Bezout and Group Laws on Cubics

Ray Huang

January 7, 2024

Abstract

In this expository paper, we define and prove the associativity of the group law on cubics via the Caley-Bacharach Theorem. To prove Caley-Bacharach, we introduce and prove Bezout's Theorem and its corollaries on families of conics and cubics through some given points over the complex projective plane. As an application of Caley-Bacharach and the associativity of the group law on cubics, we prove Pascal's Theorem (which implies Pappus and Desargues's theorems).

Contents

1 Introduction

Bezout's Theorem is a multiplication theorem that generalizes the number of common roots between two polynomials in n variables of arbitrary degrees. The theorem was first proposed as a challenge in the seventeenth century when it was still a conjecture. The problem was not fully resolved until two centuries later when the tools of complex projective space and multiplicities were fully developed. Being one of the oldest important results in algebraic geometry, Bezout's Theorem is worth writing a paper for it. In this paper, we will first introduce an algebraic proof of the theorem and will then discuss its applications: how it unveils the group properties of roots of cubics, and how its corollary provides higher-perspective solutions to classical geometry problems.

To provide the necessary tools for exploring this question, we organize this paper as follows. Section 2 is a review of some basic concepts of points at infinity, projective plane, and homogenized coordinates (Subsection 2.1), as well as the definition of intersection and multiplicity (Subsection 2.2). These concepts construct the space the curve lies into and the definition of the "number" of intersection, which is the very first step of understanding later proof.

Section 3 to Section 4 involves the development of argument by proving Bezout's Theorem, Caley-Bacharach as a lemma of Bezout's, and the Group Laws on Cubics as a lemma of Caley-Bacharach consecutively.

Section 5 is the application of the group laws on solving classical geometric problems, mainly dealing with Pascal's Mystic Hexagon, including Pappus and Desargues's theorems.

2 Preliminaries

2.1 Projective plane and homogeneous coordinates

Definition 2.1. Let $n \geq 0$. Define a binary relation $\sim$ on $\mathbb{C}^{n+1}$ by $(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n)$ if and only if there exists $0 \neq \lambda \in \mathbb{C}$ such that $a_i = \lambda b_i$ for all $0 \leq i \leq n+1$. One can check that $\sim$ gives an equivalence relation on $\mathbb{C}^{n+1}$.

Define the **n-dimensional complex projective space** $\mathbb{P}^n_{\mathbb{C}}$ as the quotient $(\mathbb{C}^{n+1} - \{(0, \ldots, 0)\})/\sim$. We denote the equivalence class of every $(a_0, \ldots, a_n) \in \mathbb{C}^{n+1}$ by $[a_0 : \ldots : a_n]$.

Remark 2.1. In general, one cannot "evaluate" polynomials at points of $\mathbb{P}^n_{\mathbb{C}}$. Given a polynomial $F \in \mathbb{C}[x_0, \ldots, x_n]$ and a point $P = [a_0 : \ldots : a_n] \in \mathbb{P}^n_{\mathbb{C}}$, it is tempting to define the value $F(P)$ of F at P as $F(P) = F(a_0, \ldots, a_n)$. However, one can check that unless F is constant, this definition is dependent on the choice of the representative $(a_0, \ldots, a_n)$ of P. In other words, the function $F : \mathbb{C}^{n+1} \to \mathbb{C}$ induces by the polynomial F does not necessarily descend to a function on $\mathbb{P}^n_{\mathbb{C}}$.

However, below we shall see that if F is *homogeneous* (Definition 2.2), we can define what it means for F to "vanish" at a point $P \in \mathbb{P}^n_{\mathbb{C}}$.

Remark 2.2. The point $(0, \ldots, 0)$ will later be denoted as the distinguished point O (Definition 2.6).

Definition 2.2. Let $n \geq 0$. The polynomial ring $\mathbb{C}[x_0, \ldots, x_n]$ has a natural $\mathbb{C}$-vector space structure. For every $d \geq 0$, let $S_d := S^n_d := \operatorname{span}_{\mathbb{C}}\{x_0^{i_0} \cdots x_n^{i_n} \mid$

$i_0 + \cdots + i_n = d\}$ be the subspace of $\mathbb{C}[x_0, \ldots, x_n]$ spanned by the monomials of degree d. By counting the number of such monomials, we have $\dim_{\mathbb{C}} S_d$.

