Lecture 6: Introduction to Commutative Algebra and Algebraic Geometry

Rafael Oliveira

University of Waterloo
Cheriton School of Computer Science

rafael.oliveira.teaching@gmail.com

January 27, 2021

Overview

- Elementary Commutative Algebra
- Algebraic Sets
- Structural & Computational Questions
- Conclusion
- Acknowledgements

Ring Basics

- Given a ring R, an *ideal* $I \subset R$ is a subset of the ring R such that:
  1. I is closed under addition

$$a, b \in I \Rightarrow a + b \in I$$

  2. I is closed under multiplication by elements of R

$$\underline{a \in I}, \underline{s \in R} \Rightarrow \underline{s \cdot a \in I}$$

Ring Basics

- Given a ring R, an *ideal* $I \subset R$ is a subset of the ring R such that:
  1. I is closed under addition
     $$a, b \in I \Rightarrow a + b \in I$$
  2. I is closed under multiplication by elements of R
     $$a \in I, s \in R \Rightarrow s \cdot a \in I$$
- Examples:
  1. (0) is ideal generated by the 0 element of the ring

Ring Basics

- Given a ring R, an *ideal* $I \subset R$ is a subset of the ring R such that:
  1. I is closed under addition
  $$a, b \in I \Rightarrow a + b \in I$$
  2. I is closed under multiplication by elements of R
  $$a \in I, s \in R \Rightarrow s \cdot a \in I$$
- Examples:
  1. (0) is ideal generated by the 0 element of the ring
  2. R is an ideal

Ring Basics

- Given a ring R, an *ideal* $I \subset R$ is a subset of the ring R such that:
  1. I is closed under addition
  $$a, b \in I \Rightarrow a + b \in I$$
  2. I is closed under multiplication by elements of R
  $$a \in I, s \in R \Rightarrow s \cdot a \in I$$
- Examples:
  1. (0) is ideal generated by the 0 element of the ring
  2. R is an ideal
  3. ring of integers $\mathbb{Z}$ then the set of all even numbers is the ideal generated by 2, denoted (2)

$$2k = 2 \cdot k \in (2)$$

Ring Basics

- Given a ring R, an *ideal* $I \subset R$ is a subset of the ring R such that:
  1. I is closed under addition
  $$a, b \in I \Rightarrow a + b \in I$$
  2. I is closed under multiplication by elements of R
  $$a \in I, s \in R \Rightarrow s \cdot a \in I$$
- Examples:
  1. (0) is ideal generated by the 0 element of the ring
  2. R is an ideal
  3. ring of integers $\mathbb{Z}$ then the set of all even numbers is the ideal generated by 2, denoted (2)
  4. In $\mathbb{Q}[x]$ the set of all polynomials whose constant coefficient is zero is the ideal (x) generated by x

$$\underbrace{\{p(x) \in \mathbb{Q}[x]}_{\text{other description}} \mid p(0) = 0\} = \underbrace{(x)}_{\text{generators}}$$

Ring Basics

- Given a ring R, an *ideal* $I \subset R$ is a subset of the ring R such that:
  1. I is closed under addition
  $$a, b \in I \Rightarrow a + b \in I$$
  2. I is closed under multiplication by elements of R
  $$a \in I, s \in R \Rightarrow s \cdot a \in I$$
- Examples:
  1. (0) is ideal generated by the 0 element of the ring
  2. R is an ideal
  3. ring of integers $\mathbb{Z}$ then the set of all even numbers is the ideal generated by 2, denoted (2)
  4. In $\mathbb{Q}[x]$ the set of all polynomials whose constant coefficient is zero is the ideal (x) generated by x
  5. In $\mathbb{Q}[x, y]$ the set of all polynomials whose constant coefficient is zero is the ideal (x, y) generated by x and y

$\{ p(x,y) \in \mathbb{Q}[x,y] \mid p(0,0) = 0 \}$

Operations with Ideals

- $I, J \subset R$ ideals, then:
  1. $I + J$ is an ideal

$$I + J := \{ a + b \mid a \in I,\ b \in J \}$$

$$(a_1 + b_1) + (a_2 + b_2) = (a_1 + a_2) + (b_1 + b_2)$$

$$r(a + b) = r \cdot a + r \cdot b$$

Operations with Ideals

- $I, J \subset R$ ideals, then:
  1. $I + J$ is an ideal
  2. $I \cap J$ is an ideal

Operations with Ideals

- $I, J \subset R$ ideals, then:
  1. $I + J$ is an ideal
  2. $I \cap J$ is an ideal
  3. $IJ :=$ ideal generated by $\{ab \mid a \in I,\ b \in J\}$

