Lecture 12: Introduction to Commutative Algebra and Algebraic Geometry

Rafael Oliveira

University of Waterloo
Cheriton School of Computer Science

rafael.oliveira.teaching@gmail.com

February 24, 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
  $$a \in I, s \in R \Rightarrow s \cdot a \in I$$

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)

$$I = \left\{ \sum_{i=1}^{t} a_i r_i \;\middle|\; r_i \in R \right\} =: (a_1, \ldots, a_t)$$

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

$(x) = \{ f(x) \in \mathbb{Q}[x] \mid f(0) = 0 \}$

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

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

Operations with Ideals

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

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

Operations with Ideals

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

$$I \cap J = \{ a \in R \mid a \in I \text{ and } a \in J \}$$

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 $\{ab \mid a \in I, \ b \in J\}$

∞'ly many generators

$I = (a_1, \ldots, a_t)$

$J = (b_1, \ldots, b_n)$

$IJ = (a_i b_j)_{i,j}$

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 $\{ab \mid a \in I,\ b \in J\}$
  4. $rad(I) := \{a \in R \mid \exists n \in \mathbb{N} \text{ s.t. } a^n \in I\}$ is an ideal

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

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

Quotient Rings

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

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

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

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 $\mathbb{Z}_2$

$\mathbb{Z}/2\mathbb{Z}$

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, $\mathbb{Z}_6$

$\mathbb{Z}_6$ not a domain (not field)

zero divisor $\bar{3} \cdot \bar{2} = \bar{0}$

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.

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 $b \in I$

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 $I + J = R$

$(a) + (b) = (gcd(a,b))$

"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 $ab = 0$

"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*: 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 nonzero 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

$x \neq 0$ but $x^2 \in (x^2)$

$\Rightarrow x^2 = 0$ in $\mathbb{Q}[x]/(x^2)$

"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

$ab \in I \Rightarrow a \in I$ or $b \in I$

$\bar{a}, \bar{b} \in R/I \quad \bar{a} \cdot \bar{b} = \bar{0} \Leftrightarrow a \cdot b \in I$

$\Rightarrow a \in I$ or $b \in I \Rightarrow \bar{a} = \bar{0}$ or $\bar{b} = 0$

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)

  and have ascending chain condition (ACC) for principal ideals

Principal ideal: ideal generated by single element.

ACC (for principal ideals): any chain of principal ideals

$(a_1) \subset (a_2) \subset (a_3) \subset \cdots$

$\exists N \in \mathbb{N}$ s.t. $(a_N) = (a_{N+1}) = (a_{N+1}) = \cdots$

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) not principal

Ring Homomorphisms

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

Rings ⟷ commutative rings with unit

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

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

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

are the *identity* homomorphisms.

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

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

  are the *identity* homomorphisms.
- Example:

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

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*.

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: $V(y - x^2, z - x^3)$

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: $V(xz, yz)$

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 $V(A\mathbf{x} - \mathbf{b})$

Properties of algebraic sets

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

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

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

$$I_\mathcal{F} = \left\{ f = \sum_{i=1}^{t} f_i r_i \;\middle|\; f_i \in \mathcal{F} \right\}$$

$$I_\mathcal{F} \supset \mathcal{F} \implies V(I_\mathcal{F}) \subset V(\mathcal{F})$$

$$a \in V(\mathcal{F}), \; f \in I_\mathcal{F}$$

$$f(a) = \sum_{i=1}^{t} \underbrace{f_i(a)}_{0} \cdot r_i(a) = 0$$

$$\implies V(\mathcal{F}) \subset V(I_\mathcal{F})$$

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 $I \subset \mathbb{F}[x_1, \ldots, x_n]$

$$V(I) = V(rad(I))$$

$$I \subset rad(I) \Rightarrow V(rad(I)) \subset V(I)$$

$$a \in V(I) \quad f \in rad(I) \Rightarrow f^n \in I$$

$$\Rightarrow f(a)^n = 0 \Rightarrow f(a) = 0$$

$$\Rightarrow a \in V(rad(I))$$

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

$$I \subset J \Rightarrow V(J) \subset V(I)$$

$U \subset \mathbb{F}^n$ $\quad I(U) = \{ f \in \mathbb{F}[x_1, \ldots, x_n] \mid f(a) = 0 \ \forall \ a \in U \}$

$(x) = \{ f \in \mathbb{Q}[x] \mid f(0) = 0 \} = I(\{0\})$

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 $I \subset \mathbb{F}[x_1, \ldots, x_n]$

$$V(I) = V(rad(I))$$

$rad(I) = I(V(rad(I)))$

- If I, J ideals

$$I \subset J \Rightarrow V(J) \subset V(I)$$

- 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!)

polynomial functions

or

rational functions

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

$$f - g \in I.$$

$$f = g + h, \quad h \in \mathrm{rad}(I)$$

$$a \in V(I)$$

$$f(a) = g(a) + h(a), \quad h(a) = 0$$

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

all polynomials $\mathbb{F}^n$

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

ring of polynomial functions in V

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 $f, g \in \mathbb{F}[x_1, \dots, x_n]$ yield same function iff

$$f - g \in I.$$

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

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

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

$\mathbb{F}[x]/(x^2) \leftrightarrow \{0\}$ multiplicity $\mathbb{F}[x]/(x)$

Algebraic Varieties

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

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

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.

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?*

$\mathcal{F}$ may not be finite

ideals can be given implicitly

as zero sets of a set of points

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

[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

- 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: $\{(t, t^2, t^3) \mid t \in \mathbb{F}\}$

$$V_1 = \{ M \in \mathbb{C}^{n \times n} \mid \mathrm{rank}(M) \leq r \}$$ linear algebra

$$= V\left((r+1) \times (r+1) \text{ minors of } X = (x_{ij}) \right)$$

$$P(\bar{x}) = \sum_{i=1}^{k} \prod_{j=1}^{d_i} \underbrace{l_{ij}(\bar{x})}_{\text{linear}}$$

$$(a_{ij1} x_1 + \cdots + a_{ijn} x_n + a_{ij0})$$

[2] or "most" of it

Implicitization Problem

"inverse problem of solving polynomial system of equations"

- 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

$$V = V(f_1, \ldots, f_s)$$

[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

$$f_1(\bar{x}) = 0$$
$$f_2(\bar{x}) = 0$$
$$\vdots$$
$$f_s(\bar{x}) = 0$$

does it have a solution?

$\Updownarrow$

$V(f_1, \ldots, f_s) \neq \emptyset$?

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

$$1 = f_1 g_1 + \cdots + f_s g_s$$

- **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.

$$V(f_1, \ldots, f_s) = \emptyset \iff 1 \in (f_1, \ldots, f_s)$$

$$(f_1, \ldots, f_s) = \mathbb{F}[x_1, \ldots, x_n]$$

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)