POLYNOMIAL RINGS IN SEVERAL VARIABLES

Abstract. These are the notes prepared for the course MTH 751 to be offered to the PhD students at IIT Kanpur.

Contents

1. Rings

A *ring* is a set with two binary structures, say, $+$ and $\times$, which satisfy:

(1) $(R, +)$ is an abelian group with identity 0.
(2) $(R, \cdot)$ is an associative binary structure with identity 1.
(3) For all $a, b, c \in R$,

$$(a+b)\cdot c = a\cdot c + b\cdot c,\ \ c\cdot(a+b) = c\cdot a + c\cdot b.$$

A subset S of R is a *subring* if S is closed under addition, subtraction and multiplication, and contains 1.

Remark 1.1 : If $1 = 0$ then $R = \{0\}$: Note first that $0 \cdot a = 0$. Hence, if $a \in R$ then $a = 1 \cdot a = 0 \cdot a = 0$.

The set of integers $\mathbb{Z}$ is a ring with usual addition and multiplication.

Example 1.2 : Given a ring R, consider the set $R[x_1, \cdots, x_m]$ of polynomials in the variables $x_1, \cdots, x_m$ with coefficients from R. Then $R[x_1, \cdots, x_m]$ is a ring with usual addition and multiplication of polynomials. The additive identity is the constant polynomial 0 and the multiplicative identity is the constant polynomial 1. ■

A complex number α is called *algebraic* if there exists a non-zero $p \in \mathbb{Z}[x]$ such that $p(\alpha) = 0$. A number is called *transcendental* if it is not algebraic.

Any rational number is algebraic: If $\alpha = m/n$ for integer m and non-zero integer n then $p(x) = nx - m$ satisfies $p(\alpha) = 0$.

Example 1.3 : Note that the imaginary number i is algebraic: $x^2+1=0$ at $x=i$. Given a number α with a priori information that it is algebraic, it may not be easy to find a $p \in \mathbb{Z}[x]$ for which $p(\alpha)=0$. Sometimes, the following trick is helpful. Consider the number $\alpha = \sqrt{3}+\sqrt{-5}$. Then

$$\alpha - \sqrt{3} = \sqrt{-5} \Rightarrow \alpha^2 - 2\sqrt{3}\alpha + 3 = -5 \Rightarrow 2\sqrt{3}\alpha = \alpha^2 + 8 \Rightarrow 12\alpha^2 = (\alpha^2+8)^2.$$

It follows that the polynomial $p(x) = x^4 + 4x^2 + 64$ satisfies $p(\alpha) = 0$. ■

Exercise 1.4 : Show that the set of algebraic numbers is at most countable.

Let R and R' denote two rings. A *ring homomorphism or homomorphism* $\phi : R \to R'$ is a map which preserves addition and multiplication, and sends 1 to 1. An *isomorphism* is a bijective homomorphism.

Remark 1.5 : If ϕ is an isomorphism then the group structures $(R,+)$ and $(R',+)$ are isomorphic. In particular, $\phi(0)=0$.

Proposition 1.6. *Let α be a complex number. Define $\phi : \mathbb{Z}[x] \to \mathbb{Z}[\alpha]$ by $\phi(p) = p(\alpha)$, where $\mathbb{Z}[\alpha]$ is the smallest subring of $\mathbb{C}$ that contains α. Then ϕ is a surjective homomorphism. Moreover, ϕ an isomorphism if and only if α is a transcendental number.*

Proof. The first part is a routine verification. Thus it suffices to check that ϕ is injective if and only if α is not algebraic. If α is algebraic then there exists a non-zero $p \in \mathbb{Z}[x]$ such that $\phi(p)=0$. Also, ϕ being homomorphism, maps the zero polynomial to 0. Hence ϕ is not injective. Conversely, if ϕ is not injective then there exist $p \neq q \in \mathbb{Z}[x]$ such that $\phi(p) = \phi(q)$, that is, $\phi(p-q) = 0$ for the non-zero polynomial $p-q \in \mathbb{Z}[x]$. That is, α is algebraic. □

Next we present a substitution principle.