A polynomial $F \in \mathbb{C}[x_0, \ldots, x_n]$ is called **homogeneous** is $F \in S_d$ for some $d \geq 0$. If $0 \neq F \in S_d$, we say that F is **homogeneous of degree** d.

Observation 2.1. Let $F \in \mathbb{C}[x_0, \ldots, x_n]$. It is not hard to show that F is homogeneous of degree d if and only if for every $(a_0, \ldots, a_n) \in \mathbb{C}^{n+1} - \{(0, \ldots, 0)\}$ and every $0 \neq \lambda \in \mathbb{C}$, we must have $F(\lambda a_0, \ldots, \lambda a_n) = \lambda^d F(a_0, \ldots, a_n)$.

In particular, $F(a_0, \ldots, a_n) = 0 \iff F(\lambda a_0, \ldots, \lambda a_n) = 0$ for all $\lambda \in \mathbb{C}^*$. This motivates the following definition.

Definition 2.3. Let $F \in \mathbb{C}[x_0, \ldots, x_n]$ be homogeneous of degree d and $P = [a_0 : \ldots : a_n] \in \mathbb{P}^n_{\mathbb{C}}$. We say that F **vanishes** at P, written $F(P) = 0$ if $F(a_0, \ldots, a_n) = 0$. (This notion is well-defined by the observation above.) If F vanishes at P, we say that P is a **zero** of F (in $\mathbb{P}^n_{\mathbb{C}}$). We denote the set of zeroes of F (in $\mathbb{P}^n_{\mathbb{C}}$) by $\mathbb{V}(F)$.

Given $P_1, \ldots, P_m \in \mathbb{P}^n_{\mathbb{C}}$, let $S_d(P_1, \ldots, P_m) := \{F \in S_d \mid F(P_i) = 0 \ \forall i\}$ be the set of all homogeneous polynomials in $\mathbb{C}[x_0, \ldots, x_n]$ of degree d vanishing at all of the P_i's. Clearly, $S_d(P_1, \ldots, P_m)$ is a $\mathbb{C}$-subspace of S_d.

Definition 2.4. A subset $C \subset \mathbb{P}^2_{\mathbb{C}}$ is called a (complex) **projective plane curve** if $C = \mathbb{V}(F)$ for some homogeneous $0 \neq F \in F[X, Y, Z]$. Such a curve C can also be written as $C(F)$. The **degree** of C is defined as $\deg C := \min\{d \in \mathbb{Z} \mid \exists 0 \neq F \in S_d \text{ such that } C = \mathbb{V}(F)\}$.

From now on, by **curves**, we always mean (complex) **projective plane curves**. In this paper, we will use C and $C(F)$ to denote the curve interchangeably, depending on whether we consider it beneficial to emphasize the curve's relation to the homogeneous polynomial $F \in F[X, Y, Z]$ of degree 2.

Definition 2.5. Let F be some homogeneous polynomial such that $0 \neq F \in \mathbb{C}[X, Y, Z]$ of degree 2, and $C(F) \subset \mathbb{P}^2_{\mathbb{C}}$ be its zero set. Let $f(x, y) \in \mathbb{C}^2$ be a new polynomial obtained by plugging $Z = 1$ into F.The curve C is **singular** if there exists $(x_0, y_0) \in \mathbb{C}^2$ so that $f(x_0, y_0) = 0$ and $\frac{\partial f(x_0, y_0)}{\partial x} = 0$, $\frac{\partial f(x_0, y_0)}{\partial y} = 0$. If C is not singular, it is **nonsingular** (or **smooth**).

Remark 2.3. f is nonconstant and has no repeated factors.

Definition 2.6. A conic (resp. **cubic curve**) is a curve of degree two (resp. three). For our purpose, an **elliptic curve** is a nonsingular conic with a distinguished point $O \in \mathbb{P}^2_{\mathbb{C}}$.

