Algebra: What Comes Next?

(In Math 4GR3 and Math 4ET3)

Mike Cummings

Math 3GR3, Tutorial 12
December 5, 2023

Slides available at:
math.mcmaster.ca/∼cummim5/teaching/2023/3GR3

Outline

Simple groups

Let G be a group. Recall:

- a subgroup N of G is **normal** if $gN = Ng$ for all g in G
- G is **simple** if it has no nontrivial normal subgroups

Examples of simple groups include:

- the alternating group A_n for $n \geq 5$
- $\mathbb{Z}_p$ for any prime p

Classification of finite simple groups

Theorem

Any finite simple group either is in one of the following inifinite families,

1. $\mathbb{Z}_p$,
2. A_n,
3. *a group of Lie type,*
4. *a derivative of a group of Lie type,*

or is one of 26 "sporadic groups" (such as the Monster)

Timeline of the classification

1832	Galois introduced normal subgroups, finds A_n
1872	Sylow Theorems proved
1892	Hölder asks for a classification of finite simple groups
1893	Cole classifies simple groups up to order 660

Work continued throughout the 1900s and culminated in 2004

Timeline of the classification

1832	Galois introduced normal subgroups, finds A_n
1872	Sylow Theorems proved
1892	Hölder asks for a classification of finite simple groups
1893	Cole classifies simple groups up to order 660

Work continued throughout the 1900s and culminated in 2004

Some mathematicians who worked on this problem include:

Galois, Sylow, Hölder, Cole, Jordan,
Frobenius, Dickson, Burnside, Conway, Gorenstein, Harada

Finitely generated groups

The group $\mathbb{Z} \times \mathbb{Z}_2$ is not cyclic, but it is *finitely generated*,

$$\mathbb{Z} \times \mathbb{Z}_2 = \langle (1,0), (0,1) \rangle$$

Finitely generated groups

The group $\mathbb{Z} \times \mathbb{Z}_2$ is not cyclic, but it is *finitely generated*,

$$\mathbb{Z} \times \mathbb{Z}_2 = \langle (1,0), (0,1) \rangle$$

Theorem (Fundamental Theorem of Finitely Generated Groups)

Any finitely generated group is isomorphic to

$$\mathbb{Z}^t \times \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_s^{r_s}}$$

for some primes $p_1 \ldots, p_s$ *and positive integer powers* $t, r_1, \ldots, r_s$

How?

- group actions
- Class equation
- Burnside's lemma
- composition series
- p-groups and Sylow theorems

PIDs

An integral domain R is a **principal ideal domain (PID)** if every ideal I of R can be generated by a single element

Example

- $\mathbb{Z}$, $\mathbb{Z}_n$
- any field
- $\mathbb{R}[x]$

PIDs

An integral domain R is a **principal ideal domain (PID)** if every ideal I of R can be generated by a single element

Example

- $\mathbb{Z}$, $\mathbb{Z}_n$
- any field
- $\mathbb{R}[x]$ but not $\mathbb{Z}[x]$

Irreducible and prime elements

Let R be an integral domain

- a **unit** in R is an element with a multiplicative inverse
- an non-zero and non-unit element $a \in R$ is **irreducible** if $a = bc$ implies that either b or c is a unit
- elements a and b in R are **associates** if $a = ub$ for a unit u

Irreducible and prime elements

Let R be an integral domain

- a **unit** in R is an element with a multiplicative inverse
- an non-zero and non-unit element $a \in R$ is **irreducible** if $a = bc$ implies that either b or c is a unit
- elements a and b in R are **associates** if $a = ub$ for a unit u

Example

- In $\mathbb{R}[x]$, the elements x and $2x$ are associates and irreducible
- In $\mathbb{Z}$, prime numbers are irreducible

UFDs

Theorem (Fundamental Theorem of Arithmetic)

1. *Any positive integer can be written as a product of primes*
2. *This product is unique up to reordering*

UFDs

Theorem (Fundamental Theorem of Arithmetic)

1. *Any positive integer can be written as a product of primes*
2. *This product is unique up to reordering*

Definition

An integral domain is a **unique factorization domain (UFD)** if

1. any element can be written as a product of irreducibles
2. this product is unique up to reordering and associates

PIDs and UFDs

Theorem

$PID \implies UFD$

PIDs and UFDs

Theorem

PID $\implies$ UFD, but the converse is false

Example

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] \quad \text{is a UFD but not a PID}$$

