**MA434 Scribe Notes**
February 26, 2020
Annie Holden

# 1 Linear Systems ("A Conclusion of the Last Episode")

This is the end of Joshua's presentation.

**Proposition 2.6:** Let $k$ be an infinite field, and $P_1, ..., P_8 \in \mathbb{P}^2_k$ distinct points; suppose that no 4 of $P_1, ..., P_8$ are collinear, and no 7 of them lie on a nondegenerate conic. Then

$$\dim S_3(P_1, ..., P_8) = 2.$$

**Proof:** Applying what we discussed last time (see Jack's scribe notes), we proved:

$$\dim S_3(P_1, ..., P_8) \leq 2.$$

$$\dim S_3(P_1, ..., P_8) \geq \binom{3+2}{2} - 8 = 2.$$

$$\dim S_3(P_1, ..., P_8) = 2. \square$$

This gives us the following corollary (which will be useful later when proving that our group is associative!).

**Corollary 2.7:** Let $C_1, C_2$ be cubics that intersect at 9 distinct points $C_1 \cap C_2 = \{P_1, ..., P_9\}$. Then any cubic $D$ through $P_1, ..., P_8$ passes through $P_9$.

**Proof:** If 4 of $P_1, ..., P_8$ were collinear, then $C_1$ and $C_2$ would share a line. Similarly, if 7 of $P_1, ..., P_8$ were conconic, then $C_1$ and $C_2$ would share a conic. But if $C_1, C_2$ shared a line or conic then $C_1 \cap C_2$ would contain infinitely many points which contradicts our assumption. It follows that no 4 of $P_1, ..., P_8$ are collinear and no 7 of $P_1, ..., P_8$ are conconic so the conditions for **Proposition 2.6** are met and so:

$$\dim S_3(P_1, ..., P_8) = 2$$

It follows that $F_1, F_2$ (the equations of $C_1$, $C_2$) form a basis of $S_3(P_1, ..., P_8)$. Note that, since these are two distinct conics (they are not scalar multiples of each other), they are linearly independent. So given some conic $D : (G = 0)$, $G = aF_1 + F_2$. Since $F_1, F_2 = 0$ at $P_9$, $G = 0$ at $P_9$ and $D$ passes through $P_9$. $\square$

In simple terms, this says that if you fix 8 points then any cubic will go through a distinct $9^{th}$ point. This means there is a linear dependence relation between equations.

---

This is where Nathaniel and Jack start presenting on sections 2.8-2.10 in Reid.

## 2 Group Law on Plane Cubics

**Goal:** to define the group structure of points on a plane cubic. First, we need to establish conditions.

Let $k$ be a subfield of $\mathbb{C}$ and $F \in k[X, Y, Z]$ a cubic form $\mathcal{C} : F = 0 \subset \mathbb{P}^2_k$. Assume $F$ satisfies the following conditions:

- $F$ is irreducible. ($F$ does not contain a line or conic.)
- For any $P \in \mathcal{C}$, there exists a unique line in $\mathbb{P}^2_k$ for which $P$ is a repeated zero of $F|L$. (Think of $L$ as a tangent line since we think of tangents as double intersections. For any point, there is one line that has two or three repeated zeros.)

We will define the **group operation:**
(1) Fix any point $O \in \mathcal{C}$ (this will be the zero element).
(2) For any $A \in \mathcal{C}$, $\bar{A}$ is the third intersection of $AO$ on $\mathcal{C}$.

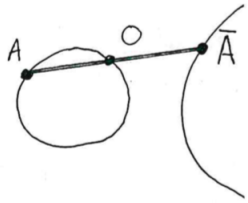


Figure 1: Finding $\bar{A}$

(3) Call $A + B = \bar{R}$ where $R$ is the third intersection of $AB$ with $\mathcal{C}$.

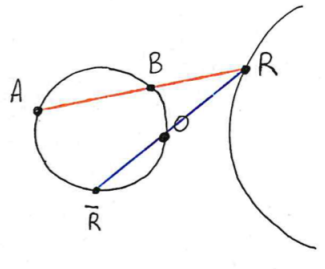


Figure 2: $A + B = \bar{R}$

Simply, follow these steps to find $A + B$: draw $AB$, find the third intersection $R$, draw $RO$, then find the third intersection $\bar{R} = A + B$.

Note that when $A = B$, $AB$ is the tangent line at $A$.

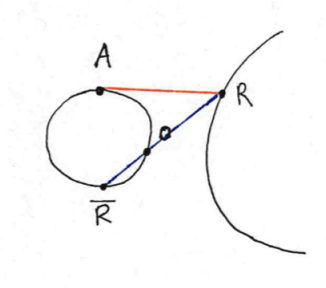


Figure 3: Finding $A + A = \bar{R}$

We are ready to present the theorem:

**Theorem:** Under the operation we constructed, the points of $\mathcal{C}$ form an Abelian group with $O$ being the zero element.

**Proof:** We will show all the conditions are satisfied.

**I. Well Defined** Let $P, Q \in \mathcal{C}$ be given. we show the group operation is well defined. We have two cases.
Case: $P \neq Q$. There exists a unique line $PQ$ with a unique third intersection with $\mathcal{C}$. Note that it is possible for $P$ or $Q$ to be this third intersection.

Case: $P = Q$. There exists a unique tangent line to $Q$ which contains a third unique intersection with $\mathcal{C}$.

In both of these cases, we rely on the fact that conics have three zeros (with multiplicity) so any line intersecting the conic will intersect it a third time, accounting for double and triple intersections. Since any line $PQ$ has a third intersection on the curve, we can find third elements $R$ (on $PQ$) and $\bar{R}$ (on $OR$) such that $P + Q = \bar{R}$. In all cases, the group operation is well defined.

**II. Zero Element** We will show that, given any $A$, $A + O = A$. ($O + A = O$ is obvious upon demonstration of commutativity.)

By definition, $A, O, \bar{A}$ are collinear. Figure 1 makes this clear. $\bar{A}$ is the third point in the intersection of $AO$ (recalling Figure 2, think $\bar{A} = R$.) Next we look at the line $\bar{A}O$ whose third point in the intersection is $A$. Thus $A + O = A$.

It's also good to check that $0 + 0 = 0$. Consider the tangent line at $O$ (which has multiplicity 2) and call $R$ the third point in the intersection with $\mathcal{C}$. Trace the line $OR$ back to $O$ to find that $O$ is the third intersection (again, with multiplicity 2). $O + O = O$.

**III. Additive Inverses** Given $A \in \mathcal{C}$, we will show there exists $B \in \mathcal{C}$ such that $A + B = O$.
(i) Find $\bar{O}$
(ii) Connect $A$ to $\bar{O}$
(iii) Label $B$ the third intersection of the curve and $A\bar{O}$

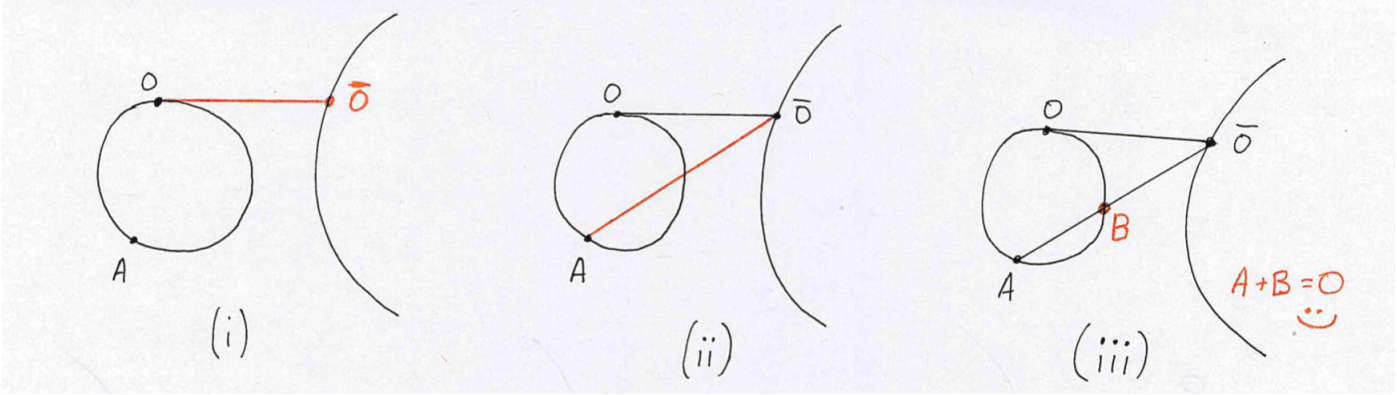


Figure 4: Finding $B$ such that $A + B = O$

Note that if $O$ is an inflection point, the tangent line at $O$ is a triple root and $O = \bar{O}$.

