Why Commutative Algebra?

Based on Eisenbud's Textbook Ch. 1

Dr. Zvi Rosen

Department of Mathematical Sciences,
Florida Atlantic University

FAU FLORIDA ATLANTIC UNIVERSITY

Three Great Research Projects

1. Number Theory.
2. Invariant Theory.
3. Algebraic Geometry.

Three Great Research Projects

1. Number Theory.
2. Invariant Theory.
3. Algebraic Geometry.

All required the machinery of commutative algebra to progress.

Number Theory: Fermat's Last Theorem

Theorem (Fermat's Last Theorem)

For $n > 2$, the equation $x^n + y^n = z^n$ has no nonzero integer solutions.

Claimed by Pierre de Fermat in 1637.

Proved by Andrew Wiles in...

Number Theory: Fermat's Last Theorem

Theorem (Fermat's Last Theorem)

For $n > 2$, the equation $x^n + y^n = z^n$ has no nonzero integer solutions.

Claimed by Pierre de Fermat in 1637.

Proved by Andrew Wiles in...1994.

Number Theory: Fermat's Last Theorem

Theorem (Fermat's Last Theorem)

For $n > 2$, the equation $x^n + y^n = z^n$ has no nonzero integer solutions.

Claimed by Pierre de Fermat in 1637.
Proved by Andrew Wiles in...1994.

Consider $\mathbb{Z}[\zeta]$ where $\zeta = \sqrt[n]{-1}$. $= e^{\pi i/n}$.

$$x^n + y^n = \left(\left(\frac{x}{y}\right)^n + 1\right) y^n$$

$$= \left[\prod_{k=0}^{n} \left(\frac{x}{y} - \zeta^{2k+1}\right)\right] y^n$$

$$= \prod_{k=0}^{n} \left(x - \zeta^{2k+1} y\right) = z^n.$$

Unique Factorization and $\mathbb{Z}[\zeta]$

Many rings of integers do not have unique factorization:

<u>Ex</u> $\mathbb{Z}[\sqrt{-5}]$.

$(1+\sqrt{-5})(1-\sqrt{-5}) = 6 = 2 \cdot 3$

3 irreducible, and not a factor of either term on LHS.

When $n = 23$, $\mathbb{Z}[\zeta]$ does NOT have unique factorization.

How CAN we factor?

Dedekind 1871: Don't factor elements, factor ideals:

$\mathbb{Z}[\sqrt{-5}]$. $(1+\sqrt{-5})(1-\sqrt{-5}) = 2 \cdot 3$.

Prime ideal: set of numbers P, so that $xy \in P \iff x \in P$ or $y \in P$.

$P_2 = (2, 1+\sqrt{-5}) = (2, 1-\sqrt{-5})$

$P_3 = (3, 1+\sqrt{-5})$

$P_3' = (3, 1-\sqrt{-5})$

$(6) = P_2^2 P_3 P_3'$

$P_2^2 = (2)$, $P_3 P_3' = (3)$

$P_2 P_3 = (1+\sqrt{-5})$, $P_2 P_3' = (1-\sqrt{-5})$

If you can factor ideals of a ring into prime ideals uniquely, then the resulting ring is a *Dedekind domain*.

Invariant Theory

Suppose that a group G acts on a space k^n, e.g. $\mathbb{C}^n$.

Which polynomial functions are *invariant* under that action?

Example ($G = \mathbb{Z}_2$)

g = generator. $\curvearrowright \mathbb{C}^1$.

$g \cdot x = -x$.

$g \cdot (p(x)) = p(x)$.

$p(-x) = p(x) \iff p(x) = \mathbb{C}[x^2]$.

S_n and Symmetric Polynomials

$G = S_n$ (symmetric group on n letters)

Let σ act on $(x_1, \ldots, x_n) \in \mathbb{C}^n$ as

$$\sigma . (x_1, \ldots, x_n) = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$$

$$e_1 = x_1 + \cdots + x_n$$

$$e_2 = x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n$$

$$\vdots$$

$$e_n = x_1 x_2 \cdots x_n .$$

$$(\mathbb{C}[x_1, \ldots, x_n])^{S_n} = \mathbb{C}[e_1, \ldots, e_n]$$

S_n and Symmetric Polynomials

ex $x_1^2 + x_2^2 + \cdots + x_n^2$

$= (x_1 + \cdots + x_n)^2 - 2(x_1x_2 + \cdots + x_{n-1}x_n)$

$= e_1^2 - 2e_2.$

Are Rings of Invariants all Polynomial Rings?

In general, no.

Example ($G = \mathbb{Z}_4$)

Let g act on (x, y) as $g(x, y) = (-y, x)$.

g generator

Are Rings of Invariants all Polynomial Rings?