$IJ \neq I \cap J$

$\subset$

Operations with Ideals

$$x^2 \in I$$

$$(n=2)$$

- $I, J \subset R$ ideals, then:
  1. $I + J$ is an ideal
  2. $I \cap J$ is an ideal
  3. $IJ :=$ ideal generated by $\{ab \mid a \in I,\ b \in J\}$
  4. $rad(I) := \{a \in R \mid \exists n \in \mathbb{N} \text{ s.t. } a^n \in I\}$ is an ideal

$$I = (x^2) \subset \mathbb{Q}[x]$$

$$rad(I) = (x)$$

$$a^n = x^2 \cdot q(x) \implies a(0) = 0 \implies a \in (x)$$

Quotient Rings

- Given a ring R, and an ideal $I \subset R$, we can form equivalence classes of elements of R modulo I

$$a \sim b \Leftrightarrow a - b \in I$$

cosets : $a + I$

Quotient Rings

- Given a ring R, and an ideal $I \subset R$, we can form equivalence classes of elements of R modulo I

$$a \sim b \Leftrightarrow a - b \in I$$

- If we only consider these equivalence classes, we have the *quotient ring* R/I

$$R/I = \{ \underbrace{a + I}_{\bar{a}} \mid a \in R \}$$

Quotient Rings

- Given a ring R, and an ideal $I \subset R$, we can form equivalence classes of elements of R modulo I

$$a \sim b \Leftrightarrow a - b \in I$$

- If we only consider these equivalence classes, we have the *quotient ring* R/I
- Examples:
  1. $R = \mathbb{Z}$ and $I = (2)$ gives the field $\mathbb{Z}_2$ $\{0, 1\}$

Quotient Rings

- Given a ring R, and an ideal $I \subset R$, we can form equivalence classes of elements of R modulo I

$$a \sim b \Leftrightarrow a - b \in I$$

- If we only consider these equivalence classes, we have the *quotient ring* R/I
- Examples:
  1. $R = \mathbb{Z}$ and $I = (2)$ gives the field $\mathbb{Z}_2$
  2. $R = \mathbb{Z}$ and $I = (6)$ gives the ring of integers modulo 6, $\mathbb{Z}_6$

2, 3 don't have inverses over $\mathbb{Z}_6$

Quotient Rings

- Given a ring R, and an ideal $I \subset R$, we can form equivalence classes of elements of R modulo I

$$a \sim b \Leftrightarrow a - b \in I$$

- If we only consider these equivalence classes, we have the *quotient ring* R/I
- Examples:
  1. $R = \mathbb{Z}$ and $I = (2)$ gives the field $\mathbb{Z}_2$
  2. $R = \mathbb{Z}$ and $I = (6)$ gives the ring of integers modulo 6, $\mathbb{Z}_6$
- An element $q \in R$ is *irreducible* if q is not a unit and $q = a \cdot b \Rightarrow$ either a or b are a unit.

divisor of 1

$\cancel{q \cdot u = 1}$

Quotient Rings

- Given a ring R, and an ideal $I \subset R$, we can form equivalence classes of elements of R modulo I

$$a \sim b \Leftrightarrow a - b \in I$$

- If we only consider these equivalence classes, we have the *quotient ring* R/I
- Examples:
  1. $R = \mathbb{Z}$ and $I = (2)$ gives the field $\mathbb{Z}_2$
  2. $R = \mathbb{Z}$ and $I = (6)$ gives the ring of integers modulo 6, $\mathbb{Z}_6$
- An element $q \in R$ is *irreducible* if q is not a unit and $q = a \cdot b \Rightarrow$ either a or b are a unit.
- An ideal $I \subset R$ is *prime* if for any $a, b \in R$, if $ab \in I$ then $a \in I$ or $b \in I$

$\mathbb{Z}$ $\quad p \to$ divisors are $\pm 1, \pm p$

$p \to a, b \in \mathbb{Z}$ $\quad p \mid ab \Rightarrow p \mid a$ or $p \mid b$

Quotient Rings

- Given a ring R, and an ideal $I \subset R$, we can form equivalence classes of elements of R modulo I

$$a \sim b \Leftrightarrow a - b \in I$$

- If we only consider these equivalence classes, we have the *quotient ring* R/I
- Examples:
  1. $R = \mathbb{Z}$ and $I = (2)$ gives the field $\mathbb{Z}_2$
  2. $R = \mathbb{Z}$ and $I = (6)$ gives the ring of integers modulo 6, $\mathbb{Z}_6$
- An element $q \in R$ is *irreducible* if q is not a unit and $q = a \cdot b \Rightarrow$ either a or b are a unit.
- An ideal $I \subset R$ is *prime* if for any $a, b \in R$, if $ab \in I$ then $a \in I$ or $b \in I$
- Two ideals $I, J \subset R$ are *coprime* if $I + J = R$

over $\mathbb{Z}$ $\gcd(a,b) \in (a)+(b)$ (Euclidean algorithm)

