Algebraic Geometry 2
Tutorial session 1

Lecturer: Rami Aizenbud
TA: Shai Shechter

April 24, 2020

Introduction

Introduction

Unless otherwise stated, all rings in this semester are commutative and unital.

Recollections from Algebraic Geometry

Recall

Definition (Noetherian ring)

A ring R is *noetherian* if it satisfies any of the following conditions:

1. R satisfies the ascending chain condition (ACC): for any chain of ideals $I_1 \subseteq I_2 \subseteq \cdots \subseteq R$ there exists $n_0 \in \mathbb{N}$ such that $I_n = I_{n+1} = \cdots$;

Recollections from Algebraic Geometry

Recall

Definition (Noetherian ring)

A ring R is *noetherian* if it satisfies any of the following conditions:

1. R satisfies the ascending chain condition (ACC): for any chain of ideals $I_1 \subseteq I_2 \subseteq \cdots \subseteq R$ there exists $n_0 \in \mathbb{N}$ such that $I_n = I_{n+1} = \cdots$;
2. Any ideal $I \lhd R$ is finitely generated, i.e. $I = a_1 R + \cdots + a_n R$ for $a_1, \ldots, a_n \in R$; and

Recollections from Algebraic Geometry

Recall

Definition (Noetherian ring)

A ring R is *noetherian* if it satisfies any of the following conditions:

1. R satisfies the ascending chain condition (ACC): for any chain of ideals $I_1 \subseteq I_2 \subseteq \cdots \subseteq R$ there exists $n_0 \in \mathbb{N}$ such that $I_n = I_{n+1} = \cdots$;
2. Any ideal $I \triangleleft R$ is finitely generated, i.e. $I = a_1 R + \cdots + a_n R$ for $a_1, \ldots, a_n \in R$; and
3. Every non-zero set of ideal of R has a maximal element with respect to inclusion.

Exercise

Show that the three conditions above are equivalent.

Solution.

1. (1)$\Rightarrow$(2): Assume towards contradiction $I \lhd R$ is not finitely generated.

Exercise

Show that the three conditions above are equivalent.

Solution.

1. (1)$\Rightarrow$(2): Assume towards contradiction $I \lhd R$ is not finitely generated. Then, arguing by induction, we can find a sequence $(a_n)_n$ of elements of I such that $\forall k : a_k \notin (a_1 R + \cdots + a_{k-1} R)$.

Exercise

Show that the three conditions above are equivalent.

Solution.

1. (1)$\Rightarrow$(2): Assume towards contradiction $I \triangleleft R$ is not finitely generated. Then, arguing by induction, we can find a sequence $(a_n)_n$ of elements of I such that $\forall k : a_k \notin (a_1 R + \cdots + a_{k-1} R)$. Putting $I_k = a_1 R + \cdots + a_k R$, we get a non-stabilizing sequence of ideals.

Exercise

Show that the three conditions above are equivalent.

Solution.

1. (1)⇒(2): Assume towards contradiction $I \triangleleft R$ is not finitely generated. Then, arguing by induction, we can find a sequence $(a_n)_n$ of elements of I such that $\forall k : a_k \notin (a_1 R + \cdots + a_{k-1} R)$. Putting $I_k = a_1 R + \cdots + a_k R$, we get a non-stabilizing sequence of ideals.
2. (2)⇒(3) Let $\mathcal{I}$ be a non-empty set of ideals of R and take $\mathcal{C} \subseteq \mathcal{I}$ to be a maximal chain.

Exercise

Show that the three conditions above are equivalent.

Solution.

1. (1)⇒(2): Assume towards contradiction $I \triangleleft R$ is not finitely generated. Then, arguing by induction, we can find a sequence $(a_n)_n$ of elements of I such that $\forall k : a_k \notin (a_1 R + \cdots + a_{k-1} R)$. Putting $I_k = a_1 R + \cdots + a_k R$, we get a non-stabilizing sequence of ideals.
2. (2)⇒(3) Let $\mathcal{I}$ be a non-empty set of ideals of R and take $\mathcal{C} \subseteq \mathcal{I}$ to be a maximal chain. Note that $I_C = \bigcup_{J \in \mathcal{C}} J$ is an ideal of R as well, and hence finitely generated. Therefore, $\exists I_1, \ldots, I_n \in \mathcal{C}$ and $a_i \in I_i$ such that $I_C = a_1 R + \cdots + a_n R$.

Exercise

Show that the three conditions above are equivalent.

Solution.

1. (1)⇒(2): Assume towards contradiction $I \triangleleft R$ is not finitely generated. Then, arguing by induction, we can find a sequence $(a_n)_n$ of elements of I such that $\forall k : a_k \notin (a_1 R + \cdots + a_{k-1} R)$. Putting $I_k = a_1 R + \cdots + a_k R$, we get a non-stabilizing sequence of ideals.
2. (2)⇒(3) Let $\mathcal{I}$ be a non-empty set of ideals of R and take $\mathcal{C} \subseteq \mathcal{I}$ to be a maximal chain. Note that $I_C = \bigcup_{J \in \mathcal{C}} J$ is an ideal of R as well, and hence finitely generated. Therefore, $\exists I_1, \ldots, I_n \in \mathcal{C}$ and $a_i \in I_i$ such that $I_C = a_1 R + \cdots + a_n R$. Assuming $I_1 \subseteq \cdots \subseteq I_n$, it follows that $I_C = I_n \in \mathcal{C}$.

$\square$

Exercise

Show that the three conditions above are equivalent.

Solution.

