Algebraic Geometry

Vanya Cheltsov

31st January 2019

Lecture 6: group law on smooth cubic curves

Lines and cubic curves

Let $\mathcal{C}_3$ be a smooth cubic curve in $\mathbb{P}^2_{\mathbb{C}}$
Then the curve $\mathcal{C}_3$ is defined by

$$f_3(x, y, z) = 0,$$

where $f_3(x, y, z)$ is a homogeneous polynomial of degree 3.

- If P is a point on the curve $\mathcal{C}_3$, then

$$\frac{\partial f_3(x, y, z)}{\partial x}(P)x + \frac{\partial f_3(x, y, z)}{\partial y}(P)y + \frac{\partial f_3(x, y, z)}{\partial z}(P)z = 0$$

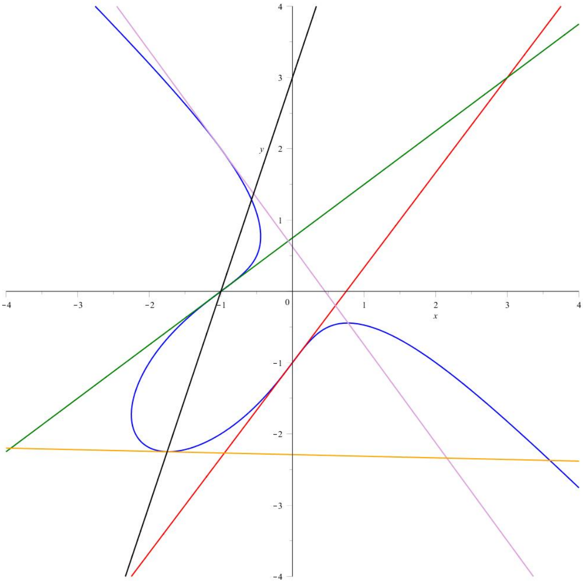
  defines the tangent line to $\mathcal{C}_3$ at the point P.

Let L be a line in $\mathbb{P}^2_{\mathbb{C}}$. Then

$$1 \leqslant \left|L \cap \mathcal{C}_3\right| \leqslant 3.$$

- If $|L \cap \mathcal{C}_3| < 3$, then L is tangent to $\mathcal{C}_3$.
- If $|L \cap \mathcal{C}_3| = 1$, then $L \cap \mathcal{C}_3$ is an inflection point of $\mathcal{C}_3$.

Lines and $x^3 + y^3 + z^3 + 4xyz = 0$



Lines and $x^3 + y^3 + z^3 + 4xyz = 0$ (Maple)

```
with(LinearAlgebra):
with(plots,implicitplot):
P1:=[0,1,-1];
P2:=[-1,0,1];
P3:=[-1,2,1];
P4:=[-7,-9,4];
f:=x^3+y^3+z^3+4*x*y*z;
fx:=diff(f,x);
fy:=diff(f,y);
fz:=diff(f,z);
a:=subs({x=P1[1],y=P1[2],z=P1[3]},fx);
b:=subs({x=P1[1],y=P1[2],z=P1[3]},fy);
c:=subs({x=P1[1],y=P1[2],z=P1[3]},fz);
TP1:=a*x+b*y+c*z;
a:=subs({x=P2[1],y=P2[2],z=P2[3]},fx);
b:=subs({x=P2[1],y=P2[2],z=P2[3]},fy);
c:=subs({x=P2[1],y=P2[2],z=P2[3]},fz);
TP2:=a*x+b*y+c*z;
a:=subs({x=P3[1],y=P3[2],z=P3[3]},fx);
b:=subs({x=P3[1],y=P3[2],z=P3[3]},fy);
c:=subs({x=P3[1],y=P3[2],z=P3[3]},fz);
TP3:=a*x+b*y+c*z;
a:=subs({x=P4[1],y=P4[2],z=P4[3]},fx);
b:=subs({x=P4[1],y=P4[2],z=P4[3]},fy);
c:=subs({x=P4[1],y=P4[2],z=P4[3]},fz);
TP4:=a*x+b*y+c*z;
L24:=Determinant([P2,P4,[x,y,z]]);
tp1:=subs(z=1, TP1);
tp2:=subs(z=1,TP2);
tp3:=subs(z=1,TP3);
tp4:=subs(z=1,TP4);
l24:=subs(z=1,L24);
g:=subs(z=1,f);
implicitplot([g=0,tp1=0,tp2=0,tp3=0,tp4=0,l24=0],x=-4..4,y=-4..4);
```

Adding points on cubic curves

Let $\mathcal{C}_3$ be a smooth cubic curve in $\mathbb{P}^2_{\mathbb{C}}$
Fix a point $\mathbf{O}$ in the curve $\mathcal{C}_3$.
For two points A and B in $\mathcal{C}_3$, let us define the point

$$A+B \in \mathcal{C}_3$$

using the following algorithm:

- If $A \neq B$, let L be the line passing through A and B.
- If $A = B$, let L be the tangent line to $\mathcal{C}_3$ at $A = B$.
- Then $L \cap \mathcal{C}_3$ consists of A, B and some point P.
- Here we count points in $L \cap \mathcal{C}_3$ with multiplicities.
  - If $A \neq B$ and L is tangent to $\mathcal{C}_3$ at A, then $P = A$.
  - If $A \neq B$ and L is tangent to $\mathcal{C}_3$ at B, then $P = B$.
  - If $A = B = L \cap \mathcal{C}_3$, then $P = A = B$.
- If $P \neq \mathbf{O}$, let L' be the line passing through P and $\mathbf{O}$.
- If $P = \mathbf{O}$, let L' be the line tangent to $\mathcal{C}_3$ at P.
- Then $L' \cap \mathcal{C}_3$ consists of P, $\mathbf{O}$ and some point Q.
- Let $A+B = Q$.

Adding points on $x^3 + y^3 + z^3 + 4xyz = 0$ (Algebra)

Let $\mathcal{C}_3$ be the cubic curve given by

$$x^3 + y^3 + x^3 + 4xyz = 0.$$

Then $\mathcal{C}_3$ is smooth.
Let $\mathbf{O} = [0 : 1 : -1]$, $A = [-1 : 0 : 1]$, $B = [-7 : -9 : 4]$.
The line L containing A and B is given by

$$3x - y + 3z = 0.$$

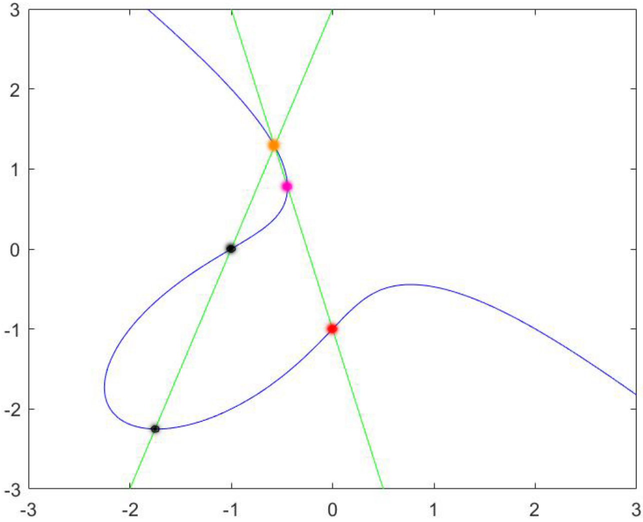
Then $L \cap \mathcal{C}_3$ consists of A, B and $P = [-4 : 9 : 7]$.
The line L' containing P and $\mathbf{O}$ is given by

$$4x + y + z = 0.$$

Then $L' \cap \mathcal{C}_3$ consists of P, $\mathbf{O}$ and $Q = [-4 : 7 : 9]$.
Thus, we have

$$A + B = \big[-4 : 7 : 9 \big]$$

Adding points on $x^3 + y^3 + z^3 + 4xyz = 0$ (Geometry)



Adding points on $x^3 + y^3 + z^3 + 4xyz = 0$ (Maple)

```
with(LinearAlgebra):
with(plots,implicitplