LECTURE 1: INTRODUCTION TO ALGEBRAIC GEOMETRY

1. What is algebraic geometry?

Algebraic geometry is the study of the geometric properties of solutions to systems of algebraic equations. This includes (among other things):

(1) How to describe or find solutions algebraically;
(2) The geometry and topology of the space of solutions;
(3) Counting the number of solutions when there are a finite number.

We will treat systems of algebraic equations as abstract geometric objects called **algebraic varieties**, or simply **varieties**. (Precise definitions of affine and projective algebraic varieties will come in later lectures.) The set of points on a variety X defined over a field K will be denoted $X(K)$.

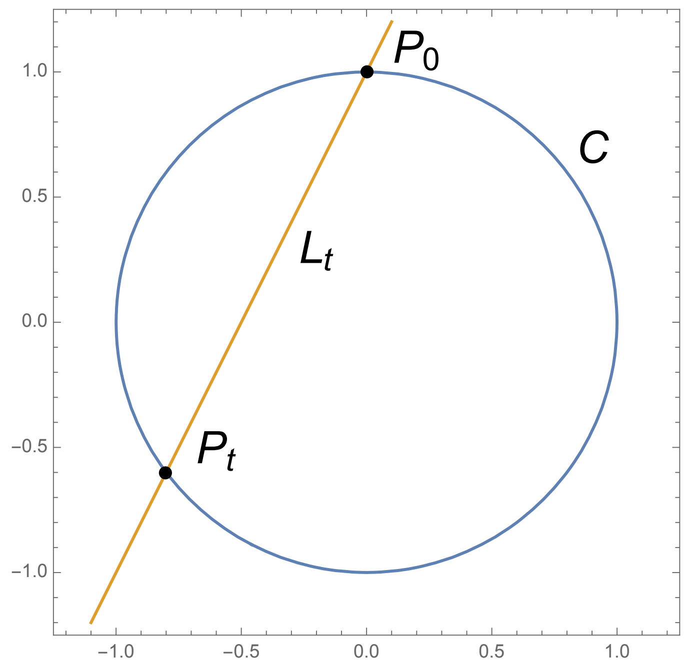
1.1. Example: the unit circle.

For a field K, let $C(K)$ be the set of points

$$C(K) = \{(x, y) \in K^2 : x^2 + y^2 = 1\}. \tag{1.1}$$

In particular, $C(\mathbb{R})$ is the unit circle in $\mathbb{R}^2$.

The unit circle C has a *rational parametrisation*—that is, a parametrisation by rational functions (ratios of polynomials). Consider the line L_t through the point $(0, 1)$ of slope t. The line L_t intersects the circle in exactly two points: $(0, 1)$ and another point P_t.



Finding P_t is a matter of solving the simultaneous equations

$$x^2 + y^2 = 1 \text{ and } y = tx + 1. \tag{1.2}$$

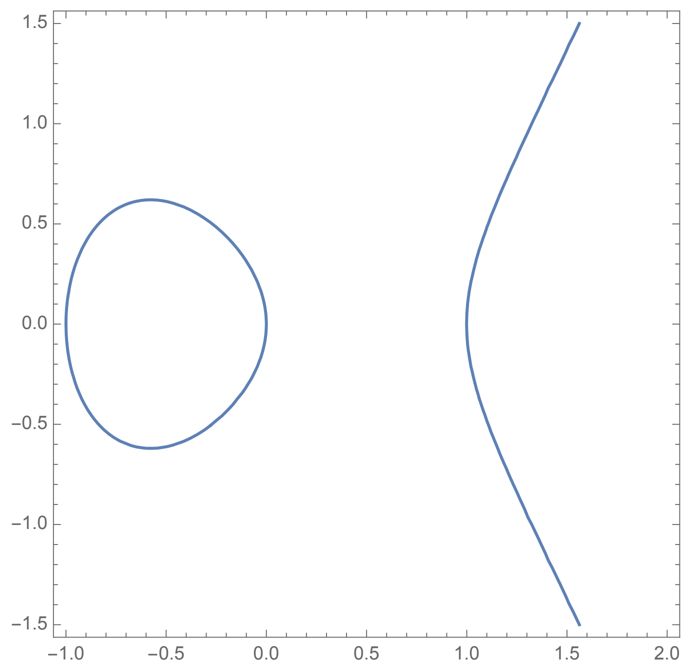
We find that $P_t = \left(\frac{-2t}{t^2+1}, \frac{-t^2+1}{t^2+1}\right)$. As t ranges over the set of real numbers, each point on the circle appears exactly once—including the original point $(0,1) = P_0$—with the exception of the point $(0,-1)$, which should correspond to the vertical line $y = 0$ of "infinite" slope.