Proposition 1.7. *Let $\phi : R \to R'$ be a ring homomorphism. Given elements $a_1, \cdots, a_n \in R'$, there is a unique homomorphism $\Phi : R[x_1, \cdots, x_n] \to R'$, which agrees with ϕ on constant polynomials, and which sends x_i to a_i for each i.*

Proof. The desired homomorphism is given by

$$\Phi(\sum_{|\alpha| \leq k} c_\alpha x^\alpha) = \sum_{|\alpha| \leq k} \phi(c_\alpha) a^\alpha \text{ for } c_\alpha \in R.$$

Clearly, Φ is unique. □

Corollary 1.8. *There exists a unique isomorphism between the polynomial ring $R[x,y]$ and the ring $R[x][y]$ of polynomials in y with coefficients from $R[x]$, which is identity on R, and which sends x to x and y to y.*

Proof. Consider the inclusion map $\phi : R \to R[x][y]$. By the Substitution Principle 1.7, there exists a unique homomorphism $\Phi : R[x,y] \to R[x][y]$,

which agrees on constant polynomials, and which sends x to x and y to y. We check that Φ is the required isomorphism by displaying the inverse of Φ.

Note that $R[x]$ is a subring of $R[x, y]$. Thus we have an inclusion map $\psi : R[x] \to R[x, y]$. Apply the Substitution Principle to ψ to get an homomorphism $\Psi : R[x][y] \to R[x, y]$, which is identity on $R[x]$, and which sends y to y. Finally, note that $\Psi \circ \Phi$ is identity on R and $\{x, y\}$. By the uniqueness part of the Substitution Principle, $\Psi \circ \Phi$ is the identity map. This shows that Ψ is surjective. Another application of the Substitution Priciple shows that $\Phi \circ \Psi$ is the identity map. □

Let $\phi : R \to R'$ be a ring homomorphism. The *kernel* $\ker \phi$ of ϕ is given by $\{a \in R : \phi(a) = 0\}$.

Remark 1.9 : Since a ring homomorphism is also a group homomorphism, $\ker \phi$ is also an additive group. Note that for $a \in \ker \phi$ and $r \in R$, then $\phi(a \cdot r) = \phi(a) \cdot \phi(r) = 0 \cdot \phi(r) = 0$. Similarly, for $a \in \ker \phi$ and $r \in R$, $r \cdot a \in \ker \phi$. Note further that $\ker \phi$ is a subring if and only if $1 \in \ker \phi$ if and only if $\ker \phi = R$ if and only if ϕ is identically zero.

Example 1.10 : Consider the ring homomorphism $\phi : \mathbb{R}[x] \to \mathbb{R}$ defined by evaluation at a real number a. By the polynomial factor theorem, $\ker \phi$ precisely consists of polynomials divisible by $x - a$. ■

Example 1.11 : Consider the homomorphism ϕ from the ring $\mathcal{H}$ of holomorphic functions on the unit disc onto the ring of complex numbers $\mathbb{C}$ given by $\phi(f) = f(0)$, $f \in \mathcal{H}$. The kernel of ϕ consists precisely of all power series convergent on the unit disc with vanishing constant term. ■

A non-empty subset I of a ring R is said to be the *left ideal* if $\sum r_i \cdot a_i \in I$ for all finitely many $r_i \in R$ and $a_i \in I$. Similarly, one can define the *right ideal*. An *ideal* is the one which is both left and right ideal.

In a commutative ring, left and right ideals coincide. In the remaining part of these notes, all the rings are commutative.

Given elements $a_1, \cdots, a_k \in R$, the set

$$< a_1, \cdots, a_k >:= \left\{ \sum_{i=1}^{k} r_i \cdot a_i : r_1, \cdots, r_k \in R \right\}$$

defines a left ideal of R. We will refer to $< a_1, \cdots, a_k >$ as the *left ideal generated by* $a_1, \cdots, a_k$.

For example, if $R := \mathbb{R}[x_1, \cdots, x_k]$ and $a_i = x_i$ for $i = 1, \cdots, k$ then $< a_1, \cdots, a_k >$ is the kernel of the homomorphism of the evaluation at 0.

The ideal I in R is *principal* if there exists $a \in R$ such that $I =< a >$.

Every ideal in $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some integer n.

Proposition 1.12. *If $\mathbb{F}$ is a field then every ideal in $\mathbb{F}[x]$ is principal.*

Proof. Let I be a non-zero ideal of $\mathbb{F}[x]$. Let $k = \min\{\deg p : p \in I\}$ and let p be in I with degree k. Clearly, $< p > \subseteq I$. Let $g \in I$. By the Division Algorithm, $g = pq + r$, where $q, r \in \mathbb{F}[x]$ and $\deg r < k$. But then $r = g - pq \in I$ with degree less than k. This is possible provided $r = 0$. This gives the desired equality $I =< p >$. □

2. Quotient Rings

Let I be an ideal of a ring R. Since I is an additive group, so is the quotient R/I. Further, if $a + I, b + I \in R/I$ then R/I is a ring with multiplication: $(a + I) \cdot (b + I)$ is the (unique) coset $a \cdot b + I$ which contains it. Note that as subsets of R, $(a + I) \cdot (b + I)$ may be strictly contained in the coset $a \cdot b + I$. The additive identity of R/I is I and the multiplicative identity is $1 + I$. The quotient map $q : R \to R/I$ given by $q(a) = a + I$ is a ring homomorphism with kernel I.