Definition 2.7. **Multiplicity** refers to the power of a factor appearing in the factorization of a polynomial.

3 Bezout's Theorem and its proof

This chapter is devoted to the development of the proof of Bezout's theorem. In the first section, we introduce an articulated version of Bezout's Theorem, and explain the necessary constraints on it. In the second section, we introduce the invention of Sylvester Matrix and the resultant as our main tool. The main result needed is Definition 3.1 and Proposition 3.1. In the last section, we show how to apply Proposition 3.1 to finally prove Bezout's Theorem.

3.1 Bezout's Theorem

Theorem 3.1 (Bezout)**.** *Suppose that polynomials $f(x,y), g(x,y) \in \mathbb{C}[x,y]$ have degrees m and n respectively and that $f \cdot g$ has no repeated factors. Let F and G be the homogenized polynomials $\in \mathbb{P}^2_{\mathbb{C}}$ of f, g in $\mathbb{P}^2_{(}C)$, and denote $C(F)$ and $C(G)$ as their curve. Then $C(F)$ and $C(G)$ intersect in mn points, counted with multiplicity (Definition 2.7).*

Remark 3.1. The theorem holds only if $C(F)$ and $C(G)$ intersect at finitely many points, i.e. F and G share no common factors. f and g themselves contain no repeated factors as well.

3.2 Proof of Bezout's Theorem

In this subsection, we will provide proof of Bezout's Theorem for the intersection of two projective curves of degree m and n. Bezout's Theorem is a collective effort of mathematicians of centries, its motivation, however, is to simply answer this question: given two polynomials not necessarily having the same degree, when do they have a common root?

3.2.1 Sylvester Matrix and resultant

Lemma 3.1. *If $0 \neq f(x) \in \mathbb{C}[x]$ is a degree n polynomial and $0 \neq g(x) \in \mathbb{C}[x]$ is a degree m polynomial, they have a common root if and only if there exist polynomials $0 \neq r(x) \in \mathbb{C}[x]$ of degree $\leq (m-1)$ and $0 \neq s(x)$ of degree $\leq (n-1)$ such that*

$$r(x)f(x) + s(x)g(x) = 0$$

Proof. Suppose that f and g have a common root $(x-a)$. We can set

$$r(x) = g(x)/(x-a)$$

$$s(x) = -f(x)/(x-a)$$

Then the Lemma is proven for one direction. Now suppose there exist polynomials $r(x)$ of degree $\leq (m-1)$ and $s(x)$ of degree at most $(n-1)$ such that $r(x)f(x) = -s(x)g(x)$. It follows that the degree of new polynomials $r(x)f(x)$ and $-s(x)g(x)$ can be denoted as $t \leq (n+m-1)$ and they have the same t factors $x-a_1, \ldots, x-a_t$. This set of factors of size t includes the n factors of $f(x)$ and the m factors of $g(x)$. The pigeonhole principle implies that at least one of these factors must be common to $f(x)$ and $g(x)$. Thus the proof is done.

Based on Lemma 3.1, a new technique should be proposed. The new technique is to construct a matrix whose entries are coefficients in $f(x)$. This $n \times m$

matrix M_1 sends the vector whose entries are coefficients in $r(x)$ to the coefficients of $r(x)f(x)$. Similarly, there exists $m \times n$ matrix M_2 whose entries are coefficients in $g(x)$ and which send coefficients to $s(x)$ to the coefficients of $s(x)g(x)$. If we combine M_1 and M_2 together, we get an $(m+n) \times (m+n)$ matrix

$$S = \begin{bmatrix} M_1 \\ M_2 \end{bmatrix}$$

with the property that $\begin{bmatrix} u & v \end{bmatrix}$ S = $\begin{bmatrix} c+d \end{bmatrix}$, where u = $\begin{bmatrix} u_{m-1} & \cdots & u_0 \end{bmatrix}$ and v = $\begin{bmatrix} u_{n-1} & \cdots & u_0 \end{bmatrix}$. Thus, S reduces the common root problem between two polynomials to linear algebra: the equation $\begin{bmatrix} u & v \end{bmatrix} S = 0$ has nontrivial solution when $det(S) = 0$.