The unit circle $C(\mathbb{R}) \subset \mathbb{R}^2$ is a *curve* in the traditional sense: a topological subspace of $\mathbb{R}^n$ that locally looks like $\mathbb{R}$. However, if we look at the *complex* points $C(\mathbb{C})$, we get a 2-dimension *surface* in $\mathbb{C}^2 \cong \mathbb{R}^4$. Indeed, in can be shown that $C(\mathbb{C})$ is topologically equivalent to a sphere with one point missing.

Nonetheless, we will refer to $C(\mathbb{C})$ as a **(complex) algebraic curve**, or an algebraic variety of dimension 1. We will justify this terminology—and define a general notion of the dimension of a variety—later in the unit.

1.2. **Example: a smooth cubic curve.** Let E be the curve defined by the equation

$$E : y^2 = x^3 - x. \tag{1.3}$$



There are some remarkable differences between E and the circle C discussed in the last section.

- Unlike the circle, E has no rational parametrisation.
- The set of complex points $E(\mathbb{C})$ forms a torus with a point missing (rather than a sphere with a point missing).

1.3. **Intersections of curves.** If two algebraic curves in $\mathbb{R}^2$ or $\mathbb{C}^2$ share no common component, then they will have finitely many points of intersection.

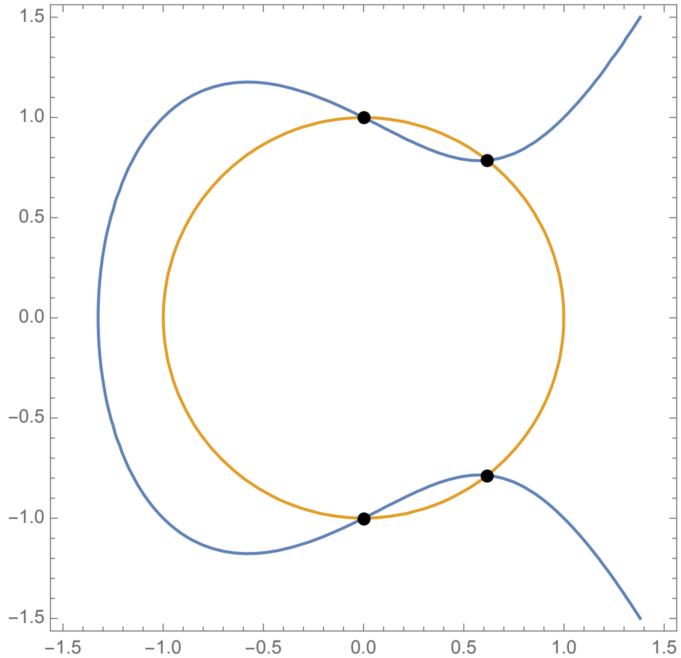
Near the end of the unit, we will prove Bézout's theorem, a result about the number of points of intersection of two complex algebraic curves. A rough, non-rigorous statement of Bézout's theorem is: Given algebraic curves C defined by an equation of degree m and D defined by an equation of degree n, with no common component, they will have mn points of intersection, provided that...

- we count complex points, not just real points;
- we count points "with multiplicity";
- we count points "at infinity".

The two curves

$$C : \{x^2 + y^2 = 1\} \text{ and } D : \{y^2 = x^3 - x + 1\} \tag{1.4}$$

have four real points of intersection, as we can see.



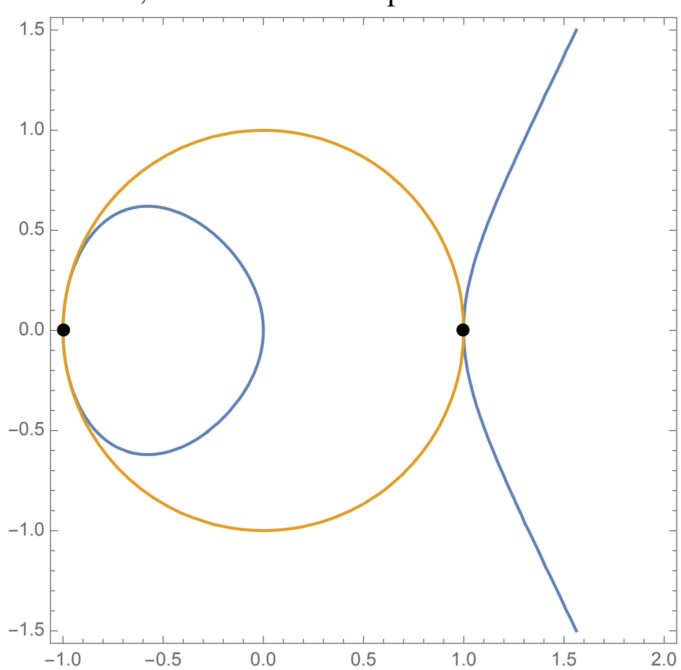
However, they actually have $6 = 2 \cdot 3$ points of intersection over $\mathbb{C}$. If $\phi = \frac{1+\sqrt{5}}{2}$, then

