nullstellensatz.

We shall prove $H_\mathfrak{A}$ by induction with respect to $n$, since $H_\mathfrak{A}$ is trivial. The proof will be based on the following lemma:

**Lemma 1.** Let $\Omega$ be an integral domain and let $R$ be an integral domain contained in $\Omega$. If $\Omega$ is a simple ring extension of $R$: $\Omega = R[\omega]$, then there
exists in $R$ an element $a \neq 0$ with the following property: if $\mathfrak{p}$ is a prime ideal in $R$ such that $a \in \mathfrak{p}$, then $\Omega \cdot \mathfrak{p} \neq (1)$.

**Proof.** We shall use small Latin and Greek letters to indicate respectively elements of $R$ and $\Omega$. In the proof we may assume that $\omega$ is algebraic over $R$, since otherwise the assertion of the lemma is trivial (if $\omega$ is a transcendental over $R$ then $\Omega \mathfrak{A} \neq (1)$ for any ideal $\mathfrak{A}$ in $R$, $\mathfrak{A} \neq (1)$). Let

$$b_0 \omega^v + b_1 \omega^{v-1} + \cdots + b_v = 0, \quad b_0 \neq 0, b_i \in R,$$

be an equation of least degree $v$ which $\omega$ satisfies over $R$. If $\mathfrak{A}$ is any ideal in $R$ then any element $\xi$ of $\Omega \mathfrak{A}$ is of the form: $\xi = f(\omega)$, where $f$ is a polynomial with coefficients in $\mathfrak{A}$. If we use (1) to reduce the degree of $f$ we see that there exists an integer $\rho$ (depending on $\xi$) such that

$$\xi \cdot b_0^\rho = c_1 \omega^{r-1} + c_2 \omega^{r-2} + \cdots + c_v, \quad c_i \in \mathfrak{A}.$$

If the element $\xi$ also belongs to $R$, say $\xi = z$, then (2) is a relation of algebraic dependence for $\omega$ over $R$, of degree less than $v$. Hence necessarily $c_1 = c_2 = \cdots = c_{v-1} = 0$ and

$$zb_0^\rho = c_v \in \mathfrak{A}.$$

If $z = 1$ then (3) yields $b_0 \in \mathfrak{A}$, that is, $b_0$ is in the radical of $\mathfrak{A}$. Hence if the radical of $\mathfrak{A}$ does not contain $b_0$ then $\Omega \mathfrak{A} \neq (1)$. It follows that the element $b_0$ is an element $a$ the existence of which is asserted in the lemma.

We now come to the proof of $H^*_\mathfrak{A}$. Let $f(x)$ be an element of $\mathfrak{A}(\mathfrak{U}(\mathfrak{p}))$. We have to show that

$$f(x) \in \mathfrak{p}.$$  

We pass to the ring of residual classes $\Omega = \mathfrak{p}_n/\mathfrak{p} = K[\xi_1, \xi_2, \cdots, \xi_n]$, where $\xi_i$ is the $p$-residue of $x_i$. Let $\xi = f(\xi)$. We have to show that

$$\xi = 0.$$  

The case $\mathfrak{p} = (0)$ is trivial. Hence we may assume that $\mathfrak{p} \neq (0)$. In this case there exists a non-identical algebraic relation between the elements $\xi_1, \xi_2, \cdots, \xi_n$, with coefficients in $K$. We may therefore assume that $\xi_n$ is algebraically dependent on $\xi_1, \xi_2, \cdots, \xi_{n-1}$, over $K$. We set $R = K[\xi_1, \xi_2, \cdots, \xi_{n-1}]$. To our present two rings $R$ and $\Omega$ we apply Lemma 1. Let $a$ be an element of $R$, $a \neq 0$, the existence of which is asserted in the lemma.

