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* $I \subseteq R$ 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** $I \subseteq R$ is a subset of the ring $R$ such that:
  1. $I$ is closed under addition
     \[ a, b \in I \implies a + b \in I \]
  2. $I$ is closed under multiplication by elements of $R$
     \[ a \in I, s \in R \implies s \cdot a \in I \]

- 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 \textit{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 $x$
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:
  - $I + J$ 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

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

$IJ \neq I \cap J$
Operations with Ideals

\( \chi^2 \in I \)
\((n=2)\)

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

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

\[ \text{rad}(I) = (\chi) \]

\[ a^n = \chi^2 \cdot q(x) \implies a(0) = 0 \implies a \in (\chi) \]
Quotient Rings

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

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

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 $I$

  \[ a \sim b \iff a - b \in I \]

- If we only consider these equivalence classes, we have the \emph{quotient ring} $R/I$

  \[ R/I = \{ \overline{a+I} \mid a \in \mathbb{R} \} \]
Quotient Rings

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

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

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 $\mathbb{Z}_2$
Quotient Rings

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

  \[ a \sim b \iff a - b \in I \]

- 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 $I$

  \[ a \sim b \iff a - b \in I \]

- 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 $I$

\[ a \sim b \iff a - b \in I \]

- 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 $I$

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

- 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 $a \neq 0$ and there exists $b \in R \setminus \{0\}$ such that $ab = 0$

$\mathbb{Z}_6$

2 and 3 are zero divisors

$2 \cdot 3 = 0 \mod 6$

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

$x$ is zero divisor

$x^2 = 0$
“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 \( a^n = 0 \)
  - \( \mathbb{Q}[x]/(x^2) \) 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

$R/\text{rad}(I)$ 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 $(p)$

$$m = p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n}$$
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)
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)
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

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
  - $\phi(1) = 1$
  - $\phi(a + b) = \phi(a) + \phi(b)$
  - $\phi(ab) = \phi(a) \cdot \phi(b)$
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 $R/I$

\[ \phi : R \to R/I \]

\[ a \mapsto a + I \ (\bar{a}) \]
Ring Homomorphisms

- A **homomorphism** between rings $R$, $S$ is a map $\phi : R \rightarrow S$ 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 $\phi : R \rightarrow S$ and $\psi : S \rightarrow R$ such that $\phi \circ \psi : S \rightarrow S$ and $\psi \circ \phi : R \rightarrow R$ are the identity homomorphisms.

$$\phi \circ \psi (s) = s \quad \text{and} \quad \psi \circ \phi (r) = r$$
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 $R \cong S$ 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:

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

  *(special case of Chinese Remainder Theorem)*
- Elementary Commutative Algebra
- Algebraic Sets
- Structural & Computational Questions
- Conclusion
- Acknowledgements
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
\[
V(\mathcal{F}) := \{(a_1, \ldots, a_n) \in \mathbb{F}^n | f(a_1, \ldots, a_n) = 0 \text{ for all } f \in \mathcal{F}\}
\]
is called an \textit{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
  
  $$f(x_1, \ldots, x_n) = 0 \text{ for all } f \in \mathcal{F}$$

- 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 $F \subset \mathbb{F}[x_1, \ldots, x_n]$ the set

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

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 $f \in F$

- 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

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

is called an \emph{algebraic set}.

- Set of all solutions to the system of equations defined by

\[ f(x_1, \ldots, x_n) = 0 \text{ for all } f \in \mathcal{F} \]

- 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:
  - Circle: \( \mathcal{V}(x^2 + y^2 - 1) \)
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: $V(y - x^2, z - x^3)$

$$V(y-x^2, z-x^3) = \{(t_1, t^2, t^3) \mid t \in \mathbb{F}\}$$

Simplest example of a lot of complications.
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
  \[ f(x_1, \ldots, x_n) = 0 \text{ for all } f \in \mathcal{F} \]