$$C(\mathbb{C}) \cap D(\mathbb{C}) = \{(0,1), (0,-1), (\phi^{-1}, \phi^{-1/2}), (\phi^{-1}, -\phi^{-1/2}), (-\phi, i\phi^{1/2}), (-\phi, -i\phi^{1/2})\}. \tag{1.5}$$

The two curves

$$C : \{x^2 + y^2 = 1\} \text{ and } E : \{y^2 = x^3 - x\} \tag{1.6}$$

have only 2 points of intersection, even over the complex numbers.



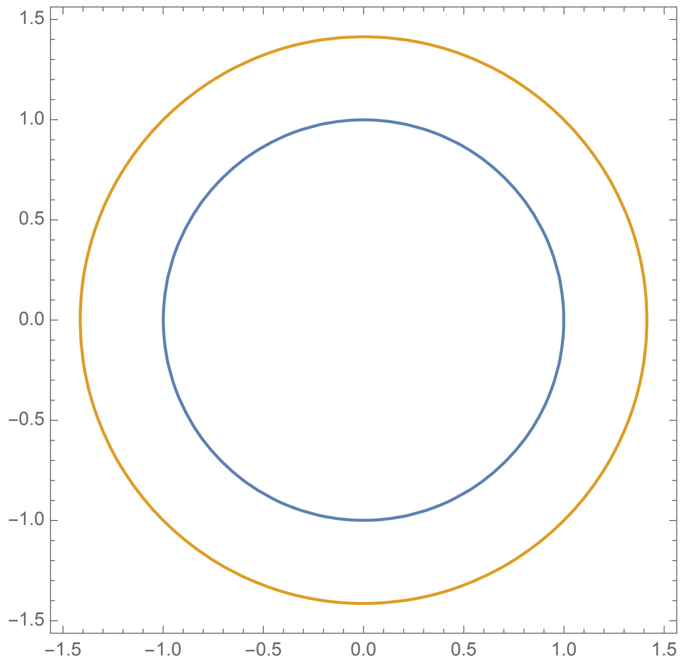
$$C(\mathbb{C}) \cap D(\mathbb{C}) = \{(1,0),(-1,0)\}. \tag{1.7}$$

However, notice how the curves are tangent at these two points. We will later define an *intersection multiplicity*, and we will be able to say that C and C intersect "with multiplicity 2" at $(1,0)$ and intersect "with multiplicity 4" at $(-1,0)$.

The two curves

$$C : \{x^2 + y^2 = 1\} \text{ and } F : \{x^2 + y^2 = 2\} \tag{1.8}$$

have no points of intersection (even over the complex numbers), because $1 \neq 2$.



However, after we develop the theory of projective geometry, we will define a precise sense in which C and F have 2 points of intersection "at infinity", each of multiplicity 2.

2. Revision of algebra topics

The mathematical foundations of algebraic geometry is *commutative algebra*. The basic objects of study in commutative algebra are *commutative rings with unity*. Unless otherwise specified, all rings R will be commutative rings with unity:

- R is a ring;
- $ab = ba$ for all $a, b \in R$;
- There is $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.

In this unit, we will be dealing primarily with polynomial rings $R = \mathbb{C}[x_1, \dots, x_n]$ and their quotients and localisations. (In all the major results we will prove, the field of complex numbers $\mathbb{C}$ could be replaced by any algebraically closed field of characteristic zero without changing the statements or proofs.)

2.1. Ideals, Spec, and mSpec.

Definition 2.1. *A subset $I \subseteq R$ is called an* ***ideal*** *if it satisfies the following properties:*

- *If $a, b \in I$, then $a + b \in I$.*
- *If $r \in \mathbb{R}$ and $a \in I$, then $ar \in I$.*

The ideal generated by $a_1, \dots, a_n \in R$ will be written as

$$(a_1, \dots, a_n) := \{a_1 r_1 + \cdots + a_n r_n : r_j \in R\}. \tag{2.1}$$

An ideal (a) with a single generator is called **principal**.

Definition 2.2. *An ideal I is* ***prime*** *if it satisfies the following properties:*

- *$I \neq R$;*
- *If $ab \in I$, then $a \in I$ or $b \in I$.*

The set of all the prime ideals is called the ***spectrum*** *of R and is denoted by* $\operatorname{Spec}(R)$.

