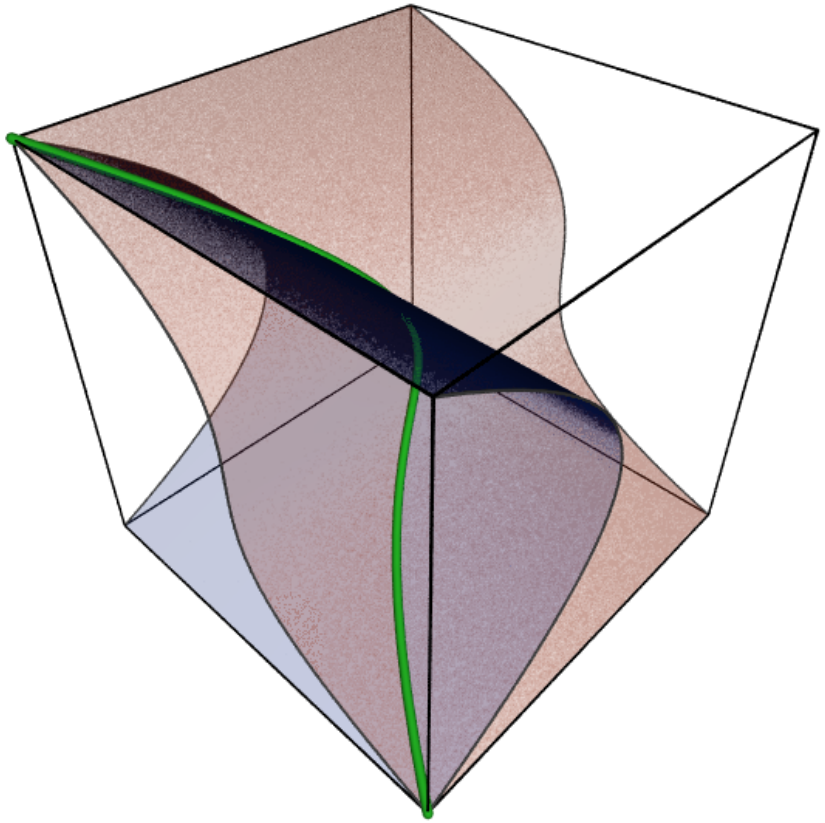
# Bezout's Theorem and Applications

Nicholas Hiebert-White

December 3, 2018

# What is Algebraic Geometry?

It's the study of solutions of systems of polynomial equations (originally).



The "Twisted Cubic" - The Solution set of $XZ - Y^2 = 0$, $Y - Z^2 = 0$, $X - YZ = 0$ (Twisted Cubic)

# Affine Plane Curves

**Definition**

The **affine plane** over a field $k$,

$$\mathbb{A}^2(k) = \{(x, y) \mid x, y \in k\}$$

is the cartesian product of $k$ with itself.

**Definition**

An **affine plane curve** $C$ is a set of the form

$$C := V(F) := \{(x, y) \in \mathbb{A}^2(k) \mid F(x, y) = 0\}$$

for some polynomial $F \in k[X, Y]$.

# Affine Plane Curves

## Definition

The **affine plane** over a field $k$,

$$\mathbb{A}^2(k) = \{(x, y) \mid x, y \in k\}$$

is the cartesian product of $k$ with itself.