“Complexities” in Rings

- *zero divisors*: an element $a \in R$ is a zero divisor if $\underbrace{a \neq 0}_{\text{nonzero}}$ and there exists $\underbrace{b \in R \setminus \{0\}}_{\text{nonzero}}$ such that $\underline{ab = 0}$

$\mathbb{Z}_6$ 2 and 3 are zero divisors

$2 \cdot 3 = 0 \mod 6$

$\mathbb{Q}[x]/(x^2)$ x is zero divisor

$\overline{x^2} = \overline{0}$

“Complexities” in Rings

- *zero divisors*: an element $a \in R$ is a zero divisor if $a \neq 0$ and there exists $b \in R \setminus \{0\}$ such that $ab = 0$
  - $\mathbb{Z}_6$ has 2 as zero divisor

"Complexities" in Rings

zero divisors related to not being prime

- *zero divisors*: an element $a \in R$ is a zero divisor if $a \neq 0$ and there exists $b \in R \setminus \{0\}$ such that $ab = 0$
  - $\mathbb{Z}_6$ has 2 as zero divisor
- a special type of zero divisors are *nilpotent* elements. These are elements $a \in R$ such that there exists $n \in \mathbb{N}$ for which $a^n = 0$

$a \neq 0$

  - $\mathbb{Q}[x]/(x^2)$ has x as nilpotent element

nilpotent related to not being radical

“Complexities” in Rings

- *zero divisors*: an element $a \in R$ is a zero divisor if $a \neq 0$ and there exists $b \in R \setminus \{0\}$ such that $ab = 0$
  - $\mathbb{Z}_6$ has 2 as zero divisor
- a special type of zero divisors are *nilpotent* elements. These are elements $a \in R$ such that there exists $n \in \mathbb{N}$ for which $a^n = 0$
  - $\mathbb{Q}[x]/(x^2)$ has x as nilpotent element
- Rings with no zero divisors are called *integral domains*
  - R/I is a domain whenever I is prime

no nilpotents

$R/\mathrm{rad}(I)$ for I ideal

Unique Factorization Domains

- An integral domain R is a *unique factorization domain* (UFD) if
  1. every element in R is expressed as a product of finitely many irreducible elements
  2. Every irreducible element $p \in R$ yields a prime ideal (p)

$$m = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$$

Unique Factorization Domains

- An integral domain R is a *unique factorization domain* (UFD) if
  1. every element in R is expressed as a product of finitely many irreducible elements
  2. Every irreducible element $p \in R$ yields a prime ideal (p)
- A very special kind of UFD, which we have seen a lot, is a *principal ideal domain* (PID): R is a PID if every ideal of R is principal (generated by *one element*)

Unique Factorization Domains

- An integral domain R is a *unique factorization domain* (UFD) if
  1. every element in R is expressed as a product of finitely many irreducible elements
  2. Every irreducible element $p \in R$ yields a prime ideal (p)
- A very special kind of UFD, which we have seen a lot, is a *principal ideal domain* (PID): R is a PID if every ideal of R is principal (generated by *one element*)
- Examples of PIDs and UFDs
  1. $\mathbb{Z}$ is a PID (and hence UFD)

Unique Factorization Domains

- An integral domain R is a *unique factorization domain* (UFD) if
  1. every element in R is expressed as a product of finitely many irreducible elements
  2. Every irreducible element $p \in R$ yields a prime ideal (p)
- A very special kind of UFD, which we have seen a lot, is a *principal ideal domain* (PID): R is a PID if every ideal of R is principal (generated by *one element*)
- Examples of PIDs and UFDs
  1. $\mathbb{Z}$ is a PID (and hence UFD)
  2. $\mathbb{Q}[x]$ is a PID (and hence UFD)

Unique Factorization Domains

- An integral domain R is a *unique factorization domain* (UFD) if
  1. every element in R is expressed as a product of finitely many irreducible elements
  2. Every irreducible element $p \in R$ yields a prime ideal (p)
- A very special kind of UFD, which we have seen a lot, is a *principal ideal domain* (PID): R is a PID if every ideal of R is principal (generated by *one element*)
- Examples of PIDs and UFDs
  1. $\mathbb{Z}$ is a PID (and hence UFD)
  2. $\mathbb{Q}[x]$ is a PID (and hence UFD)
  3. any Euclidean domain is a PID (and hence UFD)

Unique Factorization Domains

- An integral domain R is a *unique factorization domain* (UFD) if
  1. every element in R is expressed as a product of finitely many irreducible elements
  2. Every irreducible element $p \in R$ yields a prime ideal (p)
- A very special kind of UFD, which we have seen a lot, is a *principal ideal domain* (PID): R is a PID if every ideal of R is principal (generated by *one element*)
- Examples of PIDs and UFDs
  1. $\mathbb{Z}$ is a PID (and hence UFD)
  2. $\mathbb{Q}[x]$ is a PID (and hence UFD)
  3. any Euclidean domain is a PID (and hence UFD)
  4. $\mathbb{Q}[x, y]$ is a UFD but *not* a PID

(x, y)

Gauss' lemma: R is UFD $\iff$ $R[x]$ is UFD.

Ring Homomorphisms

- A *homomorphism* between rings R, S is a map $\phi : R \to S$ *preserving the ring structure*
  1. $\phi(1) = 1$
  2. $\phi(a + b) = \phi(a) + \phi(b)$
  3. $\phi(ab) = \phi(a) \cdot \phi(b)$

Ring Homomorphisms

- A *homomorphism* between rings R, S is a map $\phi : R \to S$ *preserving the ring structure*
  1. $\phi(1) = 1$
  2. $\phi(a+b) = \phi(a) + \phi(b)$
  3. $\phi(ab) = \phi(a) \cdot \phi(b)$
- Natural homomorphism between a ring R and its quotient R/I

$$\phi : R \longrightarrow R/I$$

$$a \longmapsto a + I \quad (\bar{a})$$

Ring Homomorphisms

- A *homomorphism* between rings R, S is a map $\phi : R \to S$ *preserving the ring structure*
  1. $\phi(1) = 1$
  2. $\phi(a + b) = \phi(a) + \phi(b)$
  3. $\phi(ab) = \phi(a) \cdot \phi(b)$
- Natural homomorphism between a ring R and its quotient R/I
- Two rings R, S are *isomorphic*, denoted $R \simeq S$ if there are two homomorphisms $\phi : R \to S$ and $\psi : S \to R$ such that

$$\underbrace{\phi \circ \psi}_{id_S} : S \to S \quad \text{and} \quad \underbrace{\psi \circ \phi}_{id_R} : R \to R$$

are the *identity* homomorphisms.

$\phi \circ \psi (s) = s$ $\qquad$ $\psi \circ \phi (x) = x$

Ring Homomorphisms

- A *homomorphism* between rings R, S is a map $\phi : R \to S$ *preserving the ring structure*
  1. $\phi(1) = 1$
  2. $\phi(a + b) = \phi(a) + \phi(b)$
  3. $\phi(ab) = \phi(a) \cdot \phi(b)$
- Natural homomorphism between a ring R and its quotient R/I
- Two rings R, S are *isomorphic*, denoted $R \simeq S$ if there are two homomorphisms $\phi : R \to S$ and $\psi : S \to R$ such that

$$\phi \circ \psi : S \to S \quad \text{and} \quad \psi \circ \phi : R \to R$$

  are the *identity* homomorphisms.
- Example:

$$\mathbb{Z}_6 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$$

(special case of Chinese Remainder Theorem)

Algebraic Sets

- Given a collection of polynomials $\mathcal{F} \subset \mathbb{F}[x_1, \ldots, x_n]$ the set

$$V(\mathcal{F}) := \{(a_1, \ldots, a_n) \in \mathbb{F}^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in \mathcal{F}\}$$

is called an *algebraic set*.

Zero set of collection of
polynomials

Algebraic Sets

- Given a collection of polynomials $\mathcal{F} \subset \mathbb{F}[x_1, \ldots, x_n]$ the set

$$V(\mathcal{F}) := \{(a_1, \ldots, a_n) \in \mathbb{F}^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in \mathcal{F}\}$$

  is called an *algebraic set*.
- Set of all solutions to the system of equations defined by $f(x_1, \ldots, x_n) = 0$ for all $f \in \mathcal{F}$

Algebraic Sets

- Given a collection of polynomials $\mathcal{F} \subset \mathbb{F}[x_1, \ldots, x_n]$ the set

$$V(\mathcal{F}) := \{(a_1, \ldots, a_n) \in \mathbb{F}^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in \mathcal{F}\}$$

  is called an *algebraic set*.
- Set of all solutions to the system of equations defined by $f(x_1, \ldots, x_n) = 0$ for all $f \in \mathcal{F}$
- For this part of the course, we assume that $\mathbb{F}$ is algebraically closed, as we don't want certain oddities to come up.