We shall now show that if $H^*_{\mathfrak{A}}$ is granted, then the hypothesis that (5) is not satisfied leads to a contradiction. Every element of $\Omega$
is algebraic over \( R \). In particular, let

\[
(6) \quad d_0 \xi^r + d_1 \xi^{r-1} + \cdots + d_s = 0, \quad d_s \in R,
\]

be a relation of algebraic dependence for \( \xi \) over \( R \). Let us assume that

\( (5) \) is false: \( \xi \not\approx 0 \). Then we may also assume that \( d_s \neq 0 \). Since \( a \) and \( d_s \) are in \( R \), these elements can be expressed as polynomials in \( \xi_1, \xi_2, \cdots, \xi_{n-1} \), with coefficients in \( K \):

\[
(7) \quad a = g(\xi_1, \xi_2, \cdots, \xi_{n-1}), \quad a \neq 0;
\]

\[
(7a) \quad d_s = h(\xi_1, \xi_2, \cdots, \xi_{n-1}), \quad d_s \neq 0.
\]

Let \( f_1(x) = g(x)h(x) \in \mathcal{P}_{n-1} \), and let \( p_1 = p \cap \mathcal{P}_{n-1} \). It is clear that

\( R = \mathcal{P}_{n-1}/p_1 \) and that \( \xi_1, \xi_2, \cdots, \xi_{n-1} \) are the \( p_1 \)-residues of \( x_1, x_2, \cdots, x_{n-1} \). We shall show now that

\[
(8) \quad f_1(x) \in \mathfrak{I}(\mathcal{U}(p_1)).
\]

Let \( P_1(\alpha_1, \alpha_2, \cdots, \alpha_{n-1}) \) be any point of \( \mathcal{U}(p_1) \). If \( P_1 \) is a zero of the polynomial \( g(x) \) there is nothing to prove. Assume then that \( P_1 \) is not a zero of \( g(x) \). The ideal \( \mathfrak{I}(P_1) \) is a maximal (prime) ideal in \( \mathcal{P}_{n-1} \) which contains \( p_1 \), since \( P_1 \in \mathcal{U}(p_1) \). Hence if we set \( p_0 = \mathfrak{I}(P_1)/p_1 \), then \( p_0 \) is a maximal prime ideal in \( R \), and the assumption that \( P_1 \) is not a zero of \( g(x) \) signifies, in view of (7), that \( a \not\in p_0 \). Hence, by Lemma 1, the ideal \( \Omega \cdot p_0 \) is not the unit ideal. Let \( p'_0 \) be a maximal prime ideal in \( \Omega \) which contains the ideal \( \Omega \cdot p_0 \). Since \( p_0 \subseteq p'_0 \) and since \( p_0 \) is maximal in \( R \), it follows that \( p'_0 \cap R = p_0 \). Hence the \( p'_0 \)-residues of \( \xi_1, \xi_2, \cdots, \xi_{n-1} \) can be identified with their \( p_0 \)-residues, that is, with the algebraic quantities \( \alpha_1, \alpha_2, \cdots, \alpha_{n-1} \) respectively. Let \( \alpha_n \) be the \( p'_0 \)-residue of \( \xi_n \). Since \( K[\alpha_1, \alpha_2, \cdots, \alpha_{n-1}, \alpha_n]/\Omega/p'_0 \) is a field, \( \alpha_n \) is algebraically dependent on \( K[\alpha_1, \alpha_2, \cdots, \alpha_{n-1}] \), whence also \( \alpha_n \) is algebraic over \( K \). Hence \( \alpha_n = (\alpha_1, \alpha_2, \cdots, \alpha_{n-1}, \alpha_n) \) is a point of \( S_n \).

Since the coordinates of this point are residues of \( \xi_1, \xi_2, \cdots, \xi_n \) and since \( K[\xi_1, \xi_2, \cdots, \xi_n]/\mathfrak{P}/p \), it follows that the point \( P \) belongs to \( \mathcal{U}(p) \). Hence \( P \) is also a zero of the polynomial \( f(x) \), since, by hypothesis, \( f(x) \) vanishes on \( \mathcal{U}(p) \). This implies that \( \mathfrak{I}(f(\xi)) \), that is, \( \xi \), belongs to \( p_0 \). But then, in view of (6), also \( d_s \) belongs to \( p_0 \), and therefore, by (7a), \( h(\alpha) = 0 \), and this establishes (8).