1. (1)$\Rightarrow$(2): Assume towards contradiction $I \triangleleft R$ is not finitely generated. Then, arguing by induction, we can find a sequence $(a_n)_n$ of elements of I such that $\forall k : a_k \notin (a_1 R + \cdots + a_{k-1} R)$. Putting $I_k = a_1 R + \cdots + a_k R$, we get a non-stabilizing sequence of ideals.
2. (2)$\Rightarrow$(3) Let $\mathcal{J}$ be a non-empty set of ideals of R and take $\mathcal{C} \subseteq \mathcal{J}$ to be a maximal chain. Note that $I_C = \bigcup_{J \in \mathcal{C}} J$ is an ideal of R as well, and hence finitely generated. Therefore, $\exists I_1, \ldots, I_n \in \mathcal{C}$ and $a_i \in I_i$ such that $I_C = a_1 R + \cdots + a_n R$. Assuming $I_1 \subseteq \cdots \subseteq I_n$, it follows that $I_C = I_n \in \mathcal{C}$.
3. (3)$\Rightarrow$(1) Obvious.

$\square$

Exercise

Let R be a notherian ring, and let $(a_i)_{i=1}^{\infty}$ be a sequence in R. Then there exists $n_0 \in \mathbb{N}$ such that $(a_i)_{i=1}^{\infty}$ is included in $a_1 R + \ldots + a_{n_0} R$.

Exercise

Let R be a notherian ring, and let $(a_i)_{i=1}^{\infty}$ be a sequence in R. Then there exists $n_0 \in \mathbb{N}$ such that $(a_i)_{i=1}^{\infty}$ is included in $a_1 R + \ldots + a_{n_0} R$. That is, for any $k \in \mathbb{N}$, there exist $r_1, \ldots, r_{n_0} \in R$ such that $a_k = \sum_{i=1}^{n_0} r_i a_i$.

Exercise

Let R be a notherian ring, and let $(a_i)_{i=1}^{\infty}$ be a sequence in R. Then there exists $n_0 \in \mathbb{N}$ such that $(a_i)_{i=1}^{\infty}$ is included in $a_1 R + \ldots + a_{n_0} R$. That is, for any $k \in \mathbb{N}$, there exist $r_1, \ldots, r_{n_0} \in R$ such that $a_k = \sum_{i=1}^{n_0} r_i a_i$.

Solution.

The sequence of ideals $I_k = \langle a_1, \ldots, a_k \rangle$ is ascending and hence stabilizes. In particular, taking n_0 to be such that $I_{n_0} = I_{n_0+1} = \cdots$, for any $k > n_0$ we have $a_k \in I_k = I_{n_0}$. $\square$

Theorem (Hilbert Basis Theorem)

Let R be a noetherian ring. Then $R[x]$, the ring of polynomials over R, is also noetherian.

Theorem (Hilbert Basis Theorem)

Let R be a noetherian ring. Then $R[x]$, the ring of polynomials over R, is also noetherian.

Corollary

The ring $k[x_1, \ldots, x_n]$ is noetherian for any field k and $n \in \mathbb{N}$.

Proof of HBT

Let I be an ideal of $R[x]$.

Proof of HBT

Let I be an ideal of $R[x]$. We want to show I is finitely generated.

Proof of HBT

Let I be an ideal of $R[x]$. We want to show I is finitely generated. Pick a sequence $(f_i)_{i=1}^{n}$ of polynomials in I in the following manner:

Proof of HBT

Let I be an ideal of $R[x]$. We want to show I is finitely generated. Pick a sequence $(f_i)_{i=1}^{n}$ of polynomials in I in the following manner:

- Take f_1 to be a polynomial of minimal degree in I.

Proof of HBT

Let I be an ideal of $R[x]$. We want to show I is finitely generated. Pick a sequence $(f_i)_{i=1}^n$ of polynomials in I in the following manner:

- Take f_1 to be a polynomial of minimal degree in I.
- If $I = \langle f_1 \rangle$ we are done; otherwise, take $f_2 \in I \setminus \langle f_1 \rangle$ of minimal degree.

Proof of HBT

Let I be an ideal of $R[x]$. We want to show I is finitely generated. Pick a sequence $(f_i)_{i=1}^n$ of polynomials in I in the following manner:

- Take f_1 to be a polynomial of minimal degree in I.
- If $I = \langle f_1 \rangle$ we are done; otherwise, take $f_2 \in I \setminus \langle f_1 \rangle$ of minimal degree.
- Continue inductively- assuming $f_1, \ldots, f_n \in I$ are chosen, if $I \neq \langle f_1, \ldots, f_n \rangle$, take $f_{n+1} \in I \setminus \langle f_1, \ldots, f_n \rangle$ of minimal degree in this set.

Proof of HBT

Let I be an ideal of $R[x]$. We want to show I is finitely generated. Pick a sequence $(f_i)_{i=1}^n$ of polynomials in I in the following manner:

- Take f_1 to be a polynomial of minimal degree in I.
- If $I = \langle f_1 \rangle$ we are done; otherwise, take $f_2 \in I \setminus \langle f_1 \rangle$ of minimal degree.
- Continue inductively- assuming $f_1, \ldots, f_n \in I$ are chosen, if $I \neq \langle f_1, \ldots, f_n \rangle$, take $f_{n+1} \in I \setminus \langle f_1, \ldots, f_n \rangle$ of minimal degree in this set.

Note: $\deg(f_1) \leq \cdots \leq \deg(f_n) \leq \cdots$

Proof of HBT - contd

For any $i \in \mathbb{N}$, let $a_i \in R$ be the *leading coefficient* of f_i.

Proof of HBT - contd

For any $i \in \mathbb{N}$, let $a_i \in R$ be the *leading coefficient* of f_i. By 1the previous exercise, there exists n_0 such that the sequence $(a_i)_{i=1}^{\infty}$ is included in $\langle a_1, \ldots, a_{n_0} \rangle$.