The whole ring R is always an ideal

Definition 2.3. *An ideal I is* ***maximal*** *if it satisfies the following properties:*

- *$I \neq R$;*
- *If $I \leq J \leq R$, then $J = I$ or $J = R$.*

The set of all maximal ideals of R is called the ***maximal spectrum*** *of R and is denoted by* $\operatorname{mSpec}(R)$.

Proposition 2.4. *Every maximal ideal is prime.*

Proof. Let I be a maximal ideal of R, and suppose $ab \in I$. Then,

$$I \leq I + (a) \text{ and } I \leq I + (b), \tag{2.2}$$

so each of $I + (a)$ and $I + (b)$ are either I or R. If they are both R, then there exists $r, s \in I$ such that $r + a = s + b = 1$, so $1 = (r + a)(s + b) = rs + br + as + ab \in I$, so $R = I$, which is impossible by the definition of "maximal". Thus, at least one of $I + (a)$ and $I + (b)$ is equal to I, so $a \in I$ or $b \in I$. $\square$

Example 2.5. *The prime ideals of $\mathbb{C}[x]$ are the*

$$\operatorname{Spec}(\mathbb{C}[x]) = \{(x - a) : a \in \mathbb{C}\} \cup \{(0)\}; \tag{2.3}$$

$$\operatorname{mSpec}(\mathbb{C}[x]) = \{(x - a) : a \in \mathbb{C}\}. \tag{2.4}$$

Example 2.6. *The prime ideals of $\mathbb{C}[x, y]$ are the*

$$\operatorname{Spec}(\mathbb{C}[x]) = \{(x - a, y - b) : a, b \in \mathbb{C}\} \cup \{(f(x, y)) : f(x, y) \textit{ is irreducible } \} \cup \{(0)\}; \tag{2.5}$$

$$\operatorname{mSpec}(\mathbb{C}[x]) = \{(x - a, y - b) : a, b \in \mathbb{C}\}. \tag{2.6}$$

2.2. **Quotient rings and localisation.** Let R be a (commutative) ring R (with unity).

Definition 2.7. *Let I be an ideal of R. The* ***quotient ring*** *R/I is defined to be the set of cosets*

$$R/I = \{r + I : r \in R\}. \tag{2.7}$$

Definition 2.8. *Let S be any subset of R. The localisation $S^{-1}R$ of R with respect to S is formally defined as a ring of "fractions" $\frac{r}{s}$, with the addition and multiplication laws*

- $\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$;
- $\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}$;

and the equivalence relation

$$\frac{r_1}{s_1} = \frac{r_2}{s_2} \textit{ in } S^{-1}R \iff r_1 s_2 = r_2 s_1 \textit{ in } R. \tag{2.8}$$

If I is an ideal of R, then the localisation at I is defined to be

$$R_I := (R \setminus I)^{-1} R. \tag{2.9}$$

2.3. **Some ring properties.** Let R be a (commutative) ring R (with unity).

Definition 2.9. *The ring R is a **domain** (or "integral domain") if*

- $1 \neq 0$*;*
- *If $ab = 0$, then $a = 0$ or $b = 0$.*

Note that an ideal I of R is prime if and only if R/I is a domain, and I is maximal if and only if R/I is a field.

Definition 2.10. *The ring R is a **local ring** if R has a unique maximal ideal.*

If I is a prime ideal, then R_I is a local ring.

Definition 2.11. *The ring R is a **principal ideal domain (PID)** if*

- *R is a domain;*
- *Every ideal $I \leq R$ is principal, that is, $I = (a)$ for some $a \in R$.*

Definition 2.12. *The ring R is a **unique factorisation domain (UFD)** if it is a domain and every element has a unique decomposition into prime elements (i.e., elements generating prime ideals), up to ordering and multiplication by units. Precisely,*

- *R is a domain;*
- *Every nonzero $r \in R$ has a decomposition $r = p_1 \cdots p_m$ into $p_j \in R$ such that (p_j) is a prime ideal;*
- *If $p_1 \cdots p_m = q_1 \cdots q_n$ such that the (p_j) and (q_j) are nonzero prime ideals, then $m = n$, and there is a permutation $\sigma \in S_n$ such that each $q_j = u_j p_{\sigma(j)}$ for some $u_j \in R^\times$.*

Some facts about PIDs and UFDs will be used throughout the unit:

- Every PID is a UFD.
- If K is a field, then the ring $K[x]$ is a PID.
- If K is a field and $n \geq 2$, then the ring $K[x_1, \ldots, x_n]$ is a UFD but is not a PID.