

We saw that for the circle and indeed, for any irreducible plane conic there is a rational parametrization: if $C(x,y) = 0$ is the equation of the plane conic, there are nonconstant rational functions $f(t), g(t)$ such that $C(f(t), g(t)) = 0$.

Theorem let

$$F(x,y) = y^2 - x(x-1)(x-\lambda).$$

If $\lambda \neq 0, 1$, and $f(t), g(t) \in \mathbb{C}(t)$ are rational functions such that

$$(*) F(f(t), g(t)) = 0, \text{ then}$$

$$f, g \in \mathbb{C}.$$

Note $(*)$ says

$$(**) f^2 = g(g-1)(g-\lambda).$$

Lemma Suppose $a = (a_0 : a_1)$, $b = (b_0 : b_1)$,
 $c = (c_0 : c_1)$ are distinct points of \mathbb{P}_K^1 .

Then there is an
invertible 2×2 matrix $X \in GL(2, K)$
with $m_X(1:0) = a$, $m_X(0:1) = b$,
 $m_X(1:1) = c$.

Proof. Since a, b, c are distinct, the vectors
 $A = (a_0, a_1)$, $B = (b_0, b_1)$, $C = (c_0, c_1)$
are pairwise linearly independent, and C
is a linear combination of A and B , say
 $C = \mu A + \lambda B$, with $\mu \neq 0 \neq \lambda$.

If we choose $X = \begin{pmatrix} \mu a_0 & \lambda b_0 \\ \mu a_1 & \lambda b_1 \end{pmatrix}$,

then $m_X(1:0) = (\mu a_0 : \mu a_1) = (a_0 : a_1) = a$,
 $m_X(0:1) = (\lambda b_0 : \lambda b_1) = (b_0 : b_1) = b$,
 $m_X(1:1) = (\mu a_0 + \lambda b_0 : \mu a_1 + \lambda b_1) = c$. \square .

Lemma Suppose $p, q \in \mathbb{C}[t]$ are coprime, and assume that there are 4 distinct linear combinations $\lambda p + \mu q$ (that is, the 4 points $(\lambda : \mu) \in \mathbb{P}_\mathbb{C}^1$ are distinct) that are squares in $\mathbb{C}[t]$. Then $pq \in \mathbb{C}$.

Proof. Note first the following.

Let $X \in GL(2, \mathbb{C})$ (an invertible 2×2 matrix),

say $X = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$, and let

$p' = ep + gq$, $q' = fp + hq$. Then

for any (a, b) ,

$$ap' + bq' = aep + agq + bfp + bhq$$

$$= Ap + Bq$$

where $\begin{pmatrix} A \\ B \end{pmatrix} = X \cdot \begin{pmatrix} a \\ b \end{pmatrix}$.

thus, if there are 4 distinct linear combinations of p and q (corresponding to $P_1, P_2, P_3, P_4 \in \mathbb{P}^1$)

that are squares, there are 4 distinct linear combinations of p' and q' (corresponding to $m_X(p_1)$, $m_X(p_2)$, $m_X(p_3)$, $m_X(p_4)$) that are squares.

By the previous lemma, we may choose m_X (really m_X^{-1} in the lemma!) so that $m_X(p_1) = (i:0)$, $m_X(p_2) = (0:1)$, $m_X(p_3) = (1:i)$, and $m_X(p_4) = (\lambda:1)$

for some $0, i \neq \lambda \in \mathbb{C}$. Thus, we may assume p' , q' , $p'+q'$, and $\lambda p'+q'$ are squares.

Furthermore, p' and q' will also be coprime (just as p and q were) — if not, say D divides both, then D divides any linear combination of them; but p and q may be realized as linear combinations of p' and q' (this uses that X has an inverse!).

Now, suppose the lemma does not hold; let

p, q be a counterexample with

$\max \{ \deg(p), \deg(q) \}$ as small as possible

By our discussion above, we may assume

(replacing p, q by p', q') that p, q

are coprime and $p, q, p+q$, and $\lambda p+q$

are squares (for some $\lambda \in \mathbb{C}, \lambda \neq 0, 1$). Write

$p = u^2, q = v^2$ ($u, v \in \mathbb{C}[t]$). Then

(i) u, v are coprime,

$$(ii) \quad p+q = u^2+v^2 = (u+iv)(u-iv)$$

$$\lambda p+q = (\sqrt{\lambda}u+iv)(\sqrt{\lambda}u-iv)$$

are squares in $\mathbb{C}[t]$, which, by
coprimeness of u, v implies

$u+iv, u-iv, \sqrt{\lambda}u+iv, \sqrt{\lambda}u-iv$
are squares. [think it through!]

$$(iii) \quad \max \{ \deg(u), \deg(v) \} < \max \{ \deg(p), \deg(q) \}.$$

By minimality of our choice of p, q , we find

that u, v are constant, a contradiction

to p, q not being constant. So p, q
must be constant. \square

Proof of Thm. Write

$$f(t) = \frac{r(t)}{s(t)}, \quad g(t) = \frac{p(t)}{q(t)} \quad \text{with}$$

r, s coprime and p, q coprime. Clearing denominators in $F(f, g) = 0$, we get

$$(\text{***}) \quad r^2 q^3 = s^2 p (p - q) (p - \lambda q).$$

Since r and s are coprime, s^2 on RHS divides q^3 ; similarly, p and q coprime $\Rightarrow q^3$ divides s^2 . So, $s^2 = aq^3$ for some $a \in \mathbb{C}$. Then

$$\left(\frac{s}{q}\right)^2 = \frac{s^2}{q^2} = aq \quad \text{is a square in } \mathbb{C}[t].$$

Moreover, (***) also gives

$$r^2 = a p (p - q) (p - \lambda q).$$

Since p and $p - q$ are coprime, as are p and $p - \lambda q$, and $p - q$ and $p - \lambda q$, all of p , $p - q$, $p - \lambda q$ are squares in $\mathbb{C}[t]$.

Apply the second lemma to conclude that p and q , hence r and s , are constant. \square

Group Law On A Cubic

There is one amazing way in which a cubic curve

$$y^2 = x(x-1)(x-\lambda)$$

is like $\mathbb{A}_\mathbb{C}^1$. Namely, there is a nice way to make $\mathbb{A}_\mathbb{C}^1$ into an abelian group; and, suitably interpreted, the same is true of our cubic curve!

"Suitably interpreted" requires the projective plane cubic

$$C = V(y^2z - x(x-z)(x-\lambda z)) \subseteq \mathbb{P}_\mathbb{C}^2.$$

We impose the following requirements:

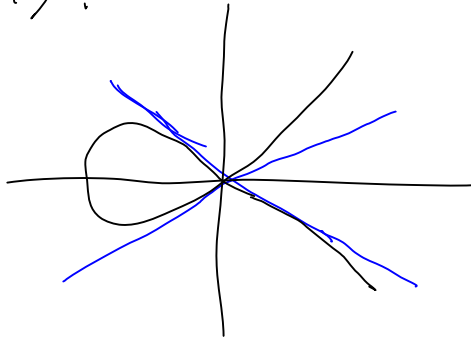
(1) C is irreducible.

(2) For every $p \in C$, there is a unique line $L \subseteq \mathbb{P}_\mathbb{C}^2$ such that p

is a repeated zero of $(y^2z - x(x-z)(x-\lambda z))|_L$.

Remark (2) is just the condition that there is a unique tangent line to the curve at p .

Example Consider $y^2 = x^2(x+1)$.



let $L = \{ (t, t) \mid t \in k \}$. then

$$(y^2 - x^2(x+1))|_L = t^2 - t^2(t+1) = -t^3.$$

if $L' = \{ (t, -t) \mid t \in k \}$, then

$$(y^2 - x^2(x+1))|_{L'} = t^2 - t^2(t+1) = -t^3$$

Theorem Suppose $C = (y^2z - x(x-z)(x-iz))$

is a complex plane cubic curve that satisfies

(1) and (2). Then there is a unique

group structure on C such that

(a) $\Theta = (0:1:0)$,

(b) $-(x:y:z) = (x:-y:z)$,

(c) $P+Q+R = \Theta$ iff $P, Q,$ and R are collinear.

Construction Given $P, Q \in C$, define

$P+Q$ as follows. Let $L = \overline{PQ}$ be the line through P and Q ; if $P=Q$, we take L to be the tangent line. Let

\bar{R} be the third point of intersection of L with C . What does it mean?

Write $F(x, y, z) = y^2z - x(x-z)(x+yz)$.

Then, when we choose a coordinate on L , $F|_L$ becomes a cubic polynomial,

so it has three zeros, although they are not necessarily distinct:



If $\bar{R} = (x:y:z)$, then we define

$$P+Q \stackrel{\text{def}}{=} (x:-y:z).$$

Example let $P=Q=(0:1:0)$. I claim that the tangent line to C at p is

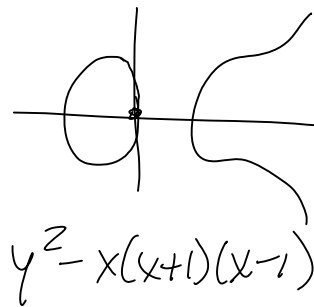
$V(z)$: indeed,

$F|_{V(z)} = -x^3$, which has a triple zero (not just a double one!) at $(0:1:0)$.

So in this case, $\bar{R} = (0:1:0)$ and
 $(0:1:0) + (0:1:0) = (0:-1:0) = (0:1:0)$.

Example What is $(0:0:1) + (0:0:1)$?

This point is fixed by the symmetry
 $(x:y:z) \mapsto (x:-y:z)$,
 so the tangent line to C at $(0:0:1)$
 must also be fixed (same as before,
 actually!).



Guess: $L = V(x)$.

The equation

$F|_L = y^2 z$, and parametrizing

the line as $\{(0, t, 1) \mid t \in \mathbb{C}\}$ on $\mathbb{A}_{\mathbb{C}}^2 \subset \mathbb{P}_{\mathbb{C}}^2$

we get

$F|_L(0, t, 1) = t^2$, which has a
 double zero at $t=0$. So yes, this

$F|_L(0, t, 1) = t$, which has a double zero at $t=0$. So yes, this is the tangent line.

$$\begin{aligned}
 \text{Now } L \cap C &= \mathcal{V}(x, y^2z - x(x-z)(x-\lambda z)) \\
 &= \{(0:y:z) \mid y^2z = 0\} \\
 &= \{(0:1:0), (0:0:1)\}.
 \end{aligned}$$

$$\begin{aligned}
 \text{So } (0:0:1) + (0:0:1) &= (0:-1:0) = (0:1:0) \\
 &= \mathcal{O}.
 \end{aligned}$$

Exactly the same argument will tell us that

$$(1:0:1) + (1:0:1) = \mathcal{O},$$

$$(\lambda:0:1) + (\lambda:0:1) = \mathcal{O}.$$