Definition 3.1. If

$$f(x) = a_m x^m + \cdots + a_0$$

$$g(x) = b_n x^n + \cdots + b_0$$

are two polynomials, their **Sylverster matrix** is the $((m+n)) \times (m+n)$ matrix

$$S(f,g,x) = \begin{bmatrix} a_m & a_{m-1} & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_m & a_{m-1} & \cdots & a_1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_m & a_{m-1} & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & b_0 & 0 & \cdots & 0 \\ 0 & b_n & b_{n-1} & \cdots & b_1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & b_n & b_{n-1} & \cdots & b_0 \end{bmatrix}$$

and its determinant $det(S(f,g,x)) = Res(f,g,x)$ is called the **resultant** of f and g.

Proposition 3.1. *The polynomials $f(x) \in \mathbb{C}[x]$ and $g(x) \in \mathbb{C}[x]$ have a common root if and only if their resultant $Res(f,g,x) = 0$.*

Proof. The above equations are satisfied only when $Res(f,g,x) = 0$.

3.2.2 Application to Bezout's Theorem

We now will apply Proposition 3.1 to prove Bezout's Theorem. In this subsection, all $F(X,Y,Z), G(X,Y,Z) \in \mathbb{C}[X,Y,Z]$ are homogeneous polynomials of degree m and n respectively, and their curves $C(F)$ and $C(G)$ are elliptic curves in $P^2_{\mathbb{C}}$.

Lemma 3.2. *Any homogeneous equation of degree $d \in \mathbb{C}$ can be factored into d linear factors in $P^2_{\mathbb{C}}$.*

Theorem 3.2. *Suppose $F[X,Y,Z]$ and $G[X,Y,Z]$ are polynomials of degree m and n respectively. Then $Res(F,G,z)$is a homogeneous equation of degree mn.*

Proof. If R(x,y) is the resultant, we can prove that $R(tx,ty) = t^{mn}R(x,y)$ for all $t \in \mathbb{C}$, which proves the theorem.

Corollary 3.1. *The* resultant *(Definition 3.1) of the polynomials F and G factors into mn linear factors.*

$$Res(F,G,z) = \prod(a_i x - b_i y)$$

Proof. This follows directly from Lemma 3.2 and Theorem 3.2.

Thus, we complete the proof for Bezout's theorem.

4 Caley-Bacharach and Group Laws on Cubics

This chapter is devoted to the proof of Caley-Bacharach and group laws on cubics in complex projective plane. This is the transitioning part in this paper: it first proves Caley-Bacharach as a Lemma of Bezout's Theorem in subsection 4.1, and then it presents an important result achieved by Caley-Bacharach: proof of group laws on elliptic curves in projective plane in subsection 4.2, which equivalently meaning the group laws on the common solutions to systems of two polynomials of the same variables. In this section, in all corollaries, $P_i \in \mathbb{P}^2_{\mathbb{C}}$ for all i, and the precise definition of S_d can be checked at Definition 2.2.

4.1 Proof of Caley-Bacharach

Corollary 4.1.

$$dimS_d(P_1,...,P_n) \geq dimS_d - n$$

A Sketch of the Proof. For any F $\in S_d$, we can rewrite its systems of linear equations given the n points as follows: (Matrix in which each row represents a unique variable part of a monomial of F with (X: Y: Z) plugged in)*(a column vector v)=0. Therefore, {v}=ker(S_d), and dim(ker(S_d))=d. The rank of the first matrix should be at most m because there are only m points. Therefore,

$$dimSd(P_1,...,P_n) \geq dimS_d - n$$

.

Proposition 4.1. *If no four of $P_1,...,P_5$ are collinear, then*

$$dim_{\mathbb{C}}S_2(P_1,...,P_5) = 1$$

, and there exists a unique conic passing through $P_1,...,P_5$.