Algebraic Sets

- Given a collection of polynomials $\mathcal{F} \subset \mathbb{F}[x_1, \ldots, x_n]$ the set

$$V(\mathcal{F}) := \{(a_1, \ldots, a_n) \in \mathbb{F}^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in \mathcal{F}\}$$

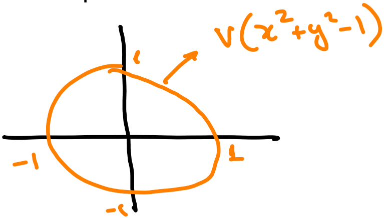
  is called an *algebraic set*.
- Set of all solutions to the system of equations defined by $f(x_1, \ldots, x_n) = 0$ for all $f \in \mathcal{F}$
- For this part of the course, we assume that $\mathbb{F}$ is algebraically closed, as we don't want certain oddities to come up.
- Examples:

Algebraic Sets

- Given a collection of polynomials $\mathcal{F} \subset \mathbb{F}[x_1, \ldots, x_n]$ the set

$$V(\mathcal{F}) := \{(a_1, \ldots, a_n) \in \mathbb{F}^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in \mathcal{F}\}$$

  is called an *algebraic set*.
- Set of all solutions to the system of equations defined by $f(x_1, \ldots, x_n) = 0$ for all $f \in \mathcal{F}$
- For this part of the course, we assume that $\mathbb{F}$ is algebraically closed, as we don't want certain oddities to come up.
- Examples:
  1. Circle: $V(x^2 + y^2 - 1)$

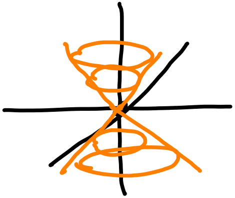


Algebraic Sets

- Given a collection of polynomials $\mathcal{F} \subset \mathbb{F}[x_1, \ldots, x_n]$ the set

$$V(\mathcal{F}) := \{(a_1, \ldots, a_n) \in \mathbb{F}^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in \mathcal{F}\}$$

  is called an *algebraic set*.
- Set of all solutions to the system of equations defined by $f(x_1, \ldots, x_n) = 0$ for all $f \in \mathcal{F}$
- For this part of the course, we assume that $\mathbb{F}$ is algebraically closed, as we don't want certain oddities to come up.
- Examples:
  1. Circle: $V(x^2 + y^2 - 1)$
  2. Lorenz cone: $V(z^2 - x^2 - y^2)$



Algebraic Sets

- Given a collection of polynomials $\mathcal{F} \subset \mathbb{F}[x_1, \ldots, x_n]$ the set

$$V(\mathcal{F}) := \{(a_1, \ldots, a_n) \in \mathbb{F}^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in \mathcal{F}\}$$

  is called an *algebraic set*.
- Set of all solutions to the system of equations defined by $f(x_1, \ldots, x_n) = 0$ for all $f \in \mathcal{F}$
- For this part of the course, we assume that $\mathbb{F}$ is algebraically closed, as we don't want certain oddities to come up.
- Examples:
  1. Circle: $V(x^2 + y^2 - 1)$
  2. Lorenz cone: $V(z^2 - x^2 - y^2)$
  3. Twisted Cubic: $V(y - x^2, z - x^3)$

$$V(y-x^2, z-x^3) = \{(t, t^2, t^3) \mid t \in \mathbb{F}\}$$

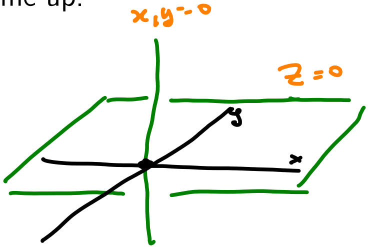
simplest example of a lot of complications/nuances

Algebraic Sets

- Given a collection of polynomials $\mathcal{F} \subset \mathbb{F}[x_1, \dots, x_n]$ the set

$$V(\mathcal{F}) := \{(a_1, \dots, a_n) \in \mathbb{F}^n \mid f(a_1, \dots, a_n) = 0 \text{ for all } f \in \mathcal{F}\}$$

  is called an *algebraic set*.
- Set of all solutions to the system of equations defined by $f(x_1, \dots, x_n) = 0$ for all $f \in \mathcal{F}$
- For this part of the course, we assume that $\mathbb{F}$ is algebraically closed, as we don't want certain oddities to come up.
- Examples:
  1. Circle: $V(x^2 + y^2 - 1)$
  2. Lorenz cone: $V(z^2 - x^2 - y^2)$
  3. Twisted Cubic: $V(y - x^2, z - x^3)$
  4. Line and Hyperplane: $V(xz, yz)$



Algebraic Sets

- Given a collection of polynomials $\mathcal{F} \subset \mathbb{F}[x_1, \ldots, x_n]$ the set

$$V(\mathcal{F}) := \{(a_1, \ldots, a_n) \in \mathbb{F}^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in \mathcal{F}\}$$

  is called an *algebraic set*.
- Set of all solutions to the system of equations defined by $f(x_1, \ldots, x_n) = 0$ for all $f \in \mathcal{F}$
- For this part of the course, we assume that $\mathbb{F}$ is algebraically closed, as we don't want certain oddities to come up.
- Examples:
  1. Circle: $V(x^2 + y^2 - 1)$
  2. Lorenz cone: $V(z^2 - x^2 - y^2)$
  3. Twisted Cubic: $V(y - x^2, z - x^3)$
  4. Line and Hyperplane: $V(xz, yz)$
  5. Solutions of linear system of equations $V(A\mathbf{x} - \mathbf{b})$

