

The purpose of these notes is to prove a special case of the Cayley-Bacharach Theorem and then to prove Pascal's Theorem as an application. The main result we prove, the Grid Theorem, will be useful when we analyze the group structure of an elliptic curve.

## 1 A Preliminary Result about Conics

Let  $\mathbf{F}$  be a field. Say that 4 points in  $P^2(\mathbf{F})$  are *in general position* if no 3 of those points are collinear. Recall that a *conic* in  $P^2(\mathbf{F})$  is the solution to a homogeneous polynomial of degree 2.

**Lemma 1.1** *Let  $A_1, A_2, A_3, A_4$  be 4 general position points and let  $B$  be some 5th point. There exists a conic that contains  $A_j$  for all  $j$  but not  $B$ .*

**Proof:** Let  $L_1$  be the line containing  $A_1$  and  $A_2$  and let  $L_2$  be the line containing  $A_3$  and  $A_4$ . Suppose first that  $B$  lies on neither  $L_1$  nor  $L_2$ . There is a homogeneous degree 1 polynomial  $\lambda_j$  such that  $L_j$  is the projective curve corresponding to  $\lambda_j$ . That is,  $L_j = V_{\lambda_j}$ . Let  $\lambda = \lambda_1 \lambda_2$ . This is a homogeneous degree 2 polynomial that vanishes exactly on  $L_1 \cup L_2$ , and hence not on  $B$ .

Suppose that  $B \in L_1$ . This time we let  $L'_1$  be the line containing  $A_1$  and  $A_3$  and  $L'_2$  be the line containing  $A_2$  and  $A_4$ . Suppose  $B \in L'_1$ . Then  $L'_1$  contains both  $A_2$  and  $B$ . But  $L_1$  contains both  $A_2$  and  $B$ . Hence  $L_1 = L'_1$ . Hence  $A_1, A_2, A_3$  are collinear. This contradiction shows that  $B \notin L'_1$ . A similar argument shows that  $B \notin L'_2$ . Now we can repeat the original argument, using  $L'_1$  and  $L'_2$  in place of  $L_1$  and  $L_2$ . ♠

## 2 The Grid Theorem

A *grid* is defined to be a collection of 9 points  $\{A_{ij}\}$  with  $i = 1, 2, 3$  and  $j = 1, 2, 3$  which are contained on 3 lines in two different ways. That is  $A_{k1}, A_{k2}, A_{k3}$  are collinear for each  $k = 1, 2, 3$  and  $A_{1k}, A_{2k}, A_{3k}$  are collinear for  $k = 1, 2, 3$ . To simplify the argument assume that no 4 of the points are collinear.

**Theorem 2.1** *Suppose that a homogeneous curve of degree at most 3 contains 8 points of a grid. Then it also contains the 9th point.*

Here is an equivalent formulation. Say that a *vector grid* is a collection of 9 vectors in  $\mathbf{F}^3$  representing the points of a grid in  $P^2(\mathbf{F})$ .

**Theorem 2.2** *A homogeneous polynomial of degree at most 3 that vanishes on 8 vectors of a vector grid also vanishes on the 9th vector.*

We'll change our notation so that the 9 points are  $v_1, \dots, v_9$ . Let  $V$  denote the set of homogeneous curves of degree 3. As a vector space  $V$  is isomorphic to  $\mathbf{F}^{10}$ . To see this, note that an element of  $V$  is specified by choosing constants  $a_1, \dots, a_{10} \in \mathbf{F}$ , which give rise to the polynomial

$$a_1X^3 + a_3Y^3 + \dots + a_{10}XYZ.$$

Given any nonzero vector  $v \in \mathbf{F}^3$ , let  $S_v \subset V$  denote those homogeneous polynomials that vanish on  $v$ . Note that  $S_v$  is a linear subspace of  $V$ .

**Lemma 2.3** *Let  $v_1, \dots, v_8$  be 8 vectors of the grid. Let  $S_j = S_{v_j}$ . Then the intersection  $S_1 \cap \dots \cap S_8$  is 2 dimensional.*

**Proof:** To each subspace  $S_j$  we have a vector  $V_j$  such that  $S_j$  is the solution of the equation  $(a_1, \dots, a_{10}) \cdot V_j = 0$ . There is a map  $\phi : \mathbf{F}^{10} \rightarrow \mathbf{F}^8$  defined by

$$\phi(v) = (v \cdot V_1, \dots, v \cdot V_8).$$

If the vectors  $V_1, \dots, V_8$  are linearly independent, then the matrix whose rows are the  $V$  has rank 8. But then so does the transpose matrix. This is to say that the image of  $\phi$  is  $\mathbf{F}^8$ . But then the kernel of  $\phi$  has dimension 2. In short, Lemma 2.3 is equivalent to the statement that the vectors  $V_1, \dots, V_8$  are linearly independent.