Proof of HBT - contd

For any $i \in \mathbb{N}$, let $a_i \in R$ be the *leading coefficient* of f_i. By 1the previous exercise, there exists n_0 such that the sequence $(a_i)_{i=1}^{\infty}$ is included in $\langle a_1, \ldots, a_{n_0} \rangle$.

Claim

I is generated by $f_1, \ldots, f_{n_0}$.

Proof of HBT - contd

For any $i \in \mathbb{N}$, let $a_i \in R$ be the *leading coefficient* of f_i. By 1the previous exercise, there exists n_0 such that the sequence $(a_i)_{i=1}^{\infty}$ is included in $\langle a_1, \ldots, a_{n_0} \rangle$.

Claim

I is generated by $f_1, \ldots, f_{n_0}$.

Proof.

Proof of HBT - contd

For any $i \in \mathbb{N}$, let $a_i \in R$ be the *leading coefficient* of f_i. By 1the previous exercise, there exists n_0 such that the sequence $(a_i)_{i=1}^{\infty}$ is included in $\langle a_1, \ldots, a_{n_0} \rangle$.

Claim

I is generated by $f_1, \ldots, f_{n_0}$.

Proof.

Assume not, and consider f_{n_0+1} with leading coefficient a_{n_0+1}. Write $a_{n_0+1} = \sum_{i=1}^{n_0} r_i a_i$.

Proof of HBT - contd

For any $i \in \mathbb{N}$, let $a_i \in R$ be the *leading coefficient* of f_i. By 1the previous exercise, there exists n_0 such that the sequence $(a_i)_{i=1}^{\infty}$ is included in $\langle a_1, \ldots, a_{n_0} \rangle$.

Claim

I is generated by $f_1, \ldots, f_{n_0}$.

Proof.

Assume not, and consider f_{n_0+1} with leading coefficient a_{n_0+1}. Write $a_{n_0+1} = \sum_{i=1}^{n_0} r_i a_i$. Write $J = \langle f_1, \ldots, f_{n_0} \rangle$ and recall that f_{n_0+1} has minimal degree in $I \setminus J$.

Proof of HBT - contd

For any $i \in \mathbb{N}$, let $a_i \in R$ be the *leading coefficient* of f_i. By 1the previous exercise, there exists n_0 such that the sequence $(a_i)_{i=1}^{\infty}$ is included in $\langle a_1, \ldots, a_{n_0} \rangle$.

Claim

I is generated by $f_1, \ldots, f_{n_0}$.

Proof.

Assume not, and consider f_{n_0+1} with leading coefficient a_{n_0+1}. Write $a_{n_0+1} = \sum_{i=1}^{n_0} r_i a_i$. Write $J = \langle f_1, \ldots, f_{n_0} \rangle$ and recall that f_{n_0+1} has minimal degree in $I \setminus J$.
Define $g(x) = \sum_{i=1}^{n_0} r_i \cdot x^{\deg f_{n_0+1} - \deg f_i} \cdot f_i(x)$. Then $g \in J$, thus $f_{n_0+1} - g \notin J$.

Proof of HBT - contd

For any $i \in \mathbb{N}$, let $a_i \in R$ be the *leading coefficient* of f_i. By 1the previous exercise, there exists n_0 such that the sequence $(a_i)_{i=1}^{\infty}$ is included in $\langle a_1, \ldots, a_{n_0} \rangle$.

Claim

I is generated by $f_1, \ldots, f_{n_0}$.

Proof.

Assume not, and consider f_{n_0+1} with leading coefficient a_{n_0+1}. Write $a_{n_0+1} = \sum_{i=1}^{n_0} r_i a_i$. Write $J = \langle f_1, \ldots, f_{n_0} \rangle$ and recall that f_{n_0+1} has minimal degree in $I \setminus J$.
Define $g(x) = \sum_{i=1}^{n_0} r_i \cdot x^{\deg f_{n_0+1} - \deg f_i} \cdot f_i(x)$. Then $g \in J$, thus $f_{n_0+1} - g \notin J$.
What is the leading coefficient of g?

Proof of HBT - contd

For any $i \in \mathbb{N}$, let $a_i \in R$ be the *leading coefficient* of f_i. By 1the previous exercise, there exists n_0 such that the sequence $(a_i)_{i=1}^{\infty}$ is included in $\langle a_1, \ldots, a_{n_0} \rangle$.

Claim

I is generated by $f_1, \ldots, f_{n_0}$.

Proof.

Assume not, and consider f_{n_0+1} with leading coefficient a_{n_0+1}. Write $a_{n_0+1} = \sum_{i=1}^{n_0} r_i a_i$. Write $J = \langle f_1, \ldots, f_{n_0} \rangle$ and recall that f_{n_0+1} has minimal degree in $I \setminus J$.
Define $g(x) = \sum_{i=1}^{n_0} r_i \cdot x^{\deg f_{n_0+1} - \deg f_i} \cdot f_i(x)$. Then $g \in J$, thus $f_{n_0+1} - g \notin J$.
What is the leading coefficient of g? It is *also* a_{n_0+1}. Therefore, $\deg(f_{n_0+1} - g) < \deg(f_{n_0+1})$. A contradiction. $\square$

Hilbert's Nullstellensatz

Let K be an algebraically closed field.

Theorem (Hilbert's Nullstellensatz)

Hilbert's Nullstellensatz

Let K be an algebraically closed field.

Theorem (Hilbert's Nullstellensatz)

Let $\{p_i\}$ be a collection of polynomials in $K[\underline{x}] = K[x_1, \ldots, x_n]$. Assume $f \in K[\underline{x}]$ is another polynomial such that for any $y \in K^n$, if $p_i(y) = 0$ for all i, then $f(y) = 0$.

Hilbert's Nullstellensatz

Let K be an algebraically closed field.

Theorem (Hilbert's Nullstellensatz)

Let $\{p_i\}$ be a collection of polynomials in $K[\underline{x}] = K[x_1, \ldots, x_n]$. Assume $f \in K[\underline{x}]$ is another polynomial such that for any $y \in K^n$, if $p_i(y) = 0$ for all i, then $f(y) = 0$. Then, there exist $r \in \mathbb{N}$ and $g_i \in K[\underline{x}]$ ($g_i = 0$ for a.e. i) such that $f^r = \sum_i g_i p_i$.

Hilbert's Nullstellensatz

Let K be an algebraically closed field.

Theorem (Hilbert's Nullstellensatz)

Let $\{p_i\}$ be a collection of polynomials in $K[\underline{x}] = K[x_1, \ldots, x_n]$. Assume $f \in K[\underline{x}]$ is another polynomial such that for any $y \in K^n$, if $p_i(y) = 0$ for all i, then $f(y) = 0$. Then, there exist $r \in \mathbb{N}$ and $g_i \in K[\underline{x}]$ ($g_i = 0$ for a.e. i) such that $f^r = \sum_i g_i p_i$.

Writing I for the ideal $\langle p_i \rangle$, we have the following, more compact form:

Hilbert's Nullstellensatz

Let K be an algebraically closed field.

Theorem (Hilbert's Nullstellensatz)

Let $\{p_i\}$ be a collection of polynomials in $K[\underline{x}] = K[x_1, \ldots, x_n]$. Assume $f \in K[\underline{x}]$ is another polynomial such that for any $y \in K^n$, if $p_i(y) = 0$ for all i, then $f(y) = 0$. Then, there exist $r \in \mathbb{N}$ and $g_i \in K[\underline{x}]$ ($g_i = 0$ for a.e. i) such that $f^r = \sum_i g_i p_i$.

Writing I for the ideal $\langle p_i \rangle$, we have the following, more compact form:

Theorem (Nullstellensatz- slogan form)

$I(V(I)) = \sqrt{I}$.

Example

Consider $p_1(x, y) = x + y$, $p_2(x, y) = (x - y)^3$, and take $f(x) = x$. Assuming $\mathrm{Char}(K) \neq 2$, if $p_1(x, y) = p_2(x, y) = 0$ then necessarily $x = 0$. Therefore $x^r \in \langle x + y, (x - y)^3 \rangle$ for some r.

Example

Consider $p_1(x, y) = x + y$, $p_2(x, y) = (x - y)^3$, and take $f(x) = x$. Assuming $\mathrm{Char}(K) \neq 2$, if $p_1(x, y) = p_2(x, y) = 0$ then necessarily $x = 0$. Therefore $x^r \in \langle x + y, (x - y)^3 \rangle$ for some r.

Is this obvious from computation?

Example

Consider $p_1(x,y) = x + y$, $p_2(x,y) = (x-y)^3$, and take $f(x) = x$. Assuming $\mathrm{Char}(K) \neq 2$, if $p_1(x,y) = p_2(x,y) = 0$ then necessarily $x = 0$. Therefore $x^r \in \langle x+y, (x-y)^3 \rangle$ for some r.

Is this obvious from computation?

$$(x+y)\frac{7x^2 - 4xy + y^2}{8} + \frac{1}{8}(x-y)^3 = x^3.$$

Hilbert's Nullstellensatz

Let us prove the specific case where $f = 0$, i.e.:

Theorem (Weak Nullstellensatz)

Let $\{p_i\}$ be a collection of polynomials in $K[\underline{x}] = K[x_1, \ldots, x_n]$. Assume that $I = \langle p_i \rangle \neq K[\underline{x}]$. Then there exists $y \in K^n$ such that $p_i(y) = 0$ for all i.

Remark

The proof we show is based on `http://aizenbud.org/4Publications/NSS.pdf`. The condition of the theorem in this link is formulated slightly differently.

Lemma

Let K be an infinite field, and assume $p \in K[\underline{x}]$ is a non-zero polynomial. Then $\exists y \in K^n : p(y) \neq 0$.

Lemma

Let K be an infinite field, and assume $p \in K[\underline{x}]$ is a non-zero polynomial. Then $\exists y \in K^n : p(y) \neq 0$.

Proof.

By induction on the number of variables. The case $n = 1$ is clear.

Lemma

Let K be an infinite field, and assume $p \in K[\underline{x}]$ is a non-zero polynomial. Then $\exists y \in K^n : p(y) \neq 0$.

Proof.

By induction on the number of variables. The case $n = 1$ is clear. Write

$$p(\underline{x}) = p(x_1, \ldots, x_n) = \sum_{i=0}^{D} a_i(x_1, \ldots, x_{n-1}) x_n^i$$

with $a_D \neq 0$.

Lemma

Let K be an infinite field, and assume $p \in K[\underline{x}]$ is a non-zero polynomial. Then $\exists y \in K^n : p(y) \neq 0$.

Proof.

By induction on the number of variables. The case $n = 1$ is clear. Write

$$p(\underline{x}) = p(x_1, \ldots, x_n) = \sum_{i=0}^{D} a_i(x_1, \ldots, x_{n-1}) x_n^i$$

with $a_D \neq 0$. By induction, $\exists y' \in K^{n-1}$ such that $a_D(y') \neq 0$.