Example 2.1 : Consider the ring $\mathcal{C}$ of convergent sequences of real numbers with termwise addition and multiplication. The mapping $\lim : \mathcal{C} \to \mathbb{R}$ given by $\lim\{c_n\} = \lim_{n\to\infty} c_n$ defines a ring homomorphism. The kernel of lim is the ideal $\mathcal{N}$ of null convergent sequences in $\mathcal{C}$. It is easy to see that $\mathcal{C}/\mathcal{N}$ is isomorphic to $\mathbb{R}$. ■

A ideal M of a ring R is said to be *maximal* if $M \subsetneq R$ but M is not contained in any ideals other than M and R.

Corollary 2.2. *Every ideal in $\mathbb{F}[x]$ which is generated by an irreducible polynomial is maximal.*

Proof. Let p be an irreducible polynomial in $\mathbb{F}[x]$ and let $< p >$ be the ideal generated by p. Suppose there exists an ideal I such that $< p > \subsetneq I \subseteq \mathbb{F}[x]$. By Proposition 1.12, there exists $q \in \mathbb{F}[x]$ such that $I =< q >$. But then $p = qr$ for some $r \in \mathbb{F}[x]$. Since p is irreducible and $< p > \subsetneq I$, q is a non-zero constant polynomial. Hence $I = \mathbb{F}[x]$. □

By the previous corollary, the ideal in $\mathbb{C}[z]$ generated by $z - a$ is maximal. The following natural question arises: Whether every maximal ideal M in $\mathbb{C}[z]$ arises in this way ? The answer is yes. Indeed, by Proposition 1.12, M in $\mathbb{C}[z]$ is generated by some $f \in \mathbb{C}[z]$. But then f has a root a in $\mathbb{C}$. It follows that $M \subseteq < z - a >$. Since M is maximal, we must have $M =< z - a >$.

We will later see that the last observation holds also for $\mathbb{C}[z_1, \cdots, z_n]$. This is a version of the celebrated Hilbert's Nullstellensatz.

Proposition 2.3. *Let R be a commutative ring. An ideal M of a ring R is maximal if and only if R/M is a field.*

Proof. Suppose R/M is a field. Let M' be an ideal such that $M \subseteq M'$. Then there is an $a \in M' \setminus M$. It follows that $a + M$ is a non-zero element of R/M. Thus there exists $b + M$ such that $(a + M) \cdot (b + M) = 1 + M$, that is, $ab - 1 \in M \subseteq M'$. Since $ab \in M'$, we get $1 \in M'$, and hence $M' = R$.

Conversely, suppose M is a maximal ideal of R. Let $a+M$ be a non-zero element of R/M. Then $a \notin M$. Thus the ideal I generated by M and a properly contains M. Since M is maximal, $I = R$. It follows that there exist $r \in R$ and $m \in M$ such that $1 = m + r_2 a$. Note that $r_2 + M$ is the desired inverse of $a + M$. □

Remark 2.4 : If I is an ideal in $\mathbb{F}[x]$ generated by an irreducible polynomial then $\mathbb{F}[x]/I$ is a field.

Exercise 2.5 : Let $a \in \mathbb{Q}$. Show that the quotient ring $\frac{\mathbb{Q}[x]}{<x-a>}$ is isomorphic to $\mathbb{Q}$ via the mapping $p \to p(a)$.

Example 2.6 : Consider the quotient ring $\mathbb{Q}[x]/I$, where $I =< x^2+1 >$. The mapping $p \to p(i)$ is an isomorphism between $\mathbb{Q}[x]/I$ and $\mathbb{C}$. In particular, $\mathbb{Q}[x]/I$ is a field. One can use this identification to find the inverse of a given coset in $\mathbb{Q}[x]/I$. For example, the inverse of $(x^4 - x^3 + x - 5) + I$ is the preimage of the inverse of $i^4 - i^3 + i - 5 = -4 + 2i$ under this isomorphism. Now the inverse of $-4+2i$ is $\frac{-2-i}{2\sqrt{5}}$. Hence the inverse of $(x^4 - x^3 + x - 5) + I$ is the coset $\frac{-2-x}{2\sqrt{5}} + I$. ■

The first isomorphism theorem for rings says that for a surjective ring homomorphism $\phi : R \to R'$, the quotient ring $R/\ker\phi$ is isomorphic to R'. We skip its routine verification.