3. **An application.** By the hypothesis \( \mathbb{A}_1 - 1 \) of our induction it follows from (8) that \( f_1(x) \) belongs to \( p_1 \). Hence \( f_1(\xi) = 0 \), that is, \( ad_0 = 0 \), in contradiction with \( a \neq 0 \) and \( d_s \neq 0 \). This completes the proof of \( \mathbb{A}_1 \).

We shall now proceed to the proof of the theorem stated in the introduction. Let \( R \) be a finite integral domain over \( K \):

\[
R = K[\xi_1, \xi_2, \cdots, \xi_n],
\]

and let \( K' \) be the set of elements of \( R \) which
are algebraic over $K$. It is clear that $K'$ is not only a ring but also a field, since if $\alpha \in K'$ then $K(\alpha) = K[\alpha]$. Since we have $R = K'[\xi_1, \xi_2, \ldots, \xi_n]$, we shall replace $K$ by $K'$. We assume therefore that $K$ is maximally algebraic in $R$ (that is, $K = K'$).

**Lemma 2.** $K$ is a maximal subfield of $R$.

**Proof.** Let $\mathfrak{p}$ be a fixed maximal prime ideal in $R$ and let $x$ be any element of $R$ which does not belong to $K$. By $H_\mathfrak{p}$ the field $R/\mathfrak{p}$ is an algebraic extension of $K$. Hence $x$ satisfies a congruence of the form: $f(x) \equiv 0 \pmod{\mathfrak{p}}$, where $f$ is a polynomial with coefficients in $K$, not all zero. Since $\mathfrak{p} \neq (1)$, $f(x)$ is not a unit in $R$. On the other hand since $K$ is maximally algebraic in $R$ and since $x \not\in K$, $x$ is a transcendental over $K$. Hence $f(x) \neq 0$. This shows that $K(x)$ is not contained in $R$. Since this is true for any element $x$ of $R$ which is not in $K$, the lemma follows.

**Corollary.** If $F$ is any subfield of $K$ such that $R$ is a finite integral domain over $F$, then the algebraic closure of $F$ in $R$ coincides with $K$.

For the algebraic closure of $F$ in $R$ is contained in $K$ and on the other hand it must be a maximal subfield of $R$, in view of Lemma 2.

We shall need the following generalization of Lemma 1:

**Lemma 3.** If an integral domain $\Omega$ is a finite ring extension of an integral domain $R$, then for any element $\alpha$ in $\Omega$, $\alpha \neq 0$, there exists a corresponding element $a$ in $R$, $a \neq 0$, having the following property: if the radical of an ideal $\mathfrak{a}$ in $R$ does not contain $a$, then the radical of $\mathfrak{a} \mathcal{O}_{R}$ does not contain $a$.

**Proof.** Let $\Omega$ be an $n$-fold ring extension of $R$. We shall prove the lemma by induction with respect to $n$.

**Case** $n = 1$. We use the notation of the proof of Lemma 1 and we consider separately two cases, according as $\omega$ is transcendental or algebraic with respect to $R$.

(a) $\omega$ is a transcendental over $R$. We have $\alpha = g(\omega)$, where $g$ is a polynomial with coefficients in $R$. Let $a$ be the leading coefficient of $g$, $a \neq 0$. If $\mathfrak{a}$ is an ideal in $R$ and if some power of $\alpha$ belongs to $\mathfrak{a}$, then the same power of $a$ must belong to $\mathfrak{a}$. Hence this element $a$ has the desired property.