Proof. Suppose for contradiction that

$$dim_{\mathbb{C}}S_2(P_1,...,P_5)) \geq 2$$

by Corollary 4.1. Then there must exist at least two distinct conics C_1 and C_2 that go through $P_1,...,P_5$. By Bezout's Theorem, if $C_1 \cap C_2$ does not exist, then the number of intersection points $= dim(C_1)dim(C_2) \leq 4(= 4$ when none of C_1, C_2 are degenerate), contradicting the fact that C_1 and C_2 share at least five points of intersection. Therefore, the curves C_1 and C_2 must overlap somewhere, which is only possible when C_1 and C_2 are both a pair of lines and they share a common line. Denote P_1, P_2, P_3 as the intersection of C_1 and C_2, C_2 and C_3, C_3 and C_1 respectively. Since C_1 and C_2 intersect at five points, the other two points of intersections should lie on C_1, contradicting the hypothesis that no four of $P_1,...,P_5$ are collinear. Therefore, we have proven that

$$dim_{\mathbb{C}}S_2(P_1,...,P_5) = 1$$

.

Since then, there exists some $F \in S_2$ so that $F(P_i) = 0$ for all i, and that for every $G \in S_2$, $G = aF$ for some a $\in \mathbf{C}$. Since in P^2 $C(F = 0)$ and $C(aF = 0)$ is the same conic, we conclude that every five points determine a unique conic.

Proposition 4.2. *If no four of $P_1,...,P_8$ are collinear, no seven of $P_1,...,P_8$ are conconic, then*

$$dim_{\mathbb{C}}S_2(P_1,...,P_8) = 2$$

, and there exists a unique conic passing through $P_1,...,P_9$.

Proof. We know from the Corollary that

$$dim_{\mathbb{C}}S_2(P_1,...,P_8) \geq 2$$

. Case 1: When three of the points are collinear

Suppose P_1, P_2, P_3 all lie on a unique line L. Choose another point Q on L. Then we have

$$dim_{\mathbb{C}}S_2(P_1,...,P_8) \geq dim_{\mathbb{C}}S_2(P_1,...,P_8,Q) - 1$$

by Corollary 4.1. Let E be the elliptic curve that contains $P_1,...,P_8, andQ$. By Bezout's Theorem, if E does not contain L, then the number of intersections between E and L should be three instead of nine. Therefore, $E = L \cup C$ for some conic C which contains $P_4,...,P_8$. By the last proposition, such conic C should be unique. Therefore, the conic E is unique, equivalently meaning that

$$dim_{\mathbb{C}}S_3(P_1,...,P_8,Q) = 1$$

, and

$$dim_{\mathbb{C}}S_3(P_1,...,P_8) \leq 2$$

. We know from the Corollary 4.1 that

$$dim_{\mathbb{C}}S_3(P_1,...,P_8) \geq 2$$

, so we conclude that

$$dim_{\mathbb{C}}S_3(P_1,...,P_8) = 2$$

.

Case 2: When six of the points are conconic

Suppose $P_1,...,P_6$ lie on the conic C. Take another point Q on E. Similarly, after using Bezout's Theorem to prove that F contains E, we reach the conclusion

$$dim_{\mathbb{C}}S_3(P_1,...,P_8,Q) = 1$$

and thus

$$dim_{\mathbb{C}}S_3(P_1,...,P_8) = 2$$

.

Case 3: the general case where no three points collinear and no six points conconic By Corollary 4.1 we know that

$$dim_{\mathbb{C}}S_3(P_1,...,P_8) \geq dim_{\mathbb{C}}S_3(P_1,...,P_8,A,B) - 2$$

, for any other two points A, B on the line L joining P_1, P_2. We want to show that $dim_{\mathbb{C}}S_3(P_1,...,P_8) = 2$ by contradiction. Suppose for contradiction that $dim_{\mathbb{C}}S_3(P_1,...,P_8) \geq 3$. Thus,

$$dim_{\mathbb{C}}S_3(P_1,...,P_8) \geq 1$$

, which means that there exists a cubic E passing through the ten points $P_1,...,P_8, A$, and B. By Bzout's Theorem, E is the union of the line L and the conic C joining $P_3,...,P_8$. Since no three points among $P_1,...,P_8$ are collinear, $P_3,...,andP_8$ lie on the conic part, contradicting the hypothesis that no six of the points are conconic. Thus, it is only possible that $dim_{\mathbb{C}}S_3(P_1,...,P_8) = 2$ by Corollary.