Example 2.7 : Consider the ring homomorphism $\phi : \mathbb{R}[x,y] \to \mathbb{R}[t]$ given by $\phi(x) = t^2$, $\phi(y) = t$ and $\phi(a) = a$ for $a \in \mathbb{R}$. We claim that the quotient ring $\mathbb{R}[x,y]/I$ is isomorphic to $\mathbb{R}[t]$, where $I =< x - y^2 >$. By the first isomorphism theorem, it suffices to check that $\ker\phi = I$. Clearly, $x - y^2 \in \ker\phi$, and hence $I \subseteq \ker\phi$. To see that $\ker\phi \subseteq I$, let $f \in \ker\phi$. Consider the quotient ring $\mathbb{R}[x,y]/I$ and the coset $f+I$. Since $\mathbb{R}[x,y] = \mathbb{R}[x][y]$ (Corollary 1.8), $f(x,y) = \sum_{i=0}^{2k} f_i(x)y^i$ for $f_1, \cdots, f_{2k} \in \mathbb{R}[x]$. It follows that

$$\begin{aligned} f(x,y) &= \sum_{i=0}^{2k} f_i(x)y^i \\ &= f_0(x) + (f_1(x) + f_3(x)y^2 + \cdots + f_{2k-1}(x)y^{2k-2})y \\ &+ (f_2(x)y^2 + f_4(x)y^4 + \cdots + f_{2k}(x)y^{2k}). \end{aligned}$$

Thus $f + I$ is same as the coset containing the polynomial

$$f_0(x)+(f_1(x)+f_3(x)x+\cdots+f_{2k-1}(x)x^{k-1})y+(f_2(x)x+f_4(x)x^2+\cdots+f_{2k}(x)x^k),$$

which is of the form $p(x) + yq(x)$ for some polynomials $p, q \in \mathbb{R}[x]$. Thus $f(x,y) = p(x) + yq(x) + h(x,y)$ with $h \in I$. Now since $f, h \in \ker\phi$, we obtain $0 = \phi(f(x,y)) = p(\phi(x)) + \phi(y)q(\phi(x)) + \phi(h(x,y)) = p(t^2) + tq(t^2)$. Since there are no common powers in the polynomials $p(t^2)$ and $tq(t^2)$, this is possible provided $p = 0 = q$. Thus $f = h$ belongs to I, and the claim stands verified. ■

Example 2.8 : Consider the quotient ring $\mathbb{Z}[i]/I$, where $I =< 1+3i >$. In this quotient ring, $1+3i = 0$, that is, $i = 3$ or $10 = 0$. Indeed, $\mathbb{Z}[i]/I$ is isomorphic to the quotient ring $\mathbb{Z}/10\mathbb{Z}$. To see this, define the ring homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}[i]/I$ by $\phi(n) = n + I$. By the first isomorphism theorem, the image of ϕ is isomorphic to $\mathbb{Z}/\ker\phi$. We check that ϕ is surjective and $\ker\phi = 10\mathbb{Z}$. Since $a+bi$ and $a+3b$ belong to the same coset in $\mathbb{Z}[i]/I$, $\phi(a+3b) = a+ib$. Thus ϕ is surjective. Note further that if $n \in 10\mathbb{Z}$ then $n = 10m$ for some integer m, and hence $\phi(n) = 10m + I = I$. Also, if $n \in \ker\phi$ then $n \in I$, that is, $n = (a+ib)(1+3i) = (a-3b)+(3a+b)i$ for some integers a, b, and hence $3a + b = 0$ forcing $n = a - 3b = 10a \in 10\mathbb{Z}$. ■

Exercise 2.9 : Let I (resp. J) denote the ideal $< x^3 + x + 1, 5 >$ (resp. $< x^3 + x + 1 >$) in $\mathbb{Z}[x]$. Verify:

(1) The polynomial $x^3 + x + 1$ is irreducible in $\mathbb{Z}_5[x]$.
(2) The quotient rings $\mathbb{Z}[x]/I$ and $\mathbb{Z}_5[x]/J$ are isomorphic.
(3) The quotient ring $\mathbb{Z}[x]/I$ is a field.
(4) The ideal I is maximal in $\mathbb{Z}[x]$.

A non-zero ring R is an integral domain if it is without zero divisors: If $ab = 0$ for $a, b \in R$ then either $a = 0$ or $b = 0$.