(b) $\omega$ is algebraic over $R$. In this case also $\alpha$ is algebraic over $R$. Let $d_0 \alpha^n + d_1 \alpha^{n-1} + \cdots + d_n = 0$, $d_i \in R$, $d_n \neq 0$, be an equation of algebraic dependence for $\alpha$ over $R$. If some power $\alpha^\rho$ of $\alpha$ belongs to $\omega \mathfrak{a}$, then also $d_n^\rho$ belongs to $\omega \mathfrak{a}$, since $\alpha$ divides $d_n$ in $\Omega$. It follows from (3), for $\omega = d_n^\rho$, that $d_n^\rho b_0 \in \mathfrak{a}$, where $\rho$ is a suitable integer. Therefore if some power of $\alpha$ belongs to $\omega\mathfrak{a}$ then some power of
Case \( n > 1 \). Let \( \Omega = R[\xi_1, \xi_2, \ldots, \xi_n] \), \( \Omega_1 = R[\xi_1, \xi_2, \ldots, \xi_{n-1}] \), so that \( \Omega = \Omega_1[\xi_n] \). By the case \( n = 1 \), the lemma is applicable if we replace \( R \) by \( \Omega_1 \). Let \( \alpha_1 \) be an element of \( \Omega_1 \) which plays now the role of \( a \). By the case \( n - 1 \), the lemma is applicable if we replace \( \Omega \) by \( \Omega_1 \) and \( \alpha \) by \( \alpha_1 \). This yields an element \( \alpha \) of \( R, \alpha \neq 0 \), which has the desired property in relation to the rings \( R, \Omega \) and the given element \( \alpha \) of \( \Omega \). The proof of Lemma 3 is now complete.

We now go back to our original finite integral domain \( R = K[\xi_1, \xi_2, \ldots, \xi_n] \), where we assume that \( K \) is maximally algebraic in \( R \). We have to show that if \( F \) is a field contained in \( R \) then \( F \) is already contained in \( K \). Let \( x \) be an arbitrary element of \( R \) which does not belong to \( K \). We apply Lemma 3 to the two integral domains \( K[x] \) and \( R \) (these two rings now play respectively the role of the rings \( R \) and \( \Omega \) of the lemma). We take for \( \alpha \) the element 1 of \( R \) (nevertheless it is clear that our inductive proof of Lemma 3 could not have been carried out if we had restricted ourselves to the special case \( \alpha = 1 \)). In this special case, Lemma 3, and the fact that \( x \) is a transcendental over \( K \), yield the following result: there exists a polynomial \( g(x) \) in \( K[x] \) such that any irreducible polynomial in \( K[x] \) which does not divide \( g(x) \) is a nonunit in \( R \). Now let \( \Delta \) be the intersection of the two fields \( K \) and \( F \) (the two fields have in common at least the prime subfield of \( K \)). We can certainly find a polynomial in \( \Delta[x] \) which is relatively prime to \( g(x) \) in \( K[x] \). If \( f(x) \) is such a polynomial, then by the preceding result \( f(x) \) is a nonunit in \( R \). Consequently \( f(x) \) does not belong to the field \( F \), and since the coefficients of \( f(x) \) are in \( F \) it follows that \( x \) is not in \( F \). Since \( x \) was an arbitrary element of \( R \) not belonging to \( K \), we conclude that \( F \subseteq K \), q.e.d.

From the theorem just proved and from the corollary to Lemma 2 we draw immediately the following consequence:

If \( R \) is a finite integral domain over a field \( K \) and if \( F \) is any subfield of \( R \) such that \( R \) is a finite integral domain also over \( F \), then \( R \) has the same degree of transcendency over \( K \) as it has over \( F \).

This result is of course also a consequence of the fundamental theorem in the dimension theory of ideals in finite integral domains: if \( r \) is the degree of transcendency of \( R \) over \( K \) then every minimal prime ideal in \( R \) is of dimension \( r - 1 \). On the other hand, the above result gives an a priori reason for the fact that when the dimension of a prime ideal in \( R \) is defined relative to \( K \) as ground field, the resulting dimension theory is intrinsically related to \( R \).