Theorem 4.1 (Caley-Bacharach). *Let $E_1, E_2 \in P^2_{\mathbb{C}}$ be the projective (cubic) curves of two distinct polynomials F_1, $F_2 \in S_3P_1,...,P_8,P_9$, and $E_1 \cap E_2 = P_1, P_2,...,P_9$. Then any cubic $E \in P^2_{\mathbb{C}}$ passing through $P_1, P_2,...,P_8$ also passes through P_9.*

Proof. If four of the points $P_1,...,P_4$ were on a line L, then each of E_1 and E_2 would meet L in ≥ 4 points, and thus contain L, which contradicts the assumption on $E_1 \cap E_2$. For the same reason, no seven of the points can be conconic. Therefore, the assumptions of the two Propositions are satisfied, so we can conclude that

$$dim_{\mathbb{C}}S_3(P_1,...,P_8) = 2$$

which means that there exist two distinct cubic polynomials $F_1, F_2 \in S_3(P_1,...,P_8)$ that form a basis of $S_3(P_1,...,P_8)$. Hence, $S_3(P_1,...,P_8) = \{aF_1+bF_2 \mid a,b \in \mathbb{C}\}$.

Then, for every cubic E passing through $P_1, ..., P_8$, we have some a, b such that $F3(X : Y : Z) = aF_1(X : Y : Z) + bF_2(X : Y : Z) = 0$. Since E_1 and E_2 both contain P_9 by Bezout's Theorem, E should also pass through P_9 as $F_3(P9) = 0$. Thus, any cubic curve E passing through $P_1, ..., P_8$ must pass through P_9 as well.

4.2 Group laws among points on elliptic curves

Elliptic curves are nonsingular curve that is not empty set in $P^2_{\mathbb{C}}$. Nonsingularity can be briefly understood as having a well-defined tangent line at every point. As a result, an elliptic curve contains no line, or else the tangent line is undefined for the part of a line. The aim of this section is to show that the elliptic curve under our construction of addition is a commutative group. In this section, we will show one particular geometric structure on the elliptic curve that grants group laws on it. The aim of this section is to show that the elliptic curve under our construction of addition is a commutative group. Just as a reminder, a group with a binary operation or addition should satisfy commutativity, associativity, the existence of an identity, and the existence of an inverse.

4.2.1 Construction of Addition

We first use the identity O to define the addition. In the construction of the addition, it does not matter where O is. Let P and Q be two distinct points. There exists a unique line L connecting P and Q. By Bezout's Theorem, L would intersect E at one more point. We denote this point as $P \cdot Q$. When P and Q are the same, the line is tangential to E at P but still intersects E at one more point. After finding $P \cdot Q$, we connect O and $P \cdot Q$ and denote the unique line as L'. The third point of intersection between L' and E is defined to be the result of point addition, $P + Q$.

Through such a construction, commutativity is naturally satisfied because the line passing through two points is unique. It is also not hard to find an inverse for each P. Take the tangent line of E at O, and name its third intersection with O as $P \cdot P^{-1}$. Then, joining P and K, at the third intersection, we obtain an inverse of P, denoted as P^{-1}. We only have one property to prove: the associativity among the points on the elliptic curve.