An integral domain satisfies the cancellation law: If $a \cdot b = a \cdot c$ with $a \neq 0$ then $a \cdot (b - c) = 0$, and hence $b = c$.

Proposition 2.10. *If R is an integral domain, the so is the polynomial ring $R[x_1, \cdots, x_n]$.*

Proof. Suppose that $f, g \in R[x]$. Suppose the degree of f is p and the degree of g is q. If R is an integral domain then the degree of fg is $p + q$. In particular, $R[x]$ is an integral domain. The desired conclusion now follows from Corollary 1.8 by a finite induction. □

For an ideal I in R, consider the quotient ring R/I. Suppose R/I is an integral domain, that is, if $(a + I) \cdot (b + I) = I$ then either $a + I = I$ or $b + I = I$. This happens if and only if $ab \in I$ implies either $a \in I$ or $b \in I$. This motivates the definition of prime ideal:

An ideal I is said to be a *prime ideal* if $ab \in I$ then either $a \in I$ or $b \in I$.

Proposition 2.11. *An ideal M of a ring R is prime if and only if R/M is an integral domain.*

Example 2.12 : The ideal $I =< x - y^2 >$ in $\mathbb{R}[x, y]$ is a prime ideal. This follows from Example 2.7, where we observed that $\mathbb{R}[x, y]/I$ being isomorphic to $\mathbb{R}[t]$ is an integral domain. ■

3. Hilbert Basis Theorem

A ring R is said to be *Noetherian* if every ideal of R is finitely generated, that is, for any ideal I of R there exist $f_1, \cdots, f_k \in I$ such that

$$I = \{g_1 f_1 + \cdots + g_k f_k : g_1, \cdots, g_k \in R\}.$$

Any field F is Noetherian as the only ideals of F are $\{0\}$ and F, which are generated by 0 and 1 respectively.

Lemma 3.1. *Suppose R is a Noetherian ring. Suppose $a_1, a_2, \cdots, \in R$. Then there exists an integer m such that*

$$a_m \in I_m :=< a_1, \cdots, a_{m-1} > .$$

Proof. Since $I_l \subseteq I_{l+1}$ for each l, the union $I := \cup_{l=1}^{\infty} I_l$ is an ideal. Since R is Noetherian, I is finitely generated with generators $b_1, \cdots, b_k$ belonging to some I_l. Thus $I = \cup_{j=1}^{k} I_{i_j}$. If $m = \max\{i_1, \cdots, i_k\}$ then $a_m \in I = I_m$. □

The following is commonly known as the Hilbert Basis Theorem.

Theorem 3.2. *If R is Noetherian then so is the polynomial ring $R[x]$.*

Proof. (H. Sarges, [4, 1.C.4]) Let J be an ideal in $R[x]$. Suppose J is not finitely generated. Then one can choose $f_1, f_2, \cdots$, inductively such that f_n is of smallest degree in $J \setminus J_n$, where $J_n :=< f_1, \cdots, f_{n-1} > .$ Suppose f_n is of degree d_n and with the leading coefficient $a_n \in R$. Clearly, $d_1 \leq d_2 \leq \cdots$. Since R is Noetherian, by Lemma 3.1, there exists an integer m such that $a_m = a_1 b_1 + \cdots a_{m-1} b_{m-1}$ for some $b_1, \cdots, b_{m-1}$ in R. Note that $g := f_m - \sum_{i=1}^{m-1} b_i x^{d_m - d_i} f_i \in J \setminus J_m$ with degree less than d_m. This contradicts the choice of f_m. □

A finite induction argument combine with Corollary 1.8 immediately yields the following:

Corollary 3.3. *If R is Noetherian then so is the polynomial ring $R[x_1, \cdots, x_n]$.*

Firstly, the Hilbert's Basis Theorem (HBT) provides a simple way to generate Noetherian rings. Secondly, its importance lies in its obvious connection with the study of common zero sets of polynomials.

Example 3.4 : Let $\mathcal{F} \subseteq \mathbb{F}[x_1, \cdots, x_n]$ be an arbitrary family of polynomials. Consider the ideal $I_{\mathcal{F}}$ generated by the elements in $\mathcal{F}$. By Hilbert Basis Theorem, there exist finitely many polynomials $p_1, \cdots, p_k \in \mathbb{F}[x]$ such that $I_{\mathcal{F}} =< p_1, \cdots, p_k > .$ We claim that the common zero set

$$Z(I_{\mathcal{F}}) = \{x \in p(x) = 0 \text{ for every } p \in \mathcal{F}\}$$

is same as the common zero set $Z(p_1, \cdots, p_k)$ of $p_1, \cdots, p_k$. Clearly, $Z(\mathcal{F}) \subseteq Z(p_1, \cdots, p_k)$. Also, if $x \in Z(p_1, \cdots, p_k)$ then $p_1(x) = 0, \cdots, p_k(x) = 0$, and hence $p(x) = 0$ for every p in $I_{\mathcal{F}}$. ■

4. Hilbert's Nullstellensatz

We start with the easier half of Hilbert's Nullstellensatz.

