

**BOSTON UNIVERSITY SOCIETY OF MATHEMATICS COLLOQUIUM  
PROCEEDINGS  
AN INVITATION TO ALGEBRAIC GEOMETRY THROUGH CONICS.**

SKYLER MARKS

**ABSTRACT.** In high school algebra 1 and 2, we study the theory of single variable polynomial equations. In linear algebra, we study systems of linear equations, or polynomial equations with no exponents greater than 1. Algebraic Geometry combines these disciplines to study polynomial equations (in particular, their solutions) in many variables. This theory is useful as it is specific enough that we can compute with it, yet general enough that it applies to many problems we care about. The promised invitation will be extended by way of plane conics and cubics. After some definitions and preliminaries, we will review a family of classical results regarding plane conics (quadratic polynomials in two variables). We will begin by classifying conics into families whose members are alike. We will then leverage this classification to study the intersections of two conics. Our conclusion to this first act will be a detailed discussion of the number of conics passing through  $n$  points in the plane, introducing Moduli spaces and projective space.

**WARNING:** These notes may contain errors; if you find any, please email me at [skyler@bu.edu](mailto:skyler@bu.edu).

**NOTE:** These notes are designed for a general audience, but include remarks directed towards those with a background in algebraic geometry.

1. PRELIMINARIES

We'll be working primarily with polynomials in two variables with complex coordinates:

**Definition 1.1.** The **ring of polynomials in two variables**, denoted  $\mathbb{C}[x, y]$  is the set of all polynomials in two indeterminates together with the standard operations.

**Remark 1.2.** As far as I know, much of what follows generalizes to  $k[x, y]$  where  $k = \bar{k}$ , although some things may fail in e.g. characteristic 2. No guarantees on any of these notes, but even less if you're working in positive characteristic.

**Example 1.3.** The polynomials  $x^2y + 1$ ,  $x^2 + y$ ,  $y^2 + x^2$ , and  $x^2 + x$  are all elements of  $\mathbb{C}[x, y]$ . Recall that:

$$\begin{aligned}(x^2 + y) + (y^2 + x^2) &= 2x^2 + y^2 + y \\ (x^2 + y)(y^2 + x^2) &= x^2y^2 + x^4 + y^3 + x^2y\end{aligned}$$

**Definition 1.4.** Polynomials with no power higher than 1, like  $x - 1$  and  $y - 2$ , are called **linear**.

This notion motivates the following definition:

---

*Key words and phrases.* Algebraic Geometry, Algebra, Introduction, Conic, Moduli.

**Definition 1.5.** The **degree** of a single term is the sum of the powers in that term. The degree of a polynomial is the highest degree of any monic term.

**Definition 1.6.** An **ideal** in the ring of polynomials is a subset of the set  $\mathbb{C}[x, y]$  which is closed under addition and multiplication by any element in  $\mathbb{C}[x, y]$ .

**Definition 1.7.** A **morphism of rings** or **ring homomorphism** is a function  $f$  between two rings satisfying  $f(a + b) = f(a) + f(b)$  and  $f(ab) = f(a)f(b)$ . An **isomorphism** of rings is an invertible morphism.

**Definition 1.8.** We'll call the set of all pairs  $(z_1, z_2)$  for  $z_1, z_2 \in \mathbb{C}$  the **affine plane over  $\mathbb{C}$**  and denote it  $\mathbb{A}^2$ .

**Lemma 1.9.** *Pick some subset  $S$  of affine space. The set  $I(S)$  of all polynomials which vanish at  $S$  is an ideal.*

*Proof.* Exercise. □

**Definition 1.10.** We define the **vanishing set** of a polynomial  $f(x, y)$ , denoted  $V(f)$ , to be the set where the polynomial is zero:

$$V(f) = \{(x, y) \in \mathbb{A}^2 \mid f(x, y) = 0\}$$

We broadly wish to study, in this section, the vanishing set of polynomials of degree two; we'll call these conics:

**Definition 1.11.** A **conic** is the zero set of a polynomial of degree 2.

*Question 1.12.* We can state our main goals for this section formally as follows:

- (1) What can the set  $V(f)$  “look like” for  $f$  a degree 2 polynomial?
- (2) What does the set  $V(f) \cap V(g)$  “look like” for  $f, g$  degree two polynomials? In particular, how many points does this set contain?
- (3) What are the elements of  $I(\{p_1, \dots, p_n\})$  for  $p_i = (x_i, y_i)$  a point in  $\mathbb{A}^2$ , and for all  $n \in \mathbb{N}$ ? (how many quadratics pass through  $n$  points).