- 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 \( V(Ax - b) \)
Properties of algebraic sets

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

\[
U = V \left( f_1, \ldots, f_s \right)
\]

\[
V = V \left( g_1, \ldots, g_t \right)
\]

\[
U \cup V = V \left( f_i, g_i \right)
\]

\[
V(\text{xz, yz}) = V(z) \cup V(x, y)
\]

\[
U \cap V = V \left( f_1, \ldots, f_s, g_1, \ldots, g_t \right)
\]
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

\[ V(\mathcal{F}) = V(I_\mathcal{F}) \]

\[ f, g \in \mathcal{F} \]
\[ \overline{a}, \quad f(\overline{a}) = g(\overline{a}) = 0 \implies (f + g)(\overline{a}) = 0 \]

\[ \sum_{i=1}^{n} f_i \cdot x_i \big( \overline{a} \big) = \sum_{i=1}^{n} f_i(\overline{a}) \cdot x_i(\overline{a}) = 0 \]
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 $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$

\[ V(I) = V(\text{rad}(I)) \]

\[ a \in \text{rad}(I) \implies a^n \in I \]

\[ p \in V(I) \implies a^n(p) = 0 \implies a(p) = 0 \]
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 $I \subset \mathbb{F}[x_1, \ldots, x_n]$
  \[ V(I) = V(\text{rad}(I)) \]
- 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 $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$
  \[ V(I) = V(\text{rad}(I)) \]

- If $I, J$ ideals
  \[ I \subseteq J \Rightarrow V(J) \subseteq V(I) \]

- 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:

\[ \text{rad}(I) = I(V(I)) \]
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

\[
\forall \bar{a} \in V(I) \quad f(\bar{a}) = g(\bar{a}) \iff (f - g)(\bar{a}) = 0
\]
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
  \[ \mathbb{F}[V] := \mathbb{F}[x_1, \ldots, x_n]/I \]
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)

\[ I = (x^2) \quad V(I) = V(J) \quad \mathbb{F}[x]/(x^2) \
\]
\[ J = (x) \quad (\mathbb{F}[x]/(x)) \]
An algebraic set $V$ is said to be **irreducible** if for any decomposition

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

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

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

oodle
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 \textit{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 \textit{algebraic variety}.

- \textbf{Practice problem:} prove that if $I$ is 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

\[ P(T) = \begin{cases} 0 & \text{if } \text{rank}(T) \leq r \\ \text{to otherwise} \end{cases} \]

- Sometimes an algebraic set 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: \( \{(t, t^2, t^3) \mid t \in \mathbb{F}\} \)

\[ \left\{ \sum_{i=1}^{r+1} \left( \begin{array}{c} u_{ii} \\ \vdots \\ u_{ni} \end{array} \right) (v_{i1}, \ldots, v_{in}) \mid u_{ij}, v_{ij} \in \mathbb{F} \right\} \]

\( (r+1) \times (r+1) \) minors of \( \mathcal{M} \) must vanish

\( \times \) \( \vee \) (all symbolic \( r+1 \) minors of \( \mathcal{M} \))
\[ P \in \mathbb{V}(f_1, \ldots, f_n) \]

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

is there a procedure to actually find witnesses

\( f \in (f_1, \ldots, f_n) \) \( L \) \( \vdash \)

\( L(P) \vdash f_i(P) \neq 0 \)

what if I could sample \( f \in (f_1, \ldots, f_n) \)
in \( \text{poly}(n) \) 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
    \[
    V = V(f_1, \ldots, f_s)
    \]

\(^2\) 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

\[ f_i(\bar{x}) = 0 \quad i \in [s] \]
Solving Polynomial Equations

- **Input:** polynomials $f_1, \ldots, f_s \in 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.

$$1 \in (f_1, \ldots, f_s)$$
Elementary Commutative Algebra

Algebraic Sets

Structural & Computational Questions

Conclusion

Acknowledgements
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)