Lemma 4.1. *For $a = (a_1, \cdots, a_n) \in \mathbb{C}^n$, consider the ideal I_a in $\mathbb{C}[z_1, \cdots, z_n]$ generated by $z_1 - z_1, \cdots, z_n - a_n$. Then the ideal I_a is maximal.*

Proof. Consider the evaluation ring homomorphism $e_a : \mathbb{C}[z_1, \cdots, z_n] \to \mathbb{C}$ given by $e_a(f) = f(a)$. Since e_a is surjective, by the first isomorphism theorem, $\mathbb{C}[z_1, \cdots, z_n]/\ker e_a$ is isomorphic to the field $\mathbb{C}$. In particular, $\ker e_a$ is a maximal ideal in $\mathbb{C}[z_1, \cdots, z_n]$. To prove that I_a is a maximal ideal in $\mathbb{C}[z_1, \cdots, z_n]$, it suffices to check that $I_a = \ker e_a$. We expand $f \in \mathbb{C}[z_1, \cdots, z_n]$ about a as follows:

$$f(z) = f(a) + \sum_{i=1}^{n} \beta_i (z_i - a_i) + \sum_{i \leq j = 1}^{n} \gamma_{i,j} (z_i - a_i)(z_j - a_j) + \cdots .$$

The right hand side of the last identity consists only finitely many terms as f is a polynomial. It is now clear that $f \in \ker e_a$ if and only if $f \in I_a$. □

The other half of Hilbert's Nullstellensatz is quite difficult and needs more preparation. The following change of variable makes life easy.

Lemma 4.2. *Suppose that $f \in \mathbb{C}[z_1, \cdots, z_n]$ is of total degree d. Then one can find scalars $\lambda_1, \cdots, \lambda_{n-1} \in \mathbb{C}$ such that the coefficient of z_n^d in $f(z_1 + \lambda_1 z_n, \cdots, z_{n-1} + \lambda_{n-1} z_n, z_n)$ is non-zero. In particular, the mapping $f(z_1, \cdots, z_n) \rightsquigarrow f(z_1 + \lambda_1 z_n, \cdots, z_{n-1} + \lambda_{n-1} z_n, z_n)$ is a ring isomorphism from $\mathbb{C}[z_1, \cdots, z_n]$ onto itself.*

Proof. Let f_d denote the homogeneous component of $f = g + f_d$ of degree d. Since $f_d \neq 0$, there exists $w \in \mathbb{C}^n$ such that $f_d(w) \neq 0$. By the continuity of f_d, we may assume that $w_n \neq 0$. Put $\lambda_i := w_i / w_n,\ i = 1, \cdots, n-1$. Note that the coefficient of z_n^d in $f(z_1 + \lambda_1 z_n, \cdots, z_{n-1} + \lambda_{n-1} z_n, z_n)$ is

$$f_d(\lambda_1, \cdots, \lambda_{n-1}, 1) = f_d(w_1/w_n, \cdots, w_{n-1}/w_n, 1) = \frac{1}{w_n^d} f_d(w),$$

which is non-zero by our choice. Since the transformation $(z_1, \cdots, z_n) \rightsquigarrow (z_1 + \lambda_1 z_n, \cdots, z_{n-1} + \lambda_{n-1} z_n, z_n)$ is bijective, the remaining part follows. □

Lemma 4.3. *Let I be an ideal of $\mathbb{C}[z_1, \cdots, z_n]$. Consider the polynomials $f = f_0 + f_1 z_n + \cdots f_d z_n^d$ and $g = g_0 + g_1 z_n + \cdots g_e z_n^e$ of degree d and e respectively in $\mathbb{C}[z_1, \cdots, z_{n-1}][z_n]$. Define $R(f, g)$ as the determinant of the*

$(d+e)\times(d+e)$ *matrix*

$$\begin{bmatrix} f_0 & f_1 & \cdots & f_d & 0 & 0 & \cdots & 0 \\ 0 & f_0 & \cdots & f_{d-1} & f_d & 0 & \cdots & 0 \\ & & \ddots & & & \ddots & & \\ 0 & \cdots & 0 & f_0 & f_1 & \cdots & f_{d-1} & f_d \\ g_0 & g_1 & \cdots & g_{e-1} & g_e & 0 & \cdots & 0 \\ & \ddots & & & & \ddots & & \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{e-1} & g_e \end{bmatrix}$$

If $f, g \in I$ then so does $R(f,g)$.