Other classes of rings

- Euclidean domains: integral domains with a division algorithm

Other classes of rings

- Euclidean domains: integral domains with a division algorithm
- Noetherian
- Artinian

Other classes of rings

- Euclidean domains: integral domains with a division algorithm
- Noetherian
- Artinian
- Local
- Regular local

Other classes of rings

- Euclidean domains: integral domains with a division algorithm
- Noetherian
- Artinian
- Local
- Regular local
- Regular

Varieties

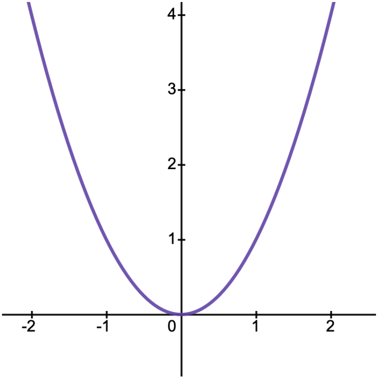


Figure: $\mathbb{V}(y - x^2)$

Varieties

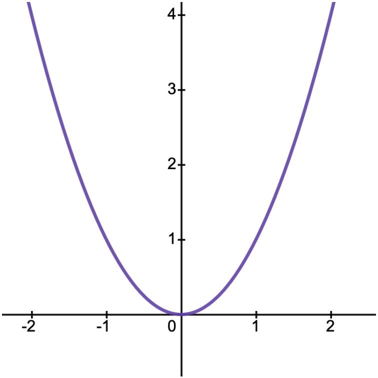


Figure: $\mathbb{V}(y - x^2)$

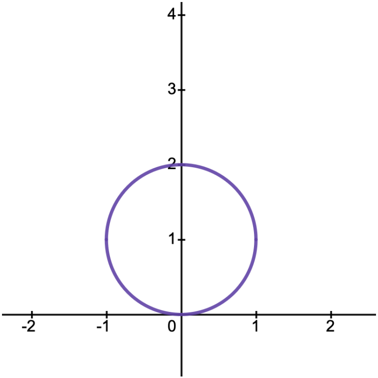
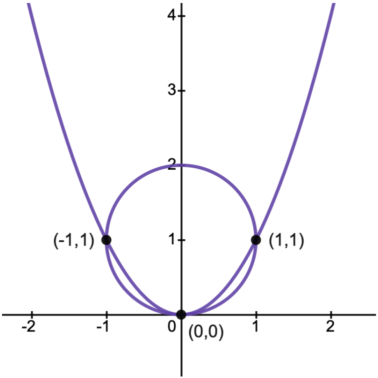


Figure: $\mathbb{V}\big(x^2 + (y-1)^2 - 1\big)$

Varieties



$$\mathbb{V}\left(y - x^2, x^2 + (y-1)^2 - 1\right)$$
$$= \left\{(0,0), (\pm 1, 1)\right\} \subseteq \mathbb{C}^2$$

Varieties $\leftrightarrow$ Ideals

$$V = \mathbb{V}(f_1, \ldots, f_r) \subseteq \mathbb{C}^n$$

$$\Updownarrow$$

$$\mathbb{I}(V) = \langle f_1, \ldots, f_r \rangle \subseteq \mathbb{C}[x_1, \ldots, x_n]$$

Coordinate ring

Let $V \subseteq \mathbb{C}^n$ be a variety

The **coordinate ring** $\mathbb{C}[V]$ of V is the ring of polynomials in n variables whose domain is V

Coordinate ring

Let $V \subseteq \mathbb{C}^n$ be a variety

The **coordinate ring** $\mathbb{C}[V]$ of V is the ring of polynomials in n variables whose domain is V

Example

Let $V = \mathbb{V}(x^2 + y^2 - 1) \subseteq \mathbb{C}^2$

- $f(x, y) = 0$
- $g(x, y) = y - x^2$
- $h(x, y) = x^2 + y^2 - 1$

Coordinate ring

Let $V \subseteq \mathbb{C}^n$ be a variety

The **coordinate ring** $\mathbb{C}[V]$ of V is the ring of polynomials in n variables whose domain is V

Example

Let $V = \mathbb{V}(x^2 + y^2 - 1) \subseteq \mathbb{C}^2$

- $f(x, y) = 0$
- $g(x, y) = y - x^2 = y + y^2 - 1$ on V
- $h(x, y) = x^2 + y^2 - 1$

Coordinate ring

Let $V \subseteq \mathbb{C}^n$ be a variety

The **coordinate ring** $\mathbb{C}[V]$ of V is the ring of polynomials in n variables whose domain is V