4.2.2 Proof of Associativity

We want to show that $(A + B) + C = A + (B + C)$ on E. In order to show that $(A + B) + C = A + (B + C)$, it suffices to show that $A \cdot (B + C) = (A + B) \cdot C$. Let L_1 be a line on which $A, B, A \cdot B$ lie, L_2 for $(A + B)$ and $(A + B) \cdot C$, L_3 for $B \cdot C, O, and (B + C)$, L_4 for $A, (B + C), and A \cdot (B + C)$, L_5 for $B, C, and B \cdot C$, L_6 for $A \cdot B, O, and (A + B)$. Write $E_1 = L_1 \cup L_2 \cup L_3$, $E_2 = L_4 \cup L_5 \cup L_6$. E_1 passes through eight points $A, B, A \cdot B, O, (A + B), C, B \cdot C, (B + C)$, thus it passes through a ninth point of intersection with E as well, which in this case can only be $A \cdot (B + C)$ by Caley-Bacharach Theorem since no three points are collinear and no six points are conconic. Similarly, E_2 also passes the same right points with $(A+B)\cdot C$. Again, by Caley-Bacharach Theorem, $(A+B)\cdot C = A\cdot(B+C)$, and thus $(A+B)+C = A+(B+C)$.

5 Application of Caley-Bacharach: Pascal's Mystic Hexagon

This chapter is devoted to the discussion of application of Caley-Bacharach in providing higher-perspective solution to classical geometric problem: Pascal's Mystic hexagon. Even though these results are proven in complex projective plane $P^2_{\mathbb{C}}$, they can still be used to solve classical geometric problems as geometric properties of curves are preserved. Thus, we would not specify which plane we are talking about in this chapter. There are in total three theorems poroven in this chapter: Pascal's Theorem, Pappus's Theorem, and Desargue's Theorem. We will first prove Pascal's Theorem, and then show that Pappus's Theorem is a subcase of Pascal's Theorem, and Descargue's Theorem a subcase of Pappu's Theorem.

Theorem 5.1 (Pascal's Theorem)**.** *Suppose A, B, C, A', B', C' six points lie on the same conic. Let P, Q, R be points of intersection between lines joining two of the six points. Then P, Q, R have to be collinear.*

Proof. Denote the conic as C. Connect the points in accordance with the graph. Let $E_1(F_1 = 0) = AB \cup BD \cup ER$, and $F_1 \in S_3(A, B, C, D, E, R)$. Let $E_2(F_2 = 0) = AB \cup ED \cup CB$, and $F_2 \in S_3(A, B, C, D, E, R)$. $E_1 \cap E_2 = \{A, B, C, D, E, F, R\}$. Let $E_3(F_3 = 0) = C \cup HI$ so that $F_3 \in S_3(A, ..., R)$. Then, by Caley Bacharach, $G \in E_3$, so either $G \in C$ or $G \in HI$. It is impossible that G $\in$ C because we have shown that no seven of the nine points can be conconic in the proof of Caley-Bacharach Theorem. Thus, $G \in HI$, which means G, H, I are collinear.

When the conic C degenerate into a pair of line, we get a special case of Pascal's Theorem: Pappus's Theorem. The nice thing about projective geometry and Caley-Bacharach is that they unveil the underlying connections between classical geometric results by changing perspective.

Pappus Theorem: Let L, L' be two distinct lines, let A, B, C be distinct points on L that do not lie on L', and let A', B', C' be distinct points on L' that do not lie on L. Suppose that $H = AB' \cap A'B, Q = AC' \cap A'C$, and $P = BC' \cap B'C$. Then R, Q, P are collinear.

Proof. Write $C(F = 0) = L \cup L'$, and $F \in S_2(A, B, C, A', B', C')$. Then we complete the proof by Pascal's Theorem.

Desargue's Theorem If the three straight lines joining the corresponding vertices of two triangles ABC and $A'B'C'$ all meet in a point then the three intersections of pairs of corresponding sides lie on a straight line (the perspective). Equivalently, if two triangles are perspective from a point, they are perspective from a line. Being a perspective from a line means that the intersections of lines are collinear.

Proof. This can be proven by the Pappus Theorem by connecting the points in the graph in a different way.

References

Have difficulty making in-text citation. Block, Adam. Introduction to Elliptic Curves. UMS talk, 2017. Smith, Justin. Introduction to Algebraic Geometry. Five Dimensions Press. Tao, Terence. "Pappus's theorem and elliptic curves", https://terrytao.wordpress.com/2011/07/15/pappuss-theorem-and-elliptic-curves/