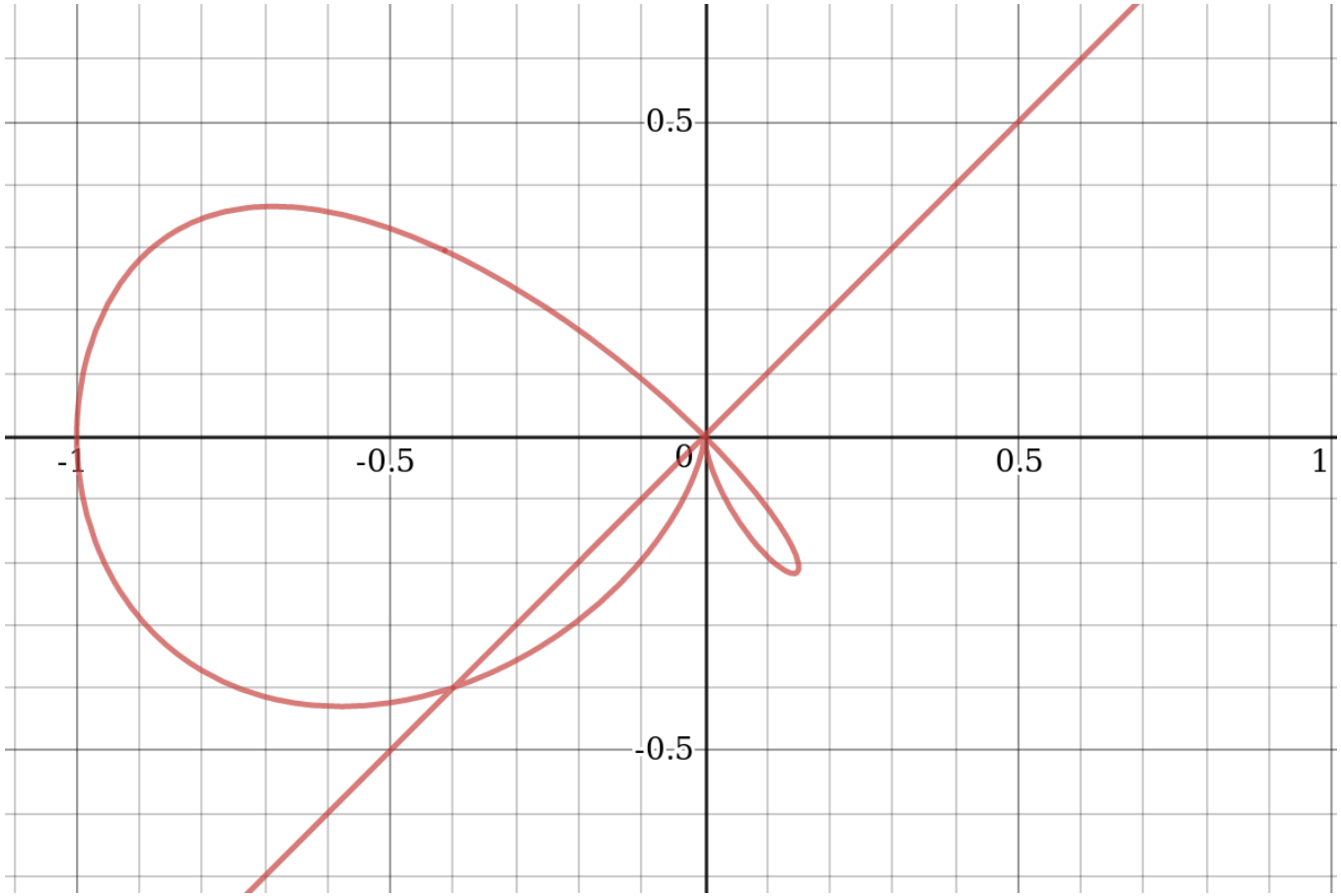
## Definition

An **affine plane curve** $C$ is a set of the form

$$C := V(F) := \{(x, y) \in \mathbb{A}^2(k) \mid F(x, y) = 0\}$$

for some polynomial $F \in k[X, Y]$.

# Example




Affine plane curve $V(X^4 - X^2Y^2 + X^5 - Y^5)$ in $\mathbb{A}^2(\mathbb{R})$

# Motivating Question

If $k$ is a field, and $F$ is a nonzero polynomial in $k[X]$, then $F$ has at most $\deg(F)$ roots. In particular if $k$ is algebraically closed $F$ has exactly $\deg(F)$ roots counting multiplicities.

**Question**

Given two polynomials $F, G \in k[X, Y]$, how many points are there in $V(F) \cap V(G)$?

# Motivating Question

If $k$ is a field, and $F$ is a nonzero polynomial in $k[X]$, then $F$ has at most $\deg(F)$ roots. In particular if $k$ is algebraically closed $F$ has exactly $\deg(F)$ roots counting multiplicities.