In general, no.

Example ($G = \mathbb{Z}_4$)

Let g act on (x, y) as $g(x, y) = (-y, x)$.

Invariants:

$$\begin{aligned} U &= x^2 + y^2 \\ V &= x^2y^2 \\ W &= x^3y - xy^3 \end{aligned}$$

$$\begin{aligned} g \cdot W &= (-y)^3 x - (-y) x^3 \\ &= -y^3 x + y x^3 = x^3 y - x y^3 = W. \end{aligned}$$

Are Rings of Invariants all Polynomial Rings?

In general, no.

Example ($G = \mathbb{Z}_4$)

Let g act on (x, y) as $g(x, y) = (-y, x)$.

Invariants:

$$\begin{aligned} U &= x^2 + y^2 \\ V &= x^2y^2 \\ W &= x^3y - xy^3 \end{aligned}$$

They satisfy $(U^2 - 4V)V = W^2$

$$((x^2+y^2)^2 - 4x^2y^2)\,x^2y^2 \stackrel{?}{=} (x^3y - xy^3)^2$$

$$(x^4 - 2x^2y^2 + y^4)\,x^2y^2 \qquad \qquad (x^3y - xy^3)^2 = (x^2 - y^2)^2 x^2y^2$$

$$(x^2 - y^2)^2 x^2y^2 = (x^2 - y^2)^2 x^2y^2$$

Are they Finitely-Generated?

Hilbert, in 1890, proved that for many groups, the ring of invariants is finitely generated.

A key part of his proof was the Hilbert basis theorem.

Definition (Noetherian Ring)

Let R be a commutative ring. If every ideal $I \subseteq R$ is finitely generated, then R is called Noetherian.

Theorem (Hilbert Basis Theorem)

If R is Noetherian, then $R[x]$ is Noetherian.

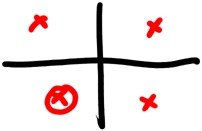
$\mathbb{C}[x_1, \ldots, x_n]$ is Noetherian.

Algebraic Geometry

Theorem (Fundamental Theorem of Algebra, 1806)

A polynomial in $\mathbb{C}[x]$ of degree n has exactly n roots counted with multiplicity.

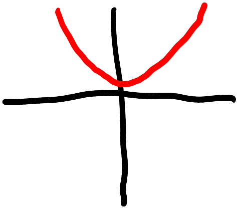
$$p(x) = \sum_{k=0}^{n} a_k x^k \quad \longleftrightarrow$$



$\mathbb{C}$

Example (Ideals in $\mathbb{C}$[x,y])

$$(x^2 - y) \quad \longleftrightarrow$$



$\mathbb{R}^2$

Ideals and Varieties

Definition ($Z(X)$)

Let $X \subseteq k[x_1, \dots, x_n]$ k field.

Define $Z(X) = \{(a_1, \dots, a_n) \mid f(a_1, \dots, a_n) = 0 \ \forall f \in X\}$

Zero-set of X. (Variety)

Definition ($I(S)$)

Let $S \subseteq k^n$, k field.

Define $I(S) = \{f \in k[x_1, \dots, x_n] \mid f(p) = 0 \ \forall p \in S\}$

Ideal of S.

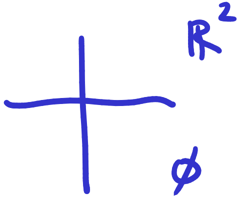
$S \subseteq Z(I(S))$ and $X \subseteq I(Z(X))$

When is this correspondence perfect?

- $\langle x^2+y^2+1\rangle \subseteq \mathbb{R}[x,y]$

$Z(X) = \emptyset$

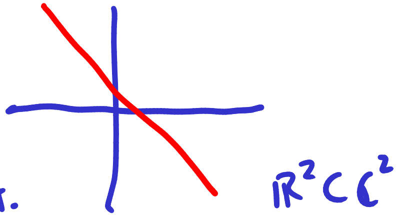
$I(Z(X)) = \mathbb{R}[x,y].$



- $\langle (x+y-1)^k\rangle \subseteq \mathbb{C}[x,y]$

$k=1,2,3,\dots$

all point to the same zero-set.



Hilbert's Nullstellensatz

"zero-places-theorem."

<u>Thm</u> Let k be an algebraically closed field. Then, radical ideals are in bijection with algebraic varieties.

Summary

Mathematical Area	Technology from Commutative Algebra
Number Theory	• UFDs. • Dedekind domain
Invariant Theory	• Symmetric poly's • Hilbert basis theorem.
Algebraic Geometry	• Fund. Thm. of Alg. • Hilbert's Nullst.sz.