These three questions exemplify three of the main fields of algebraic geometry: namely, birational geometry / the classification problem, intersection theory, and moduli theory. The first field seeks to classify all *algebraic varieties* (things which look locally like affine algebraic sets, more or less) up to some form of isomorphism; the second seeks to study how often and in what ways two such algebraic varieties intersect; the third seeks to describe families of mathematical objects using geometric objects.

The final concept that will allow us to answer these questions is a notion of isomorphism between vanishing sets of polynomials; that is, a way of determining when two vanishing sets are “essentially the same”. This will allow us to formalize and answer Question 1.12, points 1 and 2. In order to do this, we need a little more algebra:

**Definition 1.13.** Let  $R$  be a ring (in particular, the ring  $\mathbb{C}[x, y]$  of polynomials), and let  $I$  be an ideal. The **quotient**  $R/I$  is then the set of cosets of the form  $f + I$  for an element  $f$ .

**Lemma 1.14.** *The quotient  $R/I$  is a ring under the operations  $(p+I) + (q+I) = (p+q) + I$  and  $(p+I)(q+I) = (pq) + I$ .*

*Proof.* C.F. [DF08] □

**Remark 1.15.** One can consider the quotient by the ideal generated by an element  $f$  to be “evaluation at  $f = 0$ ”, or the quotient by an ideal to be the identification of everything in that ideal with zero. Indeed, we see this information captured formally in:

**Theorem 1.16** (The First Isomorphism Theorem). *Let  $f: R \rightarrow S$  be a morphism of rings; that is, a map satisfying  $f(a + b) = f(a) + f(b)$  and  $f(ab) = f(a)f(b)$ . Then  $\ker(f) = \{x \in R \mid f(x) = 0\}$  is an ideal, and  $\text{Im}(f) \cong R/\ker(f)$ . In particular, if  $f$  is surjective,  $S \cong R/\ker(f)$ . (Here  $\cong$  denotes isomorphism).*

*Proof.* C.F. [DF08] □

**Definition 1.17.** We define the **affine coordinate ring** of a subset  $S$  of  $\mathbb{A}^2$  to be  $k[x, y]/I(S)$ . We say that two (algebraic) subsets of  $\mathbb{A}^2$  are isomorphic (“look the same”) if their affine coordinate rings are isomorphic.

**Definition 1.18.** A **algebraic set** is the zero set of a polynomial in affine space. Thus the above definition associates to each algebraic set its affine coordinate ring.

**Remark 1.19** (Affine Schemes - Should probably be ignored). This association is extremely important in algebraic geometry. Those who are well-versed in abstract algebra could benefit from convincing themselves that (1) there is a bijection between points in  $\mathbb{A}^2$  and maximal ideals in  $k[x, y]$  (this is simple;  $(a, b) \mapsto (x - a, y - b)$ ), (2) that this bijection also descends to algebraic subsets of  $\mathbb{A}^2$  (think carefully about what it means for a maximal ideal in  $k[x, y]$  to remain a maximal ideal in  $k[x, y]/(f)$ ), and (3) that this argument extends to show that there is an inclusion-reversing bijection between points in algebraic sets in  $\mathbb{A}^2$  and prime ideals in their coordinate rings. If one is excited by this line of reasoning, one might continue to show that if  $g$  is a function in  $k[x, y]$ , we have that  $g/(x - a, y - b) = g(a, b)$ . This discussion motivates the construction of **affine schemes**: instead of our geometric object being a set of tuples of complex numbers, we take it to be a set of prime ideals in a ring; the zero set of a function (any element of the ring)  $f$  becomes the set of all prime ideals which include  $f$ . This captures all of the geometric intuition we develop here, but is far more powerful and general.

## 2. CONICS UP TO ISOMORPHISM

In math, a huge portion of our work is classifying objects up to some sort of isomorphism - in our case, isomorphism of affine varieties. Such a question is a good answer to Question 1.12, part 1; it turns out we can classify plane conics in a very satisfying way. Furthermore, we’ll see in the next section that this classification is extremely useful (in particular, for proving Theorem 3.4) as well as being interesting in and of itself.