**IV. Commutativity** Noting that $AB = BA$, commutativity follows. nice.

**V. Associativity** This one is hard. To make things easier, we first prove the case in which $A, B, C \in \mathcal{C}$ are distinct points.

We separately consider $(A+B)+C$ and $A+(B+C)$ in order to ultimately demonstrate that they must be the same. First, we consider $(A + B) + C$. Since we are performing the operation twice (first $A + B = \bar{R}$, then $\bar{R} + C = \bar{S}$), we now have four lines to consider:

$L_1 : ABR$ (orange)
$L_2 : RO\bar{R}$ (blue)
$L_3 : C\bar{R}S$ (green)
$L_4 : SO\bar{S}$ (purple)

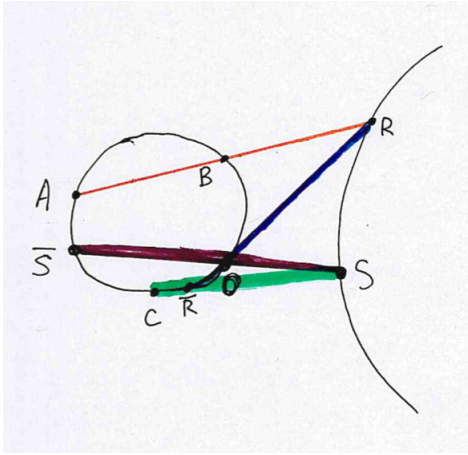


Figure 5: Drawing Four Lines to Find $(A + B) + C = \bar{S}$

Next, we follow the same process to consider $A + (B + C) = \bar{T}$. Note that, since we already proved commutativity, we can equivalently look at $(B + C) + A = \bar{T}$. We draw four more lines:

$M_1 : BCQ$
$M_2 : QO\bar{Q}$
$M_3 : Q\bar{T}S$
$M_4 : TO\bar{T}$

We aim to show that $\bar{S} = \bar{T}$. It is sufficient to show that $S = T$ because $O$ is fixed and the last step only requires connecting $S, T$ to $O$. This means we don't need to worry about lines $L_4, M_4$.

Now we construct two cubics, $D_1$ and $D_2$. Let $D_1 := L_1 \cup M_2 \cup L_3$ and $D_2 := M_1 \cup L_2 \cup M_3$. (These are cubics because we are multiplying three equations of lines together. The effect on the picture is that we union these lines together. Reid uses the notation + to denote this.) By smart construction of our unions, we now have:

$$C \cap D_1 = \{A, B, C, O, R, \bar{R}, Q, \bar{Q}, S\}$$

$$C \cap D_2 = \{A, B, C, O, R, \bar{R}, Q, \bar{Q}, T\}$$

These sets only differ in the last two elements $S$ and $T$. Recall that we assumed all of these points are distinct. So, by **Corollary 2.7**, any 2 conics that intersect at 8 points must intersect at the same $9^{th}$ point (and cubics can intersect at at most 9 points). Thus $S = T$ and associativity holds.

Note that, in this proof, it was crucial that all points were distinct. This is very hard to prove without this assumption so Reid uses continuity to"nudge things until it all works" in his proof.

**Proof by Continuity:** We handwaved this a lot but here is a list of some of the main points:

- $k$ is a subfield of $\mathbb{C}$ so if we prove that associativity holds for all points in $\mathbb{C}$, we prove that it holds for all points in $k$.
- $A + B$ is a continuous function of $A, B$.
- Given $A, B, C$ on the curve, we have $A', B', C'$ arbitrarily close to $A, B, C$ making distinct the things we want distinct ($\{A, ..., S, T\}$).
- Reid builds two continuous functions $f, g$ (such that $f = g$ implies associativity) and argues that there is a dense subset in which $f = g$.

It would be much better to prove associativity using multiplicity arguments, instead.

# 3 Final Remarks from Fernando

Recall that the cubic $y^2 = x(x-1)(x-\lambda)$ has no rational parameterization. We know that, for a circle, there exists a rational parameterization $(x(t), y(t))$ as well as an irrational parameterization $(cos\theta, sin\theta)$. So we ask: is there a pair of functions $(f(z), g(z))$ to parameterize our cubic? There is $f(z_1 + z_2)$, a rational function of $f(z_1)$ and $f(z_2)$. When you unpack this addition law, you see this is related to the group law we just defined.