We will suppose this is not the case, and derive a contradiction. If our vectors  $V_1, \dots, V_8$  are not independent, then (after relabelling) we can write  $V_8$  as a linear combination of  $V_1, \dots, V_7$ . This is the same thing as saying that  $S_1 \cap \dots \cap S_7 \subset S_8$ . In other words, any homogeneous polynomial of degree at most 3 that vanishes on  $v_1, \dots, v_7$  also vanishes on  $v_8$ . We will get a contradiction by producing a homogeneous polynomial of degree 3 that vanishes on  $v_1, \dots, v_7$  but not on  $v_8$ .

Here is the key observation. A case by case analysis shows that we can divide up the points  $[v_1], \dots, [v_7]$  so that (after relabelling if necessary)

- $[v_1], [v_2], [v_3]$  all lie on the line  $L$ . Here  $L$  is one of the 6 special lines defining the grid. Note that  $[v_8]$  does not lie on  $L$ .
- $[v_4], [v_5], [v_6], [v_7]$  are in general position: No 3 are collinear.

By the preliminary result, we can then find a conic  $M$  that contains these 4 points but does not contain the point  $[v_8]$ . (Really,  $M$  is just the union of 2 lines.) The line  $L$  is the projective curve associated to a homogeneous polynomial  $\lambda$  of degree 1. The set  $M$  is the projective curve associated to a homogeneous polynomial of degree 2. The homogeneous cubic  $\lambda\mu$  vanishes on  $[v_1], \dots, [v_7]$  but not on  $[v_8]$ . ♠

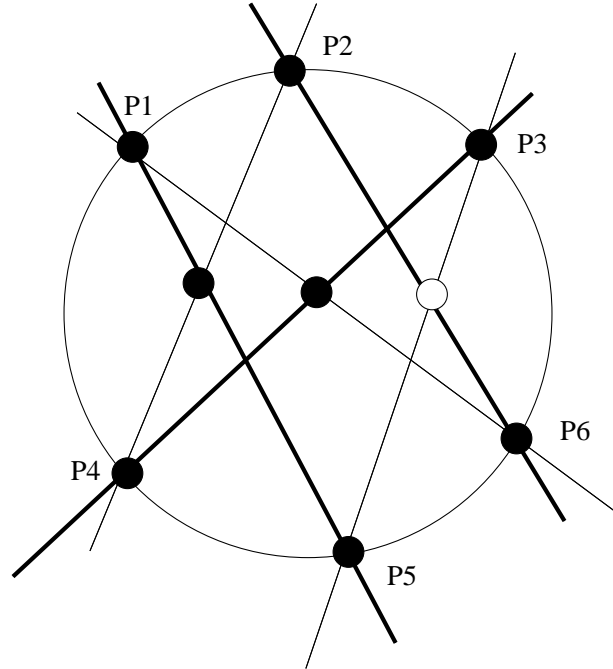
Each line  $A_i$  is the projective curve corresponding to a degree 1 homogeneous polynomial  $\alpha_i$ . Likewise, each line  $B_i$  is the projective curve corresponding to a degree 1 homogeneous polynomial  $\beta_i$ . Let  $\alpha = \alpha_1\alpha_2\alpha_3$  and  $\beta = \beta_1\beta_2\beta_3$ . Note that  $\alpha$  and  $\beta$  are both homogeneous cubics which vanish on all 9 grid vectors. Note also that  $\alpha$  and  $\beta$  are linearly independent (as elements of  $V$ ) because  $\alpha$  vanishes on  $A_1 \cup A_2 \cup A_3$  and  $\beta$  vanishes on  $B_1 \cup B_2 \cup B_3$ .

Here is the punchline: The set of polynomials of the form

$$\Sigma = \{a\alpha + b\beta; \quad a, b \in \mathbf{F}\} \tag{1}$$

is a 2 dimensional set that vanishes on  $v_1, \dots, v_8$ . Hence  $S_1 \cap \dots \cap S_8 = \Sigma$ . But, every element of  $\Sigma$  vanishes on the 9th vector as well. Hence, every element of  $S_1 \cap \dots \cap S_8$  also vanishes on the 9th vector.

### 3 Pascal's Theorem



**Figure 1:** Pascal's Theorem

Pascal's Theorem refers to the configuration in Figure 1. The 6 points  $P_1, \dots, P_6$  lie on a conic  $M$ , and the theorem is that the points  $X_1, X_2, X_3$  lie on a line. Let  $L$  be the line containing  $X_1$  and  $X_2$ . We want to see that  $X_3 \in L$ . The line  $L$  is the projective curve associated to a homogeneous degree 1 polynomial  $\lambda$ . Likewise, the conic  $M$  is the projective curve associated to a homogeneous degree 2 polynomial  $\mu$ . The polynomial  $P = \lambda\mu$  vanishes on  $L \cup M$ . Hence  $P$  vanishes on  $P_1, \dots, P_6, X_1, X_2$ .

The points  $P_1, \dots, P_6, X_1, X_2, X_3$  make a grid. Hence, by the Grid Theorem,  $P$  vanishes on  $X_3$ . But  $P$  vanishes exactly on  $L \cup M$ . Hence  $X_3 \in L \cup M$ . But a line intersects a conic at most twice, by Bezout's Theorem – or just by a direct exercise. Hence  $X_3 \in L$ . This completes the proof.