$A\bar{x} = \bar{b}$

Properties of algebraic sets

- U, V are algebraic sets, so are $U \cup V$ and $U \cap V$

$$U = V(f_1, \dots, f_s)$$

$$V = V(g_1, \dots, g_t)$$

$$U \cup V = V(f_i g_j)$$

$$V(xz, yz) = V(z) \cup V(x, y)$$

$$U \cap V = V(f_1, \dots, f_s, g_1, \dots, g_t)$$

Properties of algebraic sets

- U, V are algebraic sets, so are $U \cup V$ and $U \cap V$
- the set $\mathcal{F}$ and the ideal $I_{\mathcal{F}}$ generated by the elements of $\mathcal{F}$ define the same algebraic set

$$V(\mathcal{F}) = V(I_{\mathcal{F}})$$

$f, g \in \mathcal{F}$

$\bar{a}$ $\quad f(\bar{a}) = g(\bar{a}) = 0 \Rightarrow (f+g)(\bar{a}) = 0$

$$\sum_{i=1}^{s} \underset{\mathcal{F}}{\underset{\cap}{f_i}} \cdot \underset{R}{\underset{\cap}{r_i}} \, (\bar{a}) = \sum \cancel{f_i(\bar{a})}_{0} \cdot \underline{r_i(\bar{a})}$$

$$= 0$$

Properties of algebraic sets

- U, V are algebraic sets, so are $U \cup V$ and $U \cap V$
- the set $\mathcal{F}$ and the ideal $I_{\mathcal{F}}$ generated by the elements of $\mathcal{F}$ define the same algebraic set
$$V(\mathcal{F}) = V(I_{\mathcal{F}})$$
- For any ideal $I \subset \mathbb{F}[x_1, \ldots, x_n]$
$$V(I) \underset{\subset}{\overset{\supset}{=}} V(rad(I))$$

$$a \in rad(I) \Rightarrow a^n \in I$$

$$P \in V(I) \Rightarrow a^n(P) = 0 \Rightarrow a(P) = 0$$

Properties of algebraic sets

- U, V are algebraic sets, so are $U \cup V$ and $U \cap V$
- the set $\mathcal{F}$ and the ideal $I_{\mathcal{F}}$ generated by the elements of $\mathcal{F}$ define the same algebraic set
$$V(\mathcal{F}) = V(I_{\mathcal{F}})$$
- For any ideal $I \subset \mathbb{F}[x_1, \ldots, x_n]$
$$V(I) = V(rad(I))$$
- If I, J ideals
$$I \subset J \Rightarrow V(J) \subset V(I)$$

Properties of algebraic sets

- U, V are algebraic sets, so are $U \cup V$ and $U \cap V$
- the set $\mathcal{F}$ and the ideal $I_{\mathcal{F}}$ generated by the elements of $\mathcal{F}$ define the same algebraic set
$$V(\mathcal{F}) = V(I_{\mathcal{F}})$$
- For any ideal $I \subset \mathbb{F}[x_1, \ldots, x_n]$
$$V(I) = V(rad(I))$$
- If I, J ideals
$$I \subset J \Rightarrow V(J) \subset V(I)$$

$I(V(I)) \supset rad(I)$

- Relationship between I and $I(V(I))$

Theorem (Hilbert's Nullstellensatz)

For every ideal $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$, where $\mathbb{F}$ is algebraically closed, we have:
$$rad(I) = I(V(I))$$

Algebraic functions over algebraic sets

- It will be very important for us to study algebraic functions over algebraic sets
- Understanding these functions will help us understand the algebraic sets themselves! (and potentially more!)

Algebraic functions over algebraic sets

- It will be very important for us to study algebraic functions over algebraic sets
- Understanding these functions will help us understand the algebraic sets themselves! (and potentially more!)
- Given ideal I and algebraic set $V(I) \subset \mathbb{F}^n$, note that two polynomials $f, g \in \mathbb{F}[x_1, \ldots, x_n]$ yield same function iff

$\forall \bar{a} \in V(I)$

$$f - g \in I.$$

$$f(\bar{a}) = g(\bar{a}) \iff (f-g)(\bar{a}) = 0$$

$$\Uparrow$$

$$f - g \in I$$

Algebraic functions over algebraic sets

- It will be very important for us to study algebraic functions over algebraic sets
- Understanding these functions will help us understand the algebraic sets themselves! (and potentially more!)
- Given ideal I and algebraic set $V(I) \subset \mathbb{F}^n$, note that two polynomials $f, g \in \mathbb{F}[x_1, \ldots, x_n]$ yield same function iff

$$f - g \in I.$$

- Naturally each algebraic set $V(I)$ has its coordinate ring

$$\mathbb{F}[V] := \underbrace{\mathbb{F}[x_1, \ldots, x_n]/I}_{\text{different polynomial functions over } I.}$$