Lemma

Let K be an infinite field, and assume $p \in K[\underline{x}]$ is a non-zero polynomial. Then $\exists y \in K^n : p(y) \neq 0$.

Proof.

By induction on the number of variables. The case $n = 1$ is clear. Write

$$p(\underline{x}) = p(x_1, \ldots, x_n) = \sum_{i=0}^{D} a_i(x_1, \ldots, x_{n-1}) x_n^i$$

with $a_D \neq 0$. By induction, $\exists y' \in K^{n-1}$ such that $a_D(y') \neq 0$. Consider $f(t) = p(y', t) \in K[t]$, a polynomial in one variable.

Lemma

Let K be an infinite field, and assume $p \in K[\underline{x}]$ is a non-zero polynomial. Then $\exists y \in K^n : p(y) \neq 0$.

Proof.

By induction on the number of variables. The case $n = 1$ is clear. Write

$$p(\underline{x}) = p(x_1, \ldots, x_n) = \sum_{i=0}^{D} a_i(x_1, \ldots, x_{n-1}) x_n^i$$

with $a_D \neq 0$. By induction, $\exists y' \in K^{n-1}$ such that $a_D(y') \neq 0$. Consider $f(t) = p(y', t) \in K[t]$, a polynomial in one variable. Then f has a non-zero leading coefficient, hence $\exists y'' \in K$ such that $f(y'') = p(y', y'') \neq 0$. □

Lemma

Let L/K be a finitely generated extension of fields (i.e. L is a quotient of a polynomial ring over K). The L is isomorphic to a finite extension of $K(t_1, \ldots, t_m)$, the field of rational functions in m variables over K.

Lemma

Let L/K be a finitely generated extension of fields (i.e. L is a quotient of a polynomial ring over K). The L is isomorphic to a finite extension of $K(t_1, \ldots, t_m)$, the field of rational functions in m variables over K.

Proof.

Omitted. $\square$

Proof of w-Nullstellensatz

Wlog, assume $I \lhd K[\underline{x}]$ is maximal, and put $L = K[\underline{x}]/I$ and $\alpha = (\alpha_1, \ldots, \alpha_n) \in L^n$ be the image of $\underline{x}$ modulo I^n.

Proof of w-Nullstellensatz

Wlog, assume $I \lhd K[\underline{x}]$ is maximal, and put $L = K[\underline{x}]/I$ and $\alpha = (\alpha_1, \ldots, \alpha_n) \in L^n$ be the image of $\underline{x}$ modulo I^n. Note that α is a common solution to $\{p_i\}$ in L^n.

By the last lemma, L is isomorphic to a finite extension of $K(t_1, \ldots, t_m)$. Let $e_1, \ldots, e_k$ be a vector space basis for L over $K(t_1, \ldots, t_m)$ with $e_1 = 1$.

Proof of w-Nullstellensatz

Wlog, assume $I \triangleleft K[\underline{x}]$ is maximal, and put $L = K[\underline{x}]/I$ and $\alpha = (\alpha_1, \ldots, \alpha_n) \in L^n$ be the image of $\underline{x}$ modulo I^n. Note that α is a common solution to $\{p_i\}$ in L^n.

By the last lemma, L is isomorphic to a finite extension of $K(t_1, \ldots, t_m)$. Let $e_1, \ldots, e_k$ be a vector space basis for L over $K(t_1, \ldots, t_m)$ with $e_1 = 1$. write

$$\alpha_i = \sum_j m_{ij}(t_1, \ldots, t_m) e_j \quad \text{and} \quad e_i e_j = \sum_h b_{ijh}(t_1, \ldots, t_m) e_h$$

with $m_{ij}, b_{ijh} \in K(t_1, \ldots, t_m)$.

Proof of w-Nullstellensatz

Wlog, assume $I \lhd K[\underline{x}]$ is maximal, and put $L = K[\underline{x}]/I$ and $\alpha = (\alpha_1, \ldots, \alpha_n) \in L^n$ be the image of $\underline{x}$ modulo I^n. Note that α is a common solution to $\{p_i\}$ in L^n.

By the last lemma, L is isomorphic to a finite extension of $K(t_1, \ldots, t_m)$. Let $e_1, \ldots, e_k$ be a vector space basis for L over $K(t_1, \ldots, t_m)$ with $e_1 = 1$. write

$$\alpha_i = \sum_j m_{ij}(t_1, \ldots, t_m) e_j \quad \text{and} \quad e_i e_j = \sum_h b_{ijh}(t_1, \ldots, t_m) e_h$$

with $m_{ij}, b_{ijh} \in K(t_1, \ldots, t_m)$. Let d be their common denominator, and use the first lemma to find $y \in K^m$ such that $d(y) \neq 0$.

Proof of w-Nullstellensatz

We use the information we have thus far to construct a new algebra over K where the polynomials $\{p_i\}$ have a common zero.

Proof of w-Nullstellensatz

We use the information we have thus far to construct a new algebra over K where the polynomials $\{p_i\}$ have a common zero. Let

$A = K^k$ with $\{c_1, \dots, c_k\}$ a basis, and define a (commutative and unital) ring structure on K^k by setting $c_i c_j = \sum_h b_{ijh}(y) c_h$ (*Exercise: verify that this is well defined*).

Proof of w-Nullstellensatz

We use the information we have thus far to construct a new algebra over K where the polynomials $\{p_i\}$ have a common zero. Let

$A = K^k$ with $\{c_1, \ldots, c_k\}$ a basis, and define a (commutative and unital) ring structure on K^k by setting $c_i c_j = \sum_h b_{ijh}(y) c_h$ (*Exercise: verify that this is well defined*). Put $s_i = \sum_j m_{ij}(y) c_j$. Then $p_i(s_1, \ldots, s_m) = p_i(\alpha)(y)$ is the evaluation at y of a zero rational function. Thus, $s = (s_1, \ldots, s_m)$ is a common zero of $\{p_i\}$ in A^n.

Proof of w-Nullstellensatz

We use the information we have thus far to construct a new algebra over K where the polynomials $\{p_i\}$ have a common zero. Let

$A = K^k$ with $\{c_1, \ldots, c_k\}$ a basis, and define a (commutative and unital) ring structure on K^k by setting $c_i c_j = \sum_h b_{ijh}(y) c_h$ (*Exercise: verify that this is well defined*). Put $s_i = \sum_j m_{ij}(y) c_j$. Then $p_i(s_1, \ldots, s_m) = p_i(\alpha)(y)$ is the evaluation at y of a zero rational function. Thus, $s = (s_1, \ldots, s_m)$ is a common zero of $\{p_i\}$ in A^n.

Now, let F be the quotient of A by some maximal ideal.

Proof of w-Nullstellensatz

We use the information we have thus far to construct a new algebra over K where the polynomials $\{p_i\}$ have a common zero. Let

$A = K^k$ with $\{c_1, \ldots, c_k\}$ a basis, and define a (commutative and unital) ring structure on K^k by setting $c_i c_j = \sum_h b_{ijh}(y) c_h$ (*Exercise: verify that this is well defined*). Put $s_i = \sum_j m_{ij}(y) c_j$. Then $p_i(s_1, \ldots, s_m) = p_i(\alpha)(y)$ is the evaluation at y of a zero rational function. Thus, $s = (s_1, \ldots, s_m)$ is a common zero of $\{p_i\}$ in A^n.

Now, let F be the quotient of A by some maximal ideal. The image of s in F is again a common zero of $\{p_i\}$. But F is a *finite* field extension of K, and K is algebraically closed. Thus $F \simeq K$ and we are done.

The Strong Nullstellensatz

The Nullstellensatz, as presented earlier, in fact follows from the weak Nullstellensatz. Commonly, this is shown using the following.

Rabinowitsch Trick

The Strong Nullstellensatz

The Nullstellensatz, as presented earlier, in fact follows from the weak Nullstellensatz. Commonly, this is shown using the following.

Rabinowitsch Trick

- **Step 1**: If $p_1, \ldots, p_m \in K[\underline{x}]$ are given and f vanishes whenever the p_i's do, then the polynomials

$$p_1, \ldots, p_m, 1 - x_0 f(\underline{x}) \in K[x_0, x_1, \ldots, x_n]$$

  have no common zeros. By w-NSS, they generate the unit ideal.

The Strong Nullstellensatz

The Nullstellensatz, as presented earlier, in fact follows from the weak Nullstellensatz. Commonly, this is shown using the following.

Rabinowitsch Trick

- **Step 1**: If $p_1, \ldots, p_m \in K[\underline{x}]$ are given and f vanishes whenever the p_i's do, then the polynomials

$$p_1, \ldots, p_m, 1 - x_0 f(\underline{x}) \in K[x_0, x_1, \ldots, x_n]$$

  have no common zeros. By w-NSS, they generate the unit ideal.
- **Step 2**: We get an equality of polynomials:

$$1 = g_0(x_0, \ldots, x_n)(1 - x_0 f(\underline{x})) + \sum_{i=1}^{m} g_i(x_0, \ldots, x_n) p_i(\underline{x}).$$

The Strong Nullstellensatz

The Nullstellensatz, as presented earlier, in fact follows from the weak Nullstellensatz. Commonly, this is shown using the following.

Rabinowitsch Trick

- **Step 1**: If $p_1, \ldots, p_m \in K[\underline{x}]$ are given and f vanishes whenever the p_i's do, then the polynomials

$$p_1, \ldots, p_m, 1 - x_0 f(\underline{x}) \in K[x_0, x_1, \ldots, x_n]$$

  have no common zeros. By w-NSS, they generate the unit ideal.
- **Step 2**: We get an equality of polynomials:

$$1 = g_0(x_0, \ldots, x_n)(1 - x_0 f(\underline{x})) + \sum_{i=1}^{m} g_i(x_0, \ldots, x_n) p_i(\underline{x}).$$

- **Step 3**: Substitute $x_0 = 1/f(\underline{x})$ in $k(\underline{x})$. NSS follows.

Corollary of NSS

Over an algebraically closed field K, we have an *equivalence*:

$$\left\{\begin{matrix}\text{Closed subvarieties of} \\ K^n \text{ for some } n\end{matrix}\right\} \quad \leftrightarrow \quad \left\{\begin{matrix}\text{Finitely generated} \\ \text{reduced } K\text{-algebras}\end{matrix}\right\}$$

given by

$$V \quad \mapsto \quad K[\underline{x}]/I(V)$$

Corollary of NSS

Over an algebraically closed field K, we have an *equivalence*:

$$\left\{\begin{matrix}\text{Closed subvarieties of}\\ K^n \text{ for some } n\end{matrix}\right\} \quad \leftrightarrow \quad \left\{\begin{matrix}\text{Finitely generated}\\ \text{reduced } K\text{-algebras}\end{matrix}\right\}$$

given by

$$V \quad \mapsto \quad K[\underline{x}]/I(V)$$

Question

What happens if we consider K non-a.c? What about arbitrary K-algebras?

The spectrum of a ring

Let R be a commutative unital ring.

Definition

The spectrum of R is the set

$$\mathrm{Spec}(R) = \{\mathfrak{p} \lhd R : \mathfrak{p} \text{ prime}\}.$$

The spectrum of a ring

Let R be a commutative unital ring.

Definition

The spectrum of R is the set

$$\mathrm{Spec}(R) = \{\mathfrak{p} \triangleleft R : \mathfrak{p} \text{ prime}\}.$$

Examples

1. $\mathrm{Spec}(k) = \{*\}$ for any field k.

The spectrum of a ring

Let R be a commutative unital ring.

Definition

The spectrum of R is the set

$$\operatorname{Spec}(R) = \{\mathfrak{p} \lhd R : \mathfrak{p} \text{ prime}\} .$$

Examples

1. $\operatorname{Spec}(k) = \{*\}$ for any field k.
2. $\operatorname{Spec}(k[\underline{x}]) \sim \{\text{irreducibe monic polynomials in } \underline{x}\} \sqcup \{0\}$

The spectrum of a ring

Let R be a commutative unital ring.

Definition

The spectrum of R is the set

$$\mathrm{Spec}(R) = \{\mathfrak{p} \lhd R : \mathfrak{p} \text{ prime}\}.$$

Examples

1. $\mathrm{Spec}(k) = \{*\}$ for any field k.
2. $\mathrm{Spec}(k[\underline{x}]) \sim \{\text{irreducibe monic polynomials in } \underline{x}\} \sqcup \{0\}$
3. $\mathrm{Spec}(\mathbb{Z}) = \{\langle 0\rangle\} \sqcup \{\langle p\rangle : p \text{ prime}\}$.

The spectrum of a ring - topology

Given $I \triangleleft R$, define $V(I) := \{\mathfrak{p} \in \mathrm{Spec}(R) : I \subseteq \mathfrak{p}\}$.

Exercise

The spectrum of a ring - topology

Given $I \lhd R$, define $V(I) := \{\mathfrak{p} \in \mathrm{Spec}(R) : I \subseteq \mathfrak{p}\}$.

Exercise

1. $V((0)) = R$ and $V(R) = \emptyset$.

The spectrum of a ring - topology

Given $I \triangleleft R$, define $V(I) := \{\mathfrak{p} \in \mathrm{Spec}(R) : I \subseteq \mathfrak{p}\}$.

Exercise

1. $V((0)) = R$ and $V(R) = \emptyset$.
2. $V(IJ) = V(I) \cup V(J)$.

The spectrum of a ring - topology

Given $I \triangleleft R$, define $V(I) := \{\mathfrak{p} \in \operatorname{Spec}(R) : I \subseteq \mathfrak{p}\}$.

Exercise

1. $V((0)) = R$ and $V(R) = \emptyset$.
2. $V(IJ) = V(I) \cup V(J)$.
3. Given a collection $\{I_\alpha\}$ of ideals, $V(\sum I_\alpha) = \bigcap V(I_\alpha)$.

The spectrum of a ring - topology

Given $I \triangleleft R$, define $V(I) := \{\mathfrak{p} \in \operatorname{Spec}(R) : I \subseteq \mathfrak{p}\}$.

Exercise

1. $V((0)) = R$ and $V(R) = \emptyset$.
2. $V(IJ) = V(I) \cup V(J)$.
3. Given a collection $\{I_\alpha\}$ of ideals, $V(\sum I_\alpha) = \bigcap V(I_\alpha)$.

Proof.

The spectrum of a ring - topology

Given $I \triangleleft R$, define $V(I) := \{\mathfrak{p} \in \mathrm{Spec}(R) : I \subseteq \mathfrak{p}\}$.

Exercise

1. $V((0)) = R$ and $V(R) = \emptyset$.
2. $V(IJ) = V(I) \cup V(J)$.
3. Given a collection $\{I_\alpha\}$ of ideals, $V(\sum I_\alpha) = \bigcap V(I_\alpha)$.

Proof.

1. Clear;

The spectrum of a ring - topology

Given $I \triangleleft R$, define $V(I) := \{\mathfrak{p} \in \mathrm{Spec}(R) : I \subseteq \mathfrak{p}\}$.

Exercise

1. $V((0)) = R$ and $V(R) = \emptyset$.
2. $V(IJ) = V(I) \cup V(J)$.
3. Given a collection $\{I_\alpha\}$ of ideals, $V(\sum I_\alpha) = \bigcap V(I_\alpha)$.

Proof.

1. Clear;
2. $\supseteq$ is clear, if $\mathfrak{p} \supseteq I$ then $\mathfrak{p} \supseteq IJ$ (similarly if $\mathfrak{p} \supseteq J$).

The spectrum of a ring - topology

Given $I \triangleleft R$, define $V(I) := \{\mathfrak{p} \in \mathrm{Spec}(R) : I \subseteq \mathfrak{p}\}$.

Exercise

1. $V((0)) = R$ and $V(R) = \emptyset$.
2. $V(IJ) = V(I) \cup V(J)$.
3. Given a collection $\{I_\alpha\}$ of ideals, $V(\sum I_\alpha) = \bigcap V(I_\alpha)$.

Proof.

1. Clear;
2. $\supseteq$ is clear, if $\mathfrak{p} \supseteq I$ then $\mathfrak{p} \supseteq IJ$ (similarly if $\mathfrak{p} \supseteq J$). Conversely, assume $IJ \subseteq \mathfrak{p}$ and $I \not\subseteq \mathfrak{p}$. Take $x \in I \setminus \mathfrak{p}$, and $y \in J$. Then $xy \in IJ \subseteq \mathfrak{p}$ implies $y \in \mathfrak{p}$, since $\mathfrak{p}$ is prime.

The spectrum of a ring - topology

Given $I \triangleleft R$, define $V(I) := \{\mathfrak{p} \in \mathrm{Spec}(R) : I \subseteq \mathfrak{p}\}$.

Exercise

1. $V((0)) = R$ and $V(R) = \emptyset$.
2. $V(IJ) = V(I) \cup V(J)$.
3. Given a collection $\{I_\alpha\}$ of ideals, $V(\sum I_\alpha) = \bigcap V(I_\alpha)$.

Proof.

1. Clear;
2. $\supseteq$ is clear, if $\mathfrak{p} \supseteq I$ then $\mathfrak{p} \supseteq IJ$ (similarly if $\mathfrak{p} \supseteq J$). Conversely, assume $IJ \subseteq \mathfrak{p}$ and $I \not\subseteq \mathfrak{p}$. Take $x \in I \setminus \mathfrak{p}$, and $y \in J$. Then $xy \in IJ \subseteq \mathfrak{p}$ implies $y \in \mathfrak{p}$, since $\mathfrak{p}$ is prime.
3. $\supseteq$: $\mathfrak{p} \in \bigcap_\alpha V(I_\alpha)$ implies $\mathfrak{p} \supseteq \bigcup I_\alpha \supseteq \sum I_\alpha$.

The spectrum of a ring - topology

Given $I \triangleleft R$, define $V(I) := \{\mathfrak{p} \in \mathrm{Spec}(R) : I \subseteq \mathfrak{p}\}$.

Exercise

1. $V((0)) = R$ and $V(R) = \emptyset$.
2. $V(IJ) = V(I) \cup V(J)$.
3. Given a collection $\{I_\alpha\}$ of ideals, $V(\sum I_\alpha) = \bigcap V(I_\alpha)$.

Proof.

1. Clear;
2. $\supseteq$ is clear, if $\mathfrak{p} \supseteq I$ then $\mathfrak{p} \supseteq IJ$ (similarly if $\mathfrak{p} \supseteq J$). Conversely, assume $IJ \subseteq \mathfrak{p}$ and $I \not\subseteq \mathfrak{p}$. Take $x \in I \setminus \mathfrak{p}$, and $y \in J$. Then $xy \in IJ \subseteq \mathfrak{p}$ implies $y \in \mathfrak{p}$, since $\mathfrak{p}$ is prime.
3. $\supseteq$: $\mathfrak{p} \in \bigcap_\alpha V(I_\alpha)$ implies $\mathfrak{p} \supseteq \bigcup I_\alpha \supseteq \sum I_\alpha$.
   $\subseteq$: Since $I_{\alpha_0} \subseteq \sum I_\alpha$ for all α_0, $\mathfrak{p} \in V(\sum I_\alpha)$ implies $\mathfrak{p} \in V(I_{\alpha_0})$ for all α_0.

The collection $\{V(I) : I \triangleleft R\}$ is the set of closed sets for a topology on $\mathrm{Spec}(R)$, which is known as the *Zariski Topolgy* of R.

Exercise

Let R be a ring.

1. Show that $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$, for all $\mathfrak{p} \in \mathrm{Spec}(R)$ and, in particular, that $\{\mathfrak{p}\}$ is closed iff $\mathfrak{p}$ is maximal.
2. Show that, if R is a domain, then $\{(0)\}$ is a <u>dense</u> point.

Exercise

Let R be a ring.

1. Show that $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$, for all $\mathfrak{p} \in \mathrm{Spec}(R)$ and, in particular, that $\{\mathfrak{p}\}$ is closed iff $\mathfrak{p}$ is maximal.
2. Show that, if R is a domain, then $\{(0)\}$ is a <u>dense</u> point.

Solution.

$\square$

Exercise

Let R be a ring.

1. Show that $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$, for all $\mathfrak{p} \in \operatorname{Spec}(R)$ and, in particular, that $\{\mathfrak{p}\}$ is closed iff $\mathfrak{p}$ is maximal.
2. Show that, if R is a domain, then $\{(0)\}$ is a dense point.

Solution.

1. By definition, and by the previous exercise:

$$\overline{\mathfrak{p}} = \bigcap_{\mathfrak{p} \in F \text{ closed}} F = \bigcap_{\substack{I \lhd R \\ I \subseteq \mathfrak{p}}} V(I) = V(\sum_{I \subseteq \mathfrak{p}} I) = V(\mathfrak{p}).$$

In particular, $\{\mathfrak{p}\}$ is closed iff $\{\mathfrak{p}\} = V(\mathfrak{p})$ which occurs iff $\mathfrak{p}$ is maximal (o/w, take $\mathfrak{m} \supsetneq \mathfrak{p}$ maximal).

□

Exercise

Let R be a ring.

1. Show that $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$, for all $\mathfrak{p} \in \operatorname{Spec}(R)$ and, in particular, that $\{\mathfrak{p}\}$ is closed iff $\mathfrak{p}$ is maximal.
2. Show that, if R is a domain, then $\{(0)\}$ is a dense point.

Solution.

1. By definition, and by the previous exercise:

$$\overline{\mathfrak{p}} = \bigcap_{\mathfrak{p} \in F \text{ closed}} F = \bigcap_{\substack{I \lhd R \\ I \subseteq \mathfrak{p}}} V(I) = V\Big(\sum_{I \subseteq \mathfrak{p}} I\Big) = V(\mathfrak{p}).$$

   In particular, $\{\mathfrak{p}\}$ is closed iff $\{\mathfrak{p}\} = V(\mathfrak{p})$ which occurs iff $\mathfrak{p}$ is maximal (o/w, take $\mathfrak{m} \supsetneq \mathfrak{p}$ maximal).
2. Note: $(0) \in \operatorname{Spec}(R)$ iff R is a domain, in which case $V(0) = R$.

$\square$

Questions?