Proof. Since the determinant is unchanged by the elementary column operations, we take determinant after performing the following operations $C_1 \hookrightarrow C_1 + z_n^i C_i$, $i = 2, \cdots, d+e-1$. Note that the entries of the first column are $f, z_n f, z_n^2 f, \cdots, z_n^{d-1} f, g, z_n g, \cdots, z_n^{e-1} g$. It now clear that $R(f,g)$ belongs to the ideal generated by f and g. □

Theorem 4.4. *(Hilbert Nullstellensatz, Weak Form) The maximal ideals of the polynomial ring $\mathbb{C}[z_1, \cdots, z_m]$ are in bijective correspondence with the points of the complex n-dimensional space $\mathbb{C}^n$ via the mapping*

$$(a_1, \cdots, a_n) \rightsquigarrow < z_1 - a_1, \cdots, z_n - a_n > .$$

Proof. (E. Arrondo) In view of Lemma 4.1, it suffices to prove that every maximal ideal I of $\mathbb{C}[z_1, \cdots, z_n]$ is of the form $I_a :=< z_1 - a_1, \cdots, z_n - a_n >$ for some $a \in \mathbb{C}^n$. We prove this by induction on n. The case $n = 1$ is already discussed in the discussion following Corollary 2.2. Suppose $n > 1$ and assume that the conclusion holds for $n-1$ variables. Let I be an ideal in $\mathbb{C}[z_1, \cdots, z_n]$. By Lemma 4.2, we may assume that I contains a monic polynomial g in z_n:

$$g(z', z_n) = g_0(z') + g_1(z')z_n + \cdots + g_{e-1}(z')z_n^{e-1} + z_n^l, z' = (z_1, \cdots, z_{n-1}),$$

where $g_0, \cdots, g_{e-1} \in \mathbb{C}[z_1, \cdots, z_{n-1}]$.

Consider the ideal

$$I' := \{f \in I : \partial f / \partial z_n = 0\}$$

of the subring $\mathbb{C}[z_1, \cdots, z_{n-1}]$. Since $1 \in I$ if and only if $1 \in I'$, I' is a proper ideal of $\mathbb{C}[z_1, \cdots, z_{n-1}]$. By the induction hypothesis, there exists $a' = (a_1, \cdots, a_{n-1}) \in \mathbb{C}^{n-1}$ such that $I' =< z_1 - a_1, \cdots, z_{n-1} - a_{n-1} > .$

Consider now the ideal

$$I'' := \{f(a_1, \cdots, a_{n-1}, z_n) : f \in I\}$$

of the ring $\mathbb{C}[z_n]$. We claim that I'' is a proper ideal of $\mathbb{C}[z_n]$. Suppose to the contrary that $1 \in I''$. Then there exists $f \in I$ such that $f(a_1, \cdots, a_{n-1}, z_n) = 1$. Write $f(z', z_n) = f_0(z') + f_1(z')z_n^2 + \cdots + f_d(z')z_n^d$, where $f_0, \cdots, f_d \in \mathbb{C}[z_1, \cdots, z_{n-1}]$ are such that $f_1(a') = 1$ and $f_i(a') = 0$ for $i = 2, \cdots, d$. By Lemma 4.3, $R(f, g) \in I$. Since $R(f, g)$ is independent of z_n, $R(f, g) \in I' =< z_1 - a_1, \cdots, z_{n-1} - a_{n-1} >$. This is impossible since $R(f, g)(a') = 1$. Thus we obtain a contradiction, and hence the claim stands verified. Thus I'' is a proper ideal of $\mathbb{C}[z_n]$. Hence, by the case $n = 1$, there exists $a_n \in \mathbb{C}$ such that $I'' =< z_n - a_n >$. It now follows that I is generated by $z_1 - a_1, \cdots, z_n - a_n$. □

Remark 4.5 : Let I be a proper ideal of $\mathbb{C}[z_1, \cdots, z_n]$. Then the common zero set $Z(I)$ of members of I is non-empty. Indeed, since I is contained in some maximal ideal J. By the Hilbert Nullstellensatz, J generated by $z_1 - a_1, \cdots, z_n - a_n$ for some $a \in \mathbb{C}^n$. It follows that $a \in Z(I)$.

Corollary 4.6. *Let $f_1, \cdots, f_k \in \mathbb{C}[z_1, \cdots, z_n]$ be such that they have no common zero. Then there exist $g_1, \cdots, g_k \in \mathbb{C}[z_1, \cdots, z_n]$ such that*

$$f_1 g_1 + \cdots + f_k g_k = 1.$$

Proof. Consider the ideal I generated by $f_1, \cdots, f_k$. If I is a proper ideal then by the last theorem, $f_1, \cdots, f_k$ would have a common zero. In view of the hypothesis, the only possibility left is $I = \mathbb{C}[z_1, \cdots, z_n]$. Thus $1 \in I$, and the desired conclusion follows. □

Example 4.7 : Consider the polynomials $f(z_1, z_2) = z_1^2 + z_2^2 - 1, g(z_1, z_2) = z_1^2 - z_2 + 1, h(z_1, z_2) = z_1 z_2 - 1$. We show that the ideal generated by f, g, h is $\mathbb{C}[z_1, z_2]$. In view of the last corollary, it suffices to check that the common zero set of f, g, h is empty. To see that, let us solve the system

$$z_1^2 + z_2^2 = 1, z_1^2 + 1 = z_2, z_1 z_2 = 1.$$

By solving first two equations, we obtain $z_1^2(3 + z_1^2) = 0$. This forces $z_1 = 0$ or $z_1^2 = 3i$. It is easy to see that (z_1, z_2) does not satisfy $z_1 z_2 = 1$ and $z_1^2 + z_2^2 = 1$ simultaneously. ■

Note that the conclusion of Remark 4.5 raises the following interesting question: If I is a proper ideal of $\mathbb{C}[z_1, \cdots, z_n]$ and J denotes the ideal of all polynomials vanishing on $Z(I)$, then clearly $I \subseteq J$. Note also that if $f \in \mathbb{C}[z_1, \cdots, z_n]$ such that $f^m \in I$ for some positive integer m then $f \in J$. It is evident that, in general, $I \subsetneq J$ (e.g. $I =< z^2 >$ then $J =< z >$ in $\mathbb{C}[z]$). How to obtain J from I ?

Corollary 4.8. *(Hilbert Nullstellensatz) Suppose that I is a proper ideal of $\mathbb{C}[z_1, \cdots, z_n]$. Let J denote the ideal of all polynomials vanishing on $Z(I)$. Then $J = \{f \in \mathbb{C}[z_1, \cdots, z_n] : f^m \in I$ for some positive integer $m\}$.*

Proof. (J. Rabinowitsch, [5]) In view of the preceding discussion, it suffices to check that if $f \in J$ then $f^m \in I$ for some positive integer m. Fix $f \in J$ and introduce a new variable z_0. Consider the ideal K generated by I and $1 - z_0 f \in \mathbb{C}[z_0, z_1, \cdots, z_n]$. Since $Z(I) \cap Z(1 - z_0 f) = \emptyset$, by Theorem 4.4, $K = \mathbb{C}[z_0, z]$, where $z = (z_1, \cdots, z_n)$. Thus there exist $p \in I$ and $q, r \in \mathbb{C}[z_0, z]$ such that

$$pq + r(1 - z_0 f) = 1. \tag{4.1}$$

Consider the ring homomorphism $e : \mathbb{C}[z_0, z] \to \mathbb{C}[z]$ given by

$$\phi : g(z_0, z) \rightsquigarrow g(-1/f, z) \text{ for } g \in \mathbb{C}[z_0, z].$$

Since $\phi(1 - z_0 f) = 0$ and $\phi(p) = p$, by applying ϕ on both sides of (4.1), we obtain $p(z)q(-1/f, z) = \phi(1) = 1$. It follows that $p\frac{\tilde{q}}{f^m} = 1$ for some $\tilde{q} \in \mathbb{C}[z]$ and positive integer m. Thus $f^m \in I$ as desired. □

References

[1] E. Arrondo, *Another Elementary Proof of the Nullstellensatz*, Amer. Math. Monthly, February, 2006, 169-171.

[2] M. Artin, *Algebra*, Eastern Economy Edition, 1996.

[3] S. Kumaresan, *How to work with quotient rings: Expository Articles (Level 2)*, private communication.

[4] D. Patil and U. Storch, *Introduction to algebraic geometry and commutative algebra*, IISc Lecture Notes Series, 2010.

[5] K. Pommerening, *Hilbert's Nullstellensatz over the complex numbers*, available online, 1982.