Algebraic functions over algebraic sets

- It will be very important for us to study algebraic functions over algebraic sets
- Understanding these functions will help us understand the algebraic sets themselves! (and potentially more!)
- Given ideal I and algebraic set $V(I) \subset \mathbb{F}^n$, note that two polynomials $f, g \in \mathbb{F}[x_1, \ldots, x_n]$ yield same function iff

$$f - g \in I.$$

- Naturally each algebraic set $V(I)$ has its coordinate ring

$$\mathbb{F}[V] := \mathbb{F}[x_1, \ldots, x_n]/I$$

- These rings could help us understand extra properties of the set $V(I)$, which may not be captured by $V(I)$ (for instance, multiplicities)

$I = (x^2)$ $\quad$ $V(I) = V(J)$ $\quad$ $\boxed{\mathbb{F}[x]/(x^2)}$ nilpotent x

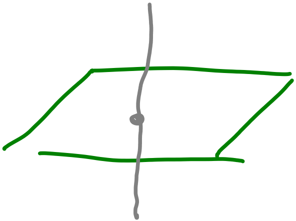
$J = (x)$ $\quad$ $\mathbb{F}[x]/(x)$

Algebraic Varieties

V reducible if $\exists$ W, U alg. sets s.t. $V = U \cup W$ and $U, W \subset V$ proper

- An algebraic set V is said to be *irreducible* if for any decomposition

$$V = U \cup W \Rightarrow U = V \text{ or } W = V$$



Algebraic Varieties

- An algebraic set V is said to be *irreducible* if for any decomposition

$$V = U \cup W \Rightarrow U = V \text{ or } W = W$$

- When the algebraic set $V(I)$ is irreducible, we call it an *algebraic variety*.

Algebraic Varieties

- An algebraic set V is said to be *irreducible* if for any decomposition

$$V = U \cup W \Rightarrow U = V \text{ or } W = W$$

- When the algebraic set $V(I)$ is irreducible, we call it an *algebraic variety*.
- **Practice problem:** prove that I prime then $V(I)$ is irreducible.

- Elementary Commutative Algebra
- Algebraic Sets
- Structural & Computational Questions
- Conclusion
- Acknowledgements

Description of Ideals

- In the definition of algebraic sets, we used any family of polynomials $\mathcal{F}$ to define an algebraic set (or the ideal $I_{\mathcal{F}}$).

Question

Does every ideal of $\mathbb{F}[x_1, \ldots, x_n]$ have a finite description?

[1] We will even get to see his motivation to prove it!

Description of Ideals

- In the definition of algebraic sets, we used any family of polynomials $\mathcal{F}$ to define an algebraic set (or the ideal $I_{\mathcal{F}}$).

Question

Does every ideal of $\mathbb{F}[x_1, \ldots, x_n]$ have a finite description?

- In coming lectures we will show that to be the case - a result known as Hilbert's basis theorem[1]

[1] We will even get to see his motivation to prove it!

Description of Ideals

- In the definition of algebraic sets, we used any family of polynomials $\mathcal{F}$ to define an algebraic set (or the ideal $I_{\mathcal{F}}$).

Question

Does every ideal of $\mathbb{F}[x_1, \ldots, x_n]$ have a finite description?

- In coming lectures we will show that to be the case - a result known as Hilbert's basis theorem[1]
- As it turns out, his proof (actually Gordan's simplification of Hilbert's proof) can be modified to construct Gröbner bases of an ideal, which are extremely important!
- The proof of Hilbert's basis theorem yields a *multivariate polynomial division* algorithm, generalizing
  - Gaussian Elimination
  - Euclidean Division

[1] We will even get to see his motivation to prove it!