**Theorem 2.1.** *Suppose  $\phi = ly^2 + axy + bx^2 + cx + dy + e$  defines a conic  $Z(\phi)$ . Then if  $4b - a^2 = 0$ ,  $A(Z(\phi)) \cong \mathbb{C}[x, y]/(y^2 - x)$ ; otherwise,  $A(Z(\phi)) \cong \mathbb{C}[x, y]/(xy - 1)$ .*

*Proof.* First consider the case where  $l = b = 0$ . Then  $\phi = axy + cx + dy + e$ . Then add and subtract  $\frac{cd}{a}$  ( $a \neq 0$ , as otherwise  $Z(\phi)$  would be a degenerate conic) to obtain  $\phi = axy + cx + dy + \frac{cd}{a} - \frac{cd}{a} + e$ . Factor to obtain  $\phi = (ax + d)(y + \frac{c}{a}) - \frac{cd}{a} + e$ . Consider the transformation  $\psi: Z(\phi) \rightarrow Z(xy + \tilde{e})$  by the rule  $(x, y) \mapsto (\frac{x-d}{a}, y + \frac{c}{a})$ . Clearly this is a polynomial function with a polynomial inverse, and thus a regular isomorphism. Thus

$$Z(\phi) \cong Z(xy + \tilde{e})$$

Moreover, another transformation  $f: Z(xy + \tilde{e}) \rightarrow Z(\tilde{e}xy + \tilde{e})$  can be constructed, by the rule  $(x, y) \mapsto (\tilde{e}x, y)$  (which is well defined as  $k = \tilde{k}$ ). Thus, as multiplication by a scalar does not change the zeros of a polynomial,  $Z(\phi) \cong Z(xy + 1)$ .

However, if  $l$  or  $b$  is nonzero, (suppose  $l$  without loss of generality) then we can divide to obtain a monic polynomial for new coefficients  $a, b, \dots$

$$y^2 + ayx + bx^2 + dy + cx + e$$

Add and subtract  $\frac{(ax)^2}{4}$ :

$$y^2 + ayx + \frac{(ax)^2}{4} - \frac{(ax)^2}{4} + bx^2 + dy + cx + e$$

Factor

$$\left(y + \frac{ax}{2}\right)^2 - \frac{(ax)^2}{4} + bx^2 + dy + cx + e$$

Use the transformation  $(x, y) \mapsto (x, y - \frac{ax}{2})$ . Note this is an isomorphism with inverse  $(x, y) \mapsto (x, y + \frac{ax}{2})$  and image

$$Z\left(y^2 - \frac{(ax)^2}{4} + bx^2 + d\left(y - \frac{ax}{2}\right) + cx + e\right)$$

Which simplifies to

$$Z(y^2 + b'x^2 + c'x + d'y + e')$$

If  $b' = 0$ , then if  $c' = 0$  the polynomial is a quadratic in  $y$  and splits, so  $c'$  or  $b'$  are nonzero.

First suppose  $c'$  is nonzero:

$$= Z(y^2 + c'x + d'y + e')$$

Add and subtract  $\frac{d'^2}{4}$  and factor to obtain

$$= Z\left(\left(y + \frac{d'}{2}\right)^2 - \frac{d'^2}{4} + c'x + e'\right)$$

Then another affine transformation  $(x, y) \mapsto \left(y - \frac{d'}{2}, \frac{-x + \frac{d'^2}{4} - e'}{c'}\right)$  yields the intended result

$$\cong Z(y^2 - x)$$

Suppose, then, that  $b' \neq 0$ .

$$Z(y^2 + b'x^2 + c'x + d'y + e')$$

Then add and subtract  $\left(\frac{c'}{2b'}\right)^2$  and factor:

$$Z\left(y^2 + \left(\sqrt{b'}x + \frac{c'}{2b'}\right)^2 - \left(\frac{c'}{2b'}\right)^2 + d'y + e'\right)$$

Another coordinate transform and re-labelling coefficients gives

$$\cong Z(y^2 + x^2 + d'y + \tilde{e})$$

Complete the square and transform again to obtain

$$\cong Z(y^2 + x^2 + \rho)$$

$$\cong Z((x + iy)(x - iy) + \rho)$$

. Transform  $(x, y) \mapsto (x + iy, y)$

$$\cong Z((x + 2iy)(x) + \rho)$$

Transform  $(x, y) \mapsto (x, \frac{-i}{2}(y - x))$ .

$$\cong Z(xy + \rho)$$

Transform  $(x, y) \mapsto (\rho x, y)$ , and note that scalar multiplication does not change the zeros of a polynomial:

$$\cong Z(xy + 1)$$

□

This solves Question 1.12, part 1.