Example

Let $V = \mathbb{V}(x^2 + y^2 - 1) \subseteq \mathbb{C}^2$

- $f(x, y) = 0$
- $g(x, y) = y - x^2 = y + y^2 - 1$ on V
- $h(x, y) = x^2 + y^2 - 1 = 0$ on V, since $h \in \mathbb{I}(V)$

Coordinate ring

Let $V \subseteq \mathbb{C}^n$ be a variety

Define a homomorphism of rings

$$\begin{aligned} \varphi : \mathbb{C}[x_1, \ldots, x_n] &\to \mathbb{C}[x_1, \ldots, x_n] \\ \varphi(f) &= f|_V \end{aligned}$$

by restriction to V

Coordinate ring

Let $V \subseteq \mathbb{C}^n$ be a variety

Define a homomorphism of rings

$$\begin{aligned} \varphi : \mathbb{C}[x_1, \dots, x_n] &\to \mathbb{C}[x_1, \dots, x_n] \\ \varphi(f) &= f|_V \end{aligned}$$

by restriction to V

- the image of φ is $\mathbb{C}[V]$
- $\ker \varphi = \mathbb{I}(V)$

Coordinate ring

Let $V \subseteq \mathbb{C}^n$ be a variety

Define a homomorphism of rings

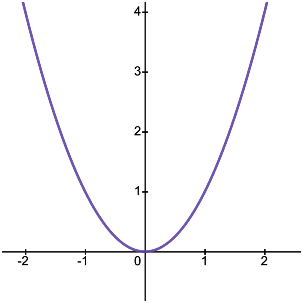
$$\begin{aligned} \varphi : \mathbb{C}[x_1, \ldots, x_n] &\to \mathbb{C}[x_1, \ldots, x_n] \\ \varphi(f) &= f|_V \end{aligned}$$

by restriction to V

- the image of φ is $\mathbb{C}[V]$
- $\ker \varphi = \mathbb{I}(V)$

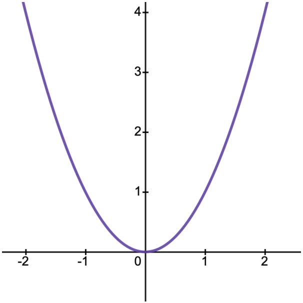
$$\mathbb{C}[V] \cong \mathbb{C}[x_1, \ldots, x_n]/\mathbb{I}(V)$$

Algebra "sees" geometry



$$V = \mathbb{V}(y - x^2) \subseteq \mathbb{C}^2 \qquad \mathbb{C}[V] \cong \mathbb{C}[x,y]/\langle y - x^2 \rangle \cong \mathbb{C}[x]$$

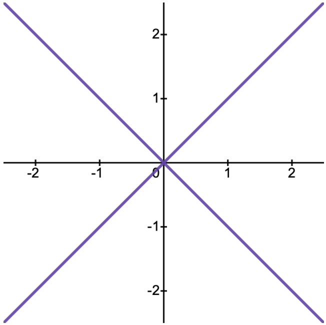
Algebra "sees" geometry



$$V = \mathbb{V}(y - x^2) \subseteq \mathbb{C}^2 \qquad \mathbb{C}[V] \cong \mathbb{C}[x, y]/\langle y - x^2 \rangle \cong \mathbb{C}[x]$$

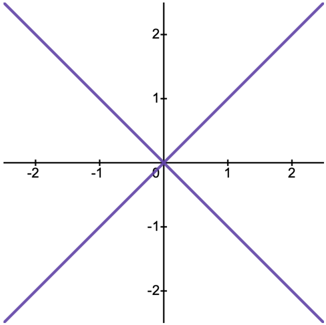
V "irreducible" $\qquad$ $\mathbb{I}(V)$ prime $\qquad$ $\mathbb{C}[V]$ integral domain

Algebra "sees" geometry



$$V = \mathbb{V}\big((y-x)(y+x)\big) \qquad \mathbb{C}[V] \cong \mathbb{C}[x,y]/\langle y^2 - x^2\rangle$$

Algebra "sees" geometry



$$V = \mathbb{V}\big((y-x)(y+x)\big) \qquad \mathbb{C}[V] \cong \mathbb{C}[x,y]/\langle y^2 - x^2 \rangle$$

	$\mathbb{I}(V)$ not prime	$\mathbb{C}[V]$ not an integral domain
V "reducible"	$y - x \notin \mathbb{I}(V)$	
	$y + x \notin \mathbb{I}(V)$	$(y-x)(y+x) \in \mathbb{I}(X)$

Morphisms and isomorphisms

Let $V \subseteq \mathbb{C}^n$ and $W \subseteq \mathbb{C}^m$ be varieties

A **map of varieties** $\varphi : V \to W$ is of the form

$$\varphi(a_1, \dots, a_n) = \big(f_1(a_1, \dots, a_n), \dots, f_m(a_1, \dots, a_n)\big)$$

where each f_i is a polynomial in n variables

Morphisms and isomorphisms

Let $V \subseteq \mathbb{C}^n$ and $W \subseteq \mathbb{C}^m$ be varieties

A **map of varieties** $\varphi : V \to W$ is of the form

$$\varphi(a_1, \ldots, a_n) = \big(f_1(a_1, \ldots, a_n), \ldots, f_m(a_1, \ldots, a_n)\big)$$

where each f_i is a polynomial in n variables

An **isomorphism** is a bijective map that admits an inverse; we say that V and W are **isomorphic**

Example of an isomorphism

$$V = \mathbb{V}(0) = \mathbb{C} \qquad\qquad W = \mathbb{V}(y - x^2) \subseteq \mathbb{C}^2$$

$$\varphi : V \to W \qquad\qquad \psi : W \to V$$

$$\varphi(t) = (t, t^2) \qquad\qquad \psi(u, v) = u$$

Example of an isomorphism

$$V = \mathbb{V}(0) = \mathbb{C} \qquad W = \mathbb{V}(y - x^2) \subseteq \mathbb{C}^2$$

$$\varphi : V \to W \qquad \psi : W \to V$$

$$\varphi(t) = (t, t^2) \qquad \psi(u, v) = u$$

$$\mathbb{C}[V] \cong \frac{\mathbb{C}[t]}{\langle 0 \rangle} = \mathbb{C}[t] \qquad \mathbb{C}[W] \cong \frac{\mathbb{C}[x, y]}{\langle y - x^2 \rangle} \cong \mathbb{C}[x]$$

Isomorphisms of varieties and coordinate rings

Theorem

Let $V \subseteq \mathbb{C}^n$ *and* $W \subseteq \mathbb{C}^m$ *be varieties*

$$V \cong W \quad \textit{if and only if} \quad \mathbb{C}[V] \cong \mathbb{C}[W]$$

Nodal cubic

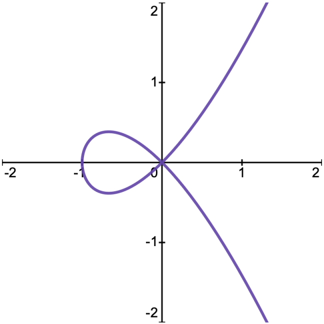


Figure: $V = \mathbb{V}(y^2 - x^3 - x^2)$

Question: $V \cong \mathbb{C}$?

Nodal cubic

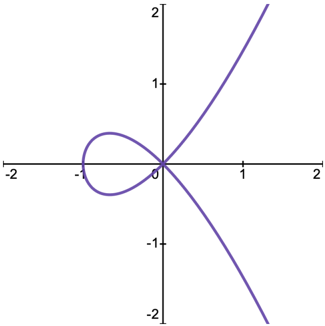


Figure: $V = \mathbb{V}(y^2 - x^3 - x^2)$

$$\mathbb{C}[V] \cong \frac{\mathbb{C}[x, y]}{\langle y^2 - x^3 - x^2 \rangle}$$

Question: $V \cong \mathbb{C}$?

Nodal cubic

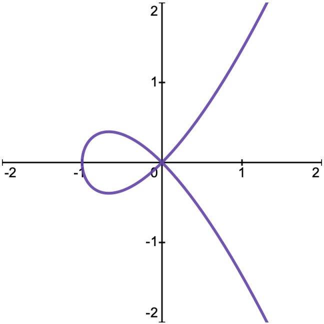


Figure: $V = \mathbb{V}(y^2 - x^3 - x^2)$

$$\mathbb{C}[V] \cong \frac{\mathbb{C}[x,y]}{\langle y^2 - x^3 - x^2 \rangle} \ncong \mathbb{C}[t]$$

Question: $V \cong \mathbb{C}$?

Nodal cubic

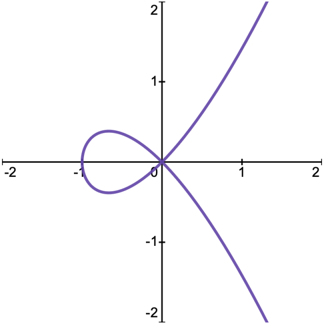


Figure: $V = \mathbb{V}(y^2 - x^3 - x^2)$

Question: $V \cong \mathbb{C}$?

$$\mathbb{C}[V] \cong \frac{\mathbb{C}[x,y]}{\langle y^2 - x^3 - x^2 \rangle} \ncong \mathbb{C}[t]$$

In $\mathbb{C}[V]$,

$$\begin{aligned} y^2 &= y \cdot y \\ &= x^2(x+1) \end{aligned}$$

$\mathbb{C}[V]$ is not a UFD, but $\mathbb{C}[t]$ is

So $V \ncong \mathbb{C}$

Twisted cubic

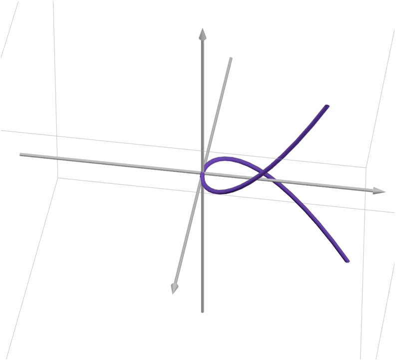


Figure: $V = \mathbb{V}(y - x^2, z - x^3)$

Desmos 3D Link

Twisted cubic

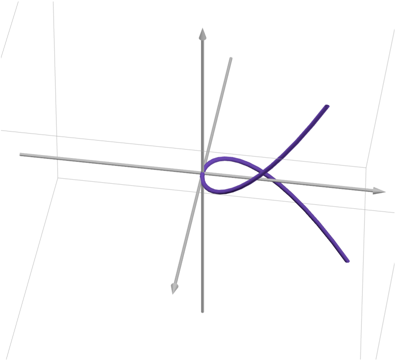


Figure: $V = \mathbb{V}(y - x^2, z - x^3)$

Desmos 3D Link

$$V \cong \mathbb{C}$$

Twisted cubic

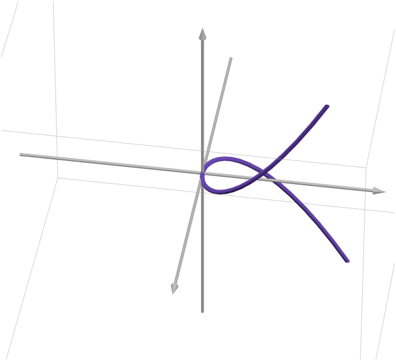


Figure: $V = \mathbb{V}(y - x^2, z - x^3)$

Desmos 3D Link

$$V \cong \mathbb{C}$$

$$\begin{aligned}\mathbb{C}[V] &\cong \frac{\mathbb{C}[x,y,z]}{\langle y - x^2, z - x^3 \rangle} \\ &\cong \mathbb{C}[x, x^2, x^3] \\ &\cong \mathbb{C}[x]\end{aligned}$$

Cuspidal cubic

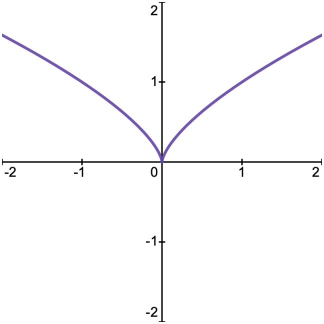


Figure: $V = \mathbb{V}(y^3 - x^2)$

$$V \ncong \mathbb{C}$$

$$\mathbb{C}[V] \cong \frac{\mathbb{C}[x,y]}{\langle y^3 - x^2 \rangle}$$

Not a UFD:

$$y^3 = y \cdot y \cdot y = x \cdot x$$

What else?

“Classical” algebraic geometry

- intersection theory
- Schubert calculus

What else?

“Classical” algebraic geometry

- intersection theory
- Schubert calculus

Connections to number theory

- Arithmetic and elliptic curves

What else?

“Classical” algebraic geometry

- intersection theory
- Schubert calculus

Connections to number theory

- Arithmetic and elliptic curves

Computational algebraic geometry (Math 4ET3)

- Gröbner bases
- degeneration (initial ideals)

Reading

Groups and Rings

- Judson, Chapters 13–15, 17, 18, 21
- Dummit and Foote. Abstract Algebra

Algebraic Geometry

- Karen Smith et al. Invitation to Algebraic Geometry
- Cox, Little, and O'Shea. Ideals, Varieties, and Algorithms