Ideal Membership Problem

- Once we know that every ideal in $\mathbb{F}[x_1, \ldots, x_n]$ is finitely generated, our first algorithmic question is:

Ideal Membership Problem

- Once we know that every ideal in $\mathbb{F}[x_1, \ldots, x_n]$ is finitely generated, our first algorithmic question is:
  - **Input:** polynomials $g, f_1, \ldots, f_s \in \mathbb{F}[x_1, \ldots, x_n]$
  - **Output:** is $g \in (f_1, \ldots, f_s)$?
- Problem above is *ideal membership problem*

Ideal Membership Problem

- Once we know that every ideal in $\mathbb{F}[x_1, \ldots, x_n]$ is finitely generated, our first algorithmic question is:
    - **Input:** polynomials $g, f_1, \ldots, f_s \in \mathbb{F}[x_1, \ldots, x_n]$
    - **Output:** is $g \in (f_1, \ldots, f_s)$?
- Problem above is *ideal membership problem*
- Fundamental computational problem
- Decidable

Ideal Membership Problem

- Once we know that every ideal in $\mathbb{F}[x_1, \ldots, x_n]$ is finitely generated, our first algorithmic question is:
  - **Input:** polynomials $g, f_1, \ldots, f_s \in \mathbb{F}[x_1, \ldots, x_n]$
  - **Output:** is $g \in (f_1, \ldots, f_s)$?
- Problem above is *ideal membership problem*
- Fundamental computational problem
- Decidable
- Our multivariate and multipolynomial division will give us an algorithm!
- EXPSPACE complete [Mayr & Meyer 80s]

Implicitization Problem

- Sometimes an algebraic set[2] is given to us in parametric form

[2] or "most" of it

Implicitization Problem

$$P(T) = \begin{cases} 0 & \text{if } \operatorname{trk}(T) \le r \\ \neq 0 & \text{otherwise} \end{cases}$$

- Sometimes an algebraic set[2] is given to us in parametric form
- Examples:
  - all matrices of rank $\leq r$
  - all tensors of rank $\leq r$
  - all polynomials computed by depth 3 circuits with top fanin k
  - Twisted cubic: $\{(t, t^2, t^3) \mid t \in \mathbb{F}\}$

$$\Big\{ \underbrace{\sum_{i=1}^{r} \begin{pmatrix} v_{1i} \\ \vdots \\ v_{ni} \end{pmatrix} (u_{1i}, \ldots, u_{ni})}_{M} \;\Big|\; u_{ij}, v_{ij} \in \mathbb{F} \Big\}$$

$(r+1) \times (r+1)$ minors of M must vanish

X

$V($all symbolic $r+1$ minors of $X)$

[2] or "most" of it

$P \in ?\ V(\underline{f_1, \dots, f_N})$

if N really large ($\exp(n)$)

is there a procedure to actually find witness

$f \in (f_1, \dots, f_N)$ f_i s.t.

$f(P) \neq 0$ $f_i(P) \neq 0$

what if I could sample $f \in (f_1, \dots, f_N)$ in poly(n) time?

Implicitization Problem

- Sometimes an algebraic set[2] is given to us in parametric form
- Examples:
  - all matrices of rank $\leq r$
  - all tensors of rank $\leq r$
  - all polynomials computed by depth 3 circuits with top fanin k
  - Twisted cubic: $\{(t, t^2, t^3) \mid t \in \mathbb{F}\}$
- Which begs the computational question:
  - **Input:** given a parametric description of a an algebraic set $V \subset \mathbb{F}^n$
  - **Output:** Equations $f_1, \ldots, f_s \in \mathbb{F}[x_1, \ldots, x_n]$ such that

$$V = \underline{V(f_1, \ldots, f_s)}$$

[2] or "most" of it

Solving Polynomial Equations

- **Input:** polynomials $f_1, \ldots, f_s \in \mathbb{F}[x_1, \ldots, x_n]$
- **Output:** is $V(f_1, \ldots, f_s) = \emptyset$? If not empty, output a solution

$$f_i(\bar{x}) = 0 \qquad i \in [s]$$

Solving Polynomial Equations

- **Input:** polynomials $f_1, \ldots, f_s \in \mathbb{F}[x_1, \ldots, x_n]$
- **Output:** is $V(f_1, \ldots, f_s) = \emptyset$? If not empty, output a solution
- The decision version of this problem is known as Hilbert's Nullstellensatz problem.

Solving Polynomial Equations

- **Input:** polynomials $f_1, \ldots, f_s \in \mathbb{F}[x_1, \ldots, x_n]$
- **Output:** is $V(f_1, \ldots, f_s) = \emptyset$? If not empty, output a solution
- The decision version of this problem is known as Hilbert's Nullstellensatz problem.
- (weak) Nullstellensatz gives us a certificate that a system of polynomial equations has NO solutions
- A solution $(a_1, \ldots, a_n)$ is a certificate of a solution
- This gives rise to an algebraic proof system! This proof system and its variants are widely used in computer science.

$1 \in (f_1, \ldots, f_s)$

Conclusion

- Today we saw overview of rings and algebraic sets
- Saw the relationship between ideals and algebraic sets
- Algebraic functions over varieties defined via coordinate rings
- Lots of computational questions related to algebraic sets
- Glimpse of hardness of algebraic computation (EXPSPACE territory)

Acknowledgement

- Lecture based largely on the book by CLO: Ideals, varieties and algorithms (see course webpage for a copy - or get online version through UW library)