### 3. INTERSECTIONS OF CONICS

We now address our second question, namely how many points two conics meet in. This is a classical problem; the intersections of lines and the simultaneous vanishing of higher-order polynomial functions has occupied much of the study of both algebra and geometry for quite some time. The notion that the algebraic viewpoint and the geometric viewpoint are linked, and can be used in concert, has been extremely fruitful and lead to modern-day *intersection theory*.

**Lemma 3.1.** *If  $T_i$  for each natural  $i$  are subsets of  $\mathbb{C}[x, y]$ , then:*

$$V(T_1) \cup V(T_2) = V(T_1 T_2)$$

Where  $T_1 T_2$  is the ideal generated by all products of elements in  $T_1$  and  $T_2$ , and

$$\bigcap_i V(T_i) = V\left(\bigcup_i T_i\right)$$

**Remark 3.2.** Those who are familiar with the topic will recognize that the above are the closure conditions necessary to specify the closed sets of a topology; indeed, the topology whose closed sets are the vanishing sets of polynomials is called the Zariski topology, and is the (main) topology used in algebraic geometry.

**Lemma 3.3.**

$$\mathbb{C}[x, y]/(f, g) \cong (\mathbb{C}[x, y]/(f)) / (g)$$

*Proof.* Consider the map  $\psi: \mathbb{C}[x, y] \rightarrow (\mathbb{C}[x, y]/(f)) / (g)$  by the rule  $a \mapsto (a + (f)) + (g)$ . Clearly this is surjective; any element in  $(\mathbb{C}[x, y]/(f)) / (g)$  is of the form  $(a + (f)) + (g)$ . Moreover, the kernel of this map is exactly  $(f, g)$ ;  $a \in (f, g)$  if and only if  $a = xf + yg$ ; <sup>1</sup> $f$  is killed by the first quotient and  $g$  is killed by the second, so  $a$  maps to zero if and only if it is of this form. Then we are done by Theorem 1.16. □

**Theorem 3.4.** *Let  $f$  and  $g$  be degree 2 polynomials in  $\mathbb{C}[x, y]$  with no common factor.<sup>2</sup> Then  $V(f) \cap V(g)$  contains at most four points.*

*Proof.* By lemma 3.1, we study  $S = V((f) \cup (g))$  where  $f, g$  are polynomials of degree 2 with no common factor. This will be the same as  $V((f, g))$ ; consider the affine coordinate ring  $\mathbb{C}[x, y]/(f, g)$ . By Lemma 3.3, this is  $(\mathbb{C}[x, y]/(f)) / (g)$ . We know that  $\mathbb{C}[x, y]/(f)$  is isomorphic to either  $\mathbb{C}[x, y]/(xy + 1)$  or  $\mathbb{C}[x, y]/(y^2 + x)$ . Consider first the second case. Note that in this quotient we can replace each instance of  $x$  with one of  $y^2$ , thereby obtaining a polynomial in  $y$ ; because there is a unique way to do this, we obtain unique

<sup>1</sup>This fact is due to the fact that the ideal generated by a set  $A$  is equal to  $RA$ ; see [DF08], page 251.

<sup>2</sup>For more information on why this condition makes sense, look into the theory of Unique Factorization Domains - a broad class of rings, of which  $\mathbb{C}[x, y]$  is an element.

representatives for each element in the quotient. Every polynomial in  $y$  can be obtained this way, yielding a well-defined homomorphism to  $\mathbb{C}[y]$ . We consider the image of  $g$  under the map “substitute  $y^2$  for  $x$ ” - this will be, in general, a degree 4 or lower polynomial (as  $g$  may have an  $x^2$  term, which maps to  $y^4$ ) in one variable over  $\mathbb{C}$ ; as  $\mathbb{C}$  is algebraically closed, this polynomial has at most four roots and splits into at most 4 linear factors. Then these linear factors are the maximal ideals which contain the image of  $(g)$ , and thus correspond bijectively to the maximal ideals in our final quotient  $\mathbb{C}[x, y]/(f, g)$ , and thus to the points in the associated affine variety.

We now consider the second case; we can view the quotient  $\mathbb{C}[x, y]/(xy + 1)$  as  $\mathbb{C}[x, x^{-1}]$  under the map  $y \mapsto -x^{-1}$ . Then we note that  $g$  maps to a polynomial of the form  $P = ax^2 + bx^{-2} + cx + dx^{-1} + e$ . But now that  $x$  is invertible, the ideal generated by this polynomial is the same as the ideal generated by  $x^2P$ ; this is because we can multiply  $x^2P$  by  $x^{-2}$  to get  $P$ , and vice versa, so any ideal which contains one must contain the other. But  $x^2P$  is a quadratic in  $x$ , and thus splits into at most 4 linear factors; a symmetric argument to the first case then shows that there are at most 4 points in the algebraic set associated to the coordinate ring.  $\square$

We can see that in the setting we’ve outlined, the maximum and minimum (zero intersections) are both attained.

**Example 3.5.** The polynomials  $\frac{x^2}{3} + \frac{y^2}{1} - 1$  and  $\frac{x^2}{1} + \frac{y^2}{3} - 1$  intersect in four points.

**Example 3.6.** The polynomials  $yx - 1$  and  $xy - 2$  do not intersect:

$$\begin{aligned} xy - 2 &= xy - 1 \\ 2 &= 1 \end{aligned}$$

*Exercise 3.7.* Find non-degenerate pairs of conics (i.e. Conics which have a nonzero order-two term and are not the product of two linear terms) which intersect exactly one, exactly two, and exactly three times, or prove that no such pair exists.

**Remark 3.8.** This result is somewhat unsatisfying as it doesn’t really tell us how many intersections any given pair of polynomials have. We can remedy this (somewhat) by some constructions which, although beyond the scope of this talk, allow us to “fix” cases like the above so that the answer to our question “how many times do two conics intersect” is a decisive “four”.

#### 4. CONICS MEETING $n$ POINTS AND MODULI SPACES

Now we address the final aspect of our question; namely, how many conics (and which) pass through  $n$  points. This may seem like the least natural question to ask; one could motivate it by saying that we wish to see how much “control” we have over a conic; in essence, how many “degrees of freedom” a conic has, or how many points are necessary to specify a conic. Indeed, we will see that the best way to answer this question is to formalize the question “how does one specify a conic lying in the plane”; the answer to that question (a so-called “moduli space”) also provides the answer to Question 1.12, part 3. We begin with the case  $n = 1$ :

**Theorem 4.1.** *There are infinitely many degree 2 polynomials passing through a point.*

*Proof.* Let  $P$  be a point in the affine plane. We can represent this point as  $P = V((x - a, y - b))$  for  $P = (a, b)$ ; the set of points where the functions  $x - a$  and  $y - b$  both vanish is exactly  $P$  (recall also our correspondence between points and maximal ideals - this ideal

is maximal). We wish to find degree two polynomials in the maximal ideal  $(x - a, y - b)$ ; but all such polynomials are of the form  $f(x - a) + g(y - b)$  where  $f$  and  $g$  are degree  $\leq 1$ , and we have found all (infinitely many) degree two polynomials through the given point.  $\square$

**Definition 4.2.** **Affine  $n$ -space** over the complex (or real) numbers is the set of all  $n$ -tuples  $(x_1, \dots, x_n)$ , for  $x_i$  in the complex (or real) numbers.

**Definition 4.3.** **Projective  $n$ -space** is the set of lines through the origin in affine  $n + 1$  space. We can view this as all points which are a scalar multiple of a nonzero point in affine  $n + 1$  space; as such, define projective space to be the set of sets  $[x_0 : \dots : x_n] = \{(\lambda x_0, \dots, \lambda x_n) | \lambda \in \mathbb{C}\}$  (note the colons, square brackets, and zero indexing).

**Remark 4.4.** The numbering conventions exist for dimensional reasons that we won't touch on in this talk. Effectively, around any point, projective  $n$  space “looks like” affine  $n$  space.

**Definition 4.5** (Loose Definition). A **moduli space** is a “space”<sup>3</sup> in which each point corresponds to a object which you wish to study, and for which nearby points usually correspond to similar objects.

**Example 4.6.** Consider the set of all lines in  $\mathbb{R}^2$ . A (non-vertical) line is given uniquely by the equation

$$y = mx + b$$

meaning that we can parametrize all non-vertical lines by  $\mathbb{R}^2$ , where a point  $(m, b)$  in  $\mathbb{R}^2$  corresponds to the line with the above equation. If we want to consider vertical lines, a line can be given by a line through the origin which is “slid” somewhere else; we have a good representation of the set of all lines through the origin in 2-space, we can consider the space  $\mathbb{RP} \times \mathbb{R}$  - the set of pairs  $(m, b)$  where  $m$  is a point in projective 1-space (aka a set of the form  $[x_1 : x_2]$ ) and  $b$  is the  $y$ -intercept of the line we want. We can't really rigorously discuss the notion of nearby points yielding similar lines, but intuitively, the idea is there - varying  $x_1$ ,  $x_2$ , or  $b$  only slightly gives a line which isn't much different.