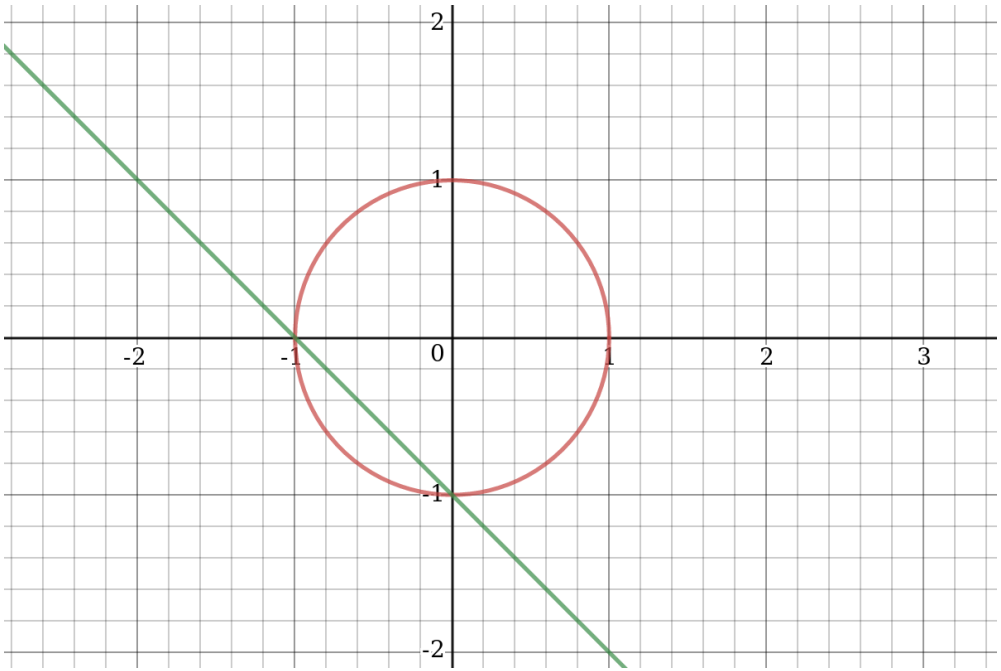
**Question**

Given two polynomials $F, G \in k[X, Y]$, how many points are there in $V(F) \cap V(G)$?

# Intersections of Plane Curves

**Theorem**

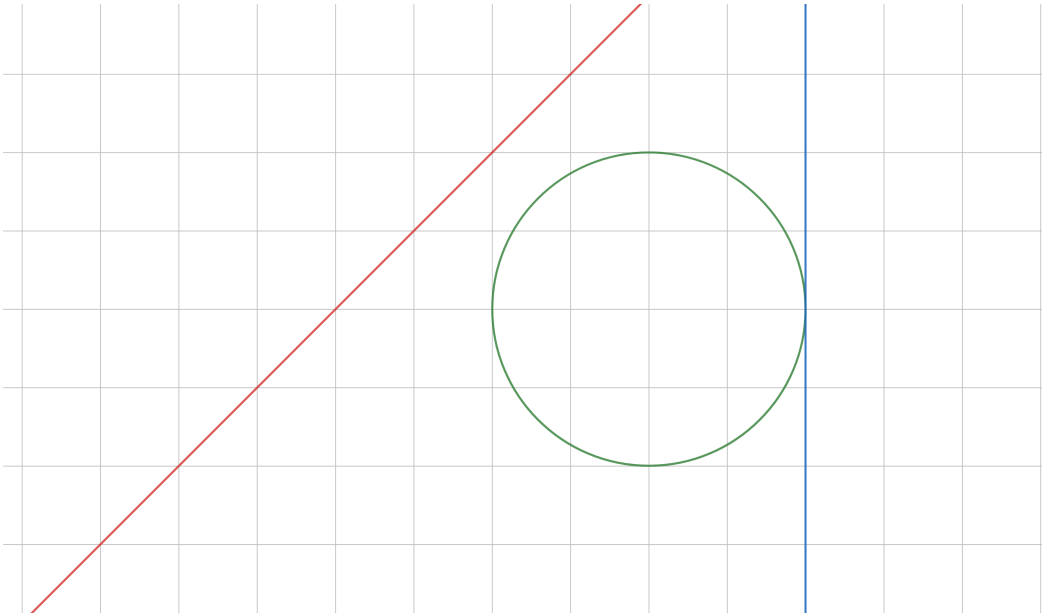
*Let $F, G \in k[X, Y]$ be nonzero polynomials that share no common factors. Then the affine plane curves $V(F)$ and $V(G)$ intersect at most at $\deg(F)\deg(G)$ points.*




The affine plane curves $V(X^2 + Y^2 - 1)$ and $V(X + Y + 1)$ in $\mathbb{A}^2(\mathbb{R})$

# Example

Sometimes curves intersect at less than $\deg(F)\deg(G)$ points.



# What is Missing?

- We need $k$ to be an algebraically closed field ($V(X^2 + Y^2 + 1)$ is empty in $\mathbb{A}^2(\mathbb{R})$ but not in $\mathbb{A}^2(\mathbb{C})$.)
- We need a "bigger" space (Parallel lines do not intersect in $\mathbb{A}^2(k)$)
- We need a notion of intersection multiplicity. (The intersection of the circle with its tangent line should be counted twice)

# What is Missing?

- We need $k$ to be an algebraically closed field
  ($V(X^2 + Y^2 + 1)$ is empty in $\mathbb{A}^2(\mathbb{R})$ but not in $\mathbb{A}^2(\mathbb{C})$.)
- We need a "bigger" space
  (Parallel lines do not intersect in $\mathbb{A}^2(k)$)
- We need a notion of intersection multiplicity.
  (The intersection of the circle with its tangent line should be counted twice)

# What is Missing?

- We need $k$ to be an algebraically closed field
  ($V(X^2 + Y^2 + 1)$ is empty in $\mathbb{A}^2(\mathbb{R})$ but not in $\mathbb{A}^2(\mathbb{C})$.)
- We need a "bigger" space
  (Parallel lines do not intersect in $\mathbb{A}^2(k)$)
- We need a notion of intersection multiplicity.
  (The intersection of the circle with its tangent line should be counted twice)

# Intersection Multiplicity

There is a "technical" definition of intersection multiplicity:

**Definition**

For any $F, G \in k[X, Y]$ and $P \in \mathbb{A}^2(k)$, the **intersection multiplicity** of $F$ and $G$ at $P$ is:

$$I(F \cap G, P) := dim_k \left( \frac{\mathcal{O}_P(\mathbb{A}^2)}{(F, G)} \right)$$

But it is also completely determined by a set of basic properties, such as:

1. $I(P, F \cap G)$ is nonnegative integer, or infinity (iff $F, G$ share common component at $P$).
2. $I(P, F \cap G) = 0$ iff $P \notin V(F) \cap V(G)$
3. $I(P, F \cap G) = I(P, G \cap F)$
4. $I(F_1 F_2 \cap G, P) = I(F_1 \cap G, P) + I(F_2 \cap G, P)$

# Intersection Multiplicity

There is a "technical" definition of intersection multiplicity:

**Definition**

For any $F, G \in k[X, Y]$ and $P \in \mathbb{A}^2(k)$, the **intersection multiplicity** of $F$ and $G$ at $P$ is:

$$I(F \cap G, P) := dim_k \left( \frac{\mathcal{O}_P(\mathbb{A}^2)}{(F, G)} \right)$$

But it is also completely determined by a set of basic properties, such as:

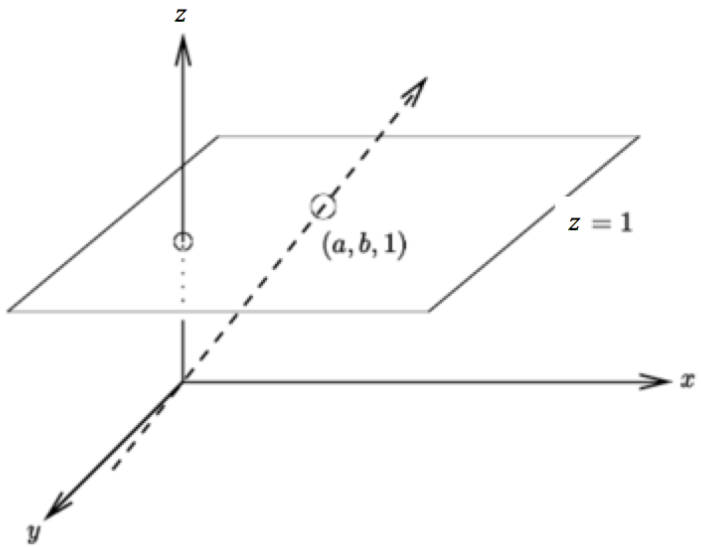
1. $I(P, F \cap G)$ is nonnegative integer, or infinity (iff $F, G$ share common component at $P$).
2. $I(P, F \cap G) = 0$ iff $P \notin V(F) \cap V(G)$
3. $I(P, F \cap G) = I(P, G \cap F)$
4. $I(F_1 F_2 \cap G, P) = I(F_1 \cap G, P) + I(F_2 \cap G, P)$

# Projective Plane

## Definition

The **Projective Plane** $\mathbb{P}^2(k)$ is set of 1-dimensional subspaces of $k^3$, or equivalence classes of points $(x, y, z) \in k^3$ under $(x, y, z) \sim (x', y', z')$ iff $(x, y, z) = (\lambda x', \lambda y', \lambda z')$ for some $\lambda \in k^*$

- The lines that do not lie in the plane $Z = 0$ form an affine plane.
- The lines in the plane are called the "points at infinity".



# Bézout's Theorem

## Definition

A **projective plane curve** $C$ is a set of the form

$$C := V(F) := \{[x : y : z] \in \mathbb{P}^2(k) \mid F(x, y, z) = 0\}$$

for some homogeneous polynomial $F \in k[X, Y, Z]$.

## Theorem (Bézout's Theorem)

*Let $k$ be an algebraically closed field. Let $F, G \in k[X, Y, Z]$ be nonzero homogeneous polynomials that share no common factors. Then the projective plane curves $V(F)$ and $V(G)$ intersect at $\deg(F)\deg(G)$ points counting intersection multiplicities.*

# Bézout's Theorem

## Definition

A **projective plane curve** $C$ is a set of the form

$$C := V(F) := \{[x : y : z] \in \mathbb{P}^2(k) \mid F(x, y, z) = 0\}$$

for some homogeneous polynomial $F \in k[X, Y, Z]$.

## Theorem (Bézout's Theorem)

*Let $k$ be an algebraically closed field. Let $F, G \in k[X, Y, Z]$ be nonzero homogeneous polynomials that share no common factors. Then the projective plane curves $V(F)$ and $V(G)$ intersect at* $\deg(F)\deg(G)$ *points counting intersection multiplicities.*

# Results

**Proposition**

Let $C, C'$ projective cubics (curves defined by homogeneous polynomials of degree 3). If $P_1, \ldots, P_9$ are the points of intersection of $C$ with $C'$ and there is a conic $Q$ intersecting with $C$ exactly at $P_1, \ldots, P_6$. Then $P_7, P_8, P_9$ lie on the same line.

**Corollary (Pascal)**

*If a hexagon is inscribed in an irreducible conic, then the opposite sides meet at collinear points.*

**Corollary (Pappus)**

*Let $L_1, L_2$ two lines and $P_1, P_2, P_3$ and $Q_1, Q_2, Q_3$ points in $L_1$ and $L_2$ respectively, but not in $L_1 \cap L_2$. For $i, j, k \in \{1, 2, 3\}$ distinct, let $R_k$ be the point of intersection of the line through $P_i$ and $Q_j$ with the line through $P_j$ and $Q_k$. Then $R_1, R_2, R_3$ are collinear.*

# Results

## Proposition

Let $C, C'$ projective cubics (curves defined by homogeneous polynomials of degree 3). If $P_1, \ldots, P_9$ are the points of intersection of $C$ with $C'$ and there is a conic $Q$ intersecting with $C$ exactly at $P_1, \ldots, P_6$. Then $P_7, P_8, P_9$ lie on the same line.

## Corollary (Pascal)

*If a hexagon is inscribed in an irreducible conic, then the opposite sides meet at collinear points.*

## Corollary (Pappus)

*Let $L_1, L_2$ two lines and $P_1, P_2, P_3$ and $Q_1, Q_2, Q_3$ points in $L_1$ and $L_2$ respectively, but not in $L_1 \cap L_2$. For $i, j, k \in \{1, 2, 3\}$ distinct, let $R_k$ be the point of intersection of the line through $P_i$ and $Q_j$ with the line through $P_j$ and $Q_k$. Then $R_1, R_2, R_3$ are collinear.*

# Results

## Proposition

Let $C, C'$ projective cubics (curves defined by homogeneous polynomials of degree 3). If $P_1, \ldots, P_9$ are the points of intersection of $C$ with $C'$ and there is a conic $Q$ intersecting with $C$ exactly at $P_1, \ldots, P_6$. Then $P_7, P_8, P_9$ lie on the same line.

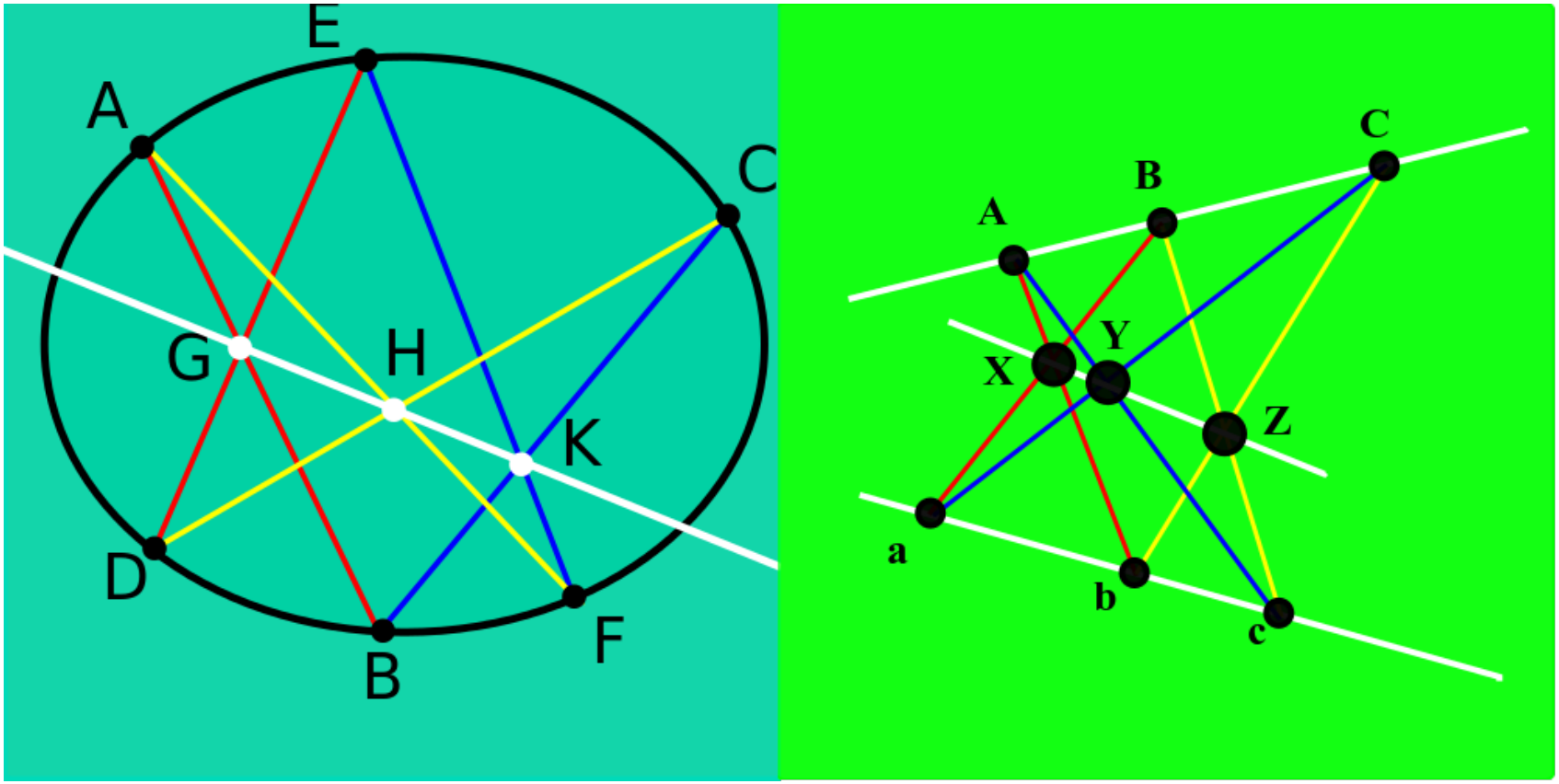
## Corollary (Pascal)

*If a hexagon is inscribed in an irreducible conic, then the opposite sides meet at collinear points.*

## Corollary (Pappus)

*Let $L_1, L_2$ two lines and $P_1, P_2, P_3$ and $Q_1, Q_2, Q_3$ points in $L_1$ and $L_2$ respectively, but not in $L_1 \cap L_2$. For $i, j, k \in \{1, 2, 3\}$ distinct, let $R_k$ be the point of intersection of the line through $P_i$ and $Q_j$ with the line through $P_j$ and $Q_k$. Then $R_1, R_2, R_3$ are collinear.*

# Pascal's and Pappus's Theorems




*Left:* Example of Pascal's Theorem

*Right:* Example of Pappus's Theorem

# Elliptic Curves

Let $C$ a nonsingular cubic and $O$ a point in $C$. For $P, Q \in C$, let $L$ the line from $P$ to $Q$ and

$$P \cdot Q = (L \bullet C) - P - Q$$

Define also

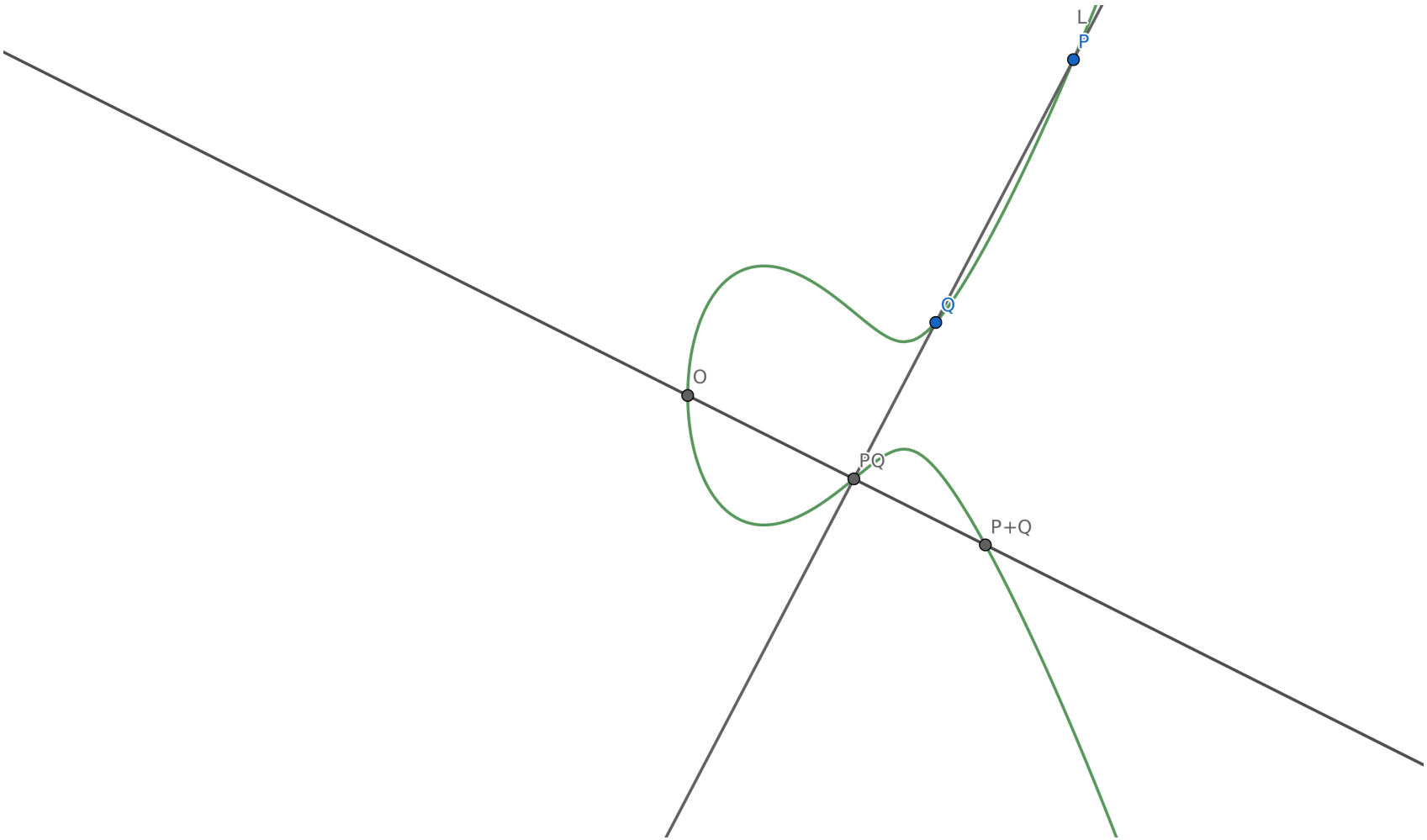
$$P \oplus Q = O \cdot (P \cdot Q)$$

**Theorem**

*$(C, \oplus)$ is an abelian group.*

Such curves $C$ with a choice of point $O$ are called elliptic curves and are used widely in number theory.

# Elliptic Curves (continued)




Addition on an elliptic curve

# References

W. Fulton. *Algebraic Curves: An Introduction to Algebraic Geometry*. 2008.