**Theorem 4.7.** *The moduli space of complex conics in the plane is  $\mathbb{P}^5$ . Moreover, 5 points determine a conic; more general points will not lie in a single conic, and less will lie in infinitely many.*

*Proof.* Consider a general conic  $P = ax^2 + bxy + cy^2 + dx + ey + f$ . The scaling  $\lambda P$  by any complex number  $\lambda$  yields a polynomial with the same roots, so we identify  $P$  with  $\lambda P$ . Identifying the conic with the tuple of it's coordinates then gives a moduli space; the space of conics is  $\mathbb{P}^5$ . Suppose we require  $P(x_1, y_1) = 0$ . Then

$$ax_1^2 + bx_1y_1 + cy_1^2 + dx_1 + ey_1 + f = 0$$

This defines a hyperplane through the origin in affine 6-space; indeed, each point we require the zero set of  $P$  to contain defines another hyperplane through the origin. Then, if we require the zero set of  $P$  contain all  $n$  distinct points, the coefficients must be in the intersection of  $n$  hyperplanes through the origin. Assuming no two points define the same hyperplane (which is true in general - changing the point slightly means it will define a different hyperplane), some linear algebra gives that the intersection of  $n$  distinct

---

<sup>3</sup>A topological space usually, often with some extra structure - but we won't go into the details of topology.

hyperplanes in affine 6-space is  $6 - n$  dimensional. In particular, if  $n = 5$ , then we are left with a line; when we consider the space of all lines in this space, it is a single point. Thus we have recovered the classical result that 5 points determine a conic. If  $n < 5$ , we have an infinite number of lines in our space; if  $n > 5$ , we have none.  $\square$

**Example 4.8.** Find the conic polynomial which passes through the points  $(0, 0)$ ,  $(0, 1)$ ,  $(1, 2)$ ,  $(-1, 0)$  and  $(0, -1)$ .

*Proof.* Begin with  $(0, 0)$ . This imposes the condition  $f = 0$ . Next we consider the point  $(0, 1)$ . This imposes the condition:

$$c + e + f = 0$$

The point  $(1, 1)$  imposes the condition:

$$a + 2b + 4c + d + 2e + f = 0$$

The point  $(-1, 0)$  imposes the condition:

$$a - d + f = 0$$

The point  $(0, -1)$  imposes the condition:

$$c - e + f = 0$$

Some linear algebra yields:

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 2 & 4 & 1 & 2 & 1 & 0 \\ 1 & -1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & -1 & 1 & 0 \end{bmatrix}$$

Row reducing:

$$\begin{bmatrix} 1 & 0 & 0 & \frac{1}{3} & 0 & 0 & 0 \\ 0 & 1 & 0 & \frac{1}{3} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

We obtain our answer in terms of a free variable,  $d$ . That is, our solution is  $c = e = f = 0$ ,  $3d = a = b$ . Identifying all scalar multiples allows us to assume  $d = 1$ , so we can write our polynomial:

$$P = 3x^2 + 3xy + x$$

This is then the (unique) degree 2 polynomial which is zero at each of these points!  $\square$

*Exercise 4.9.* Check that the above polynomial is indeed zero at each of these points.

*Exercise 4.10.* Pick 5 points and find a polynomial passing through those. Try to pick your points such that the resulting polynomial doesn't factor.

**Remark 4.11.** It's interesting to think about how difficult it is to complete the above exercise. In theory, there is a 100% probability that you'll pick at random such sets of five points which don't define a reducible polynomial (this fact relies on some advanced statistics that's beyond the scope of this lecture, but I still find it interesting). Why, if this is the case, is it so easy to find sets of points for which the polynomial *is* reducible?



## REFERENCES

- [DF08] David S Dummit and Richard M Foote. *Abstract Algebra, 2Nd Ed.* July 2008. ISBN: 9788126517763.
- [Gro74] Alexandre Grothendieck. *Eléments de Géométrie Algébrique.* 1974.
- [Har11] Robin Hartshorne. *Algebraic geometry.* New York ; London: Springer, 2011. ISBN: 9781441928078.

DEPARTMENT OF MATHEMATICS & STATISTICS; BOSTON UNIVERSITY; BOSTON, MASSACHUSETTS 02215  
Email address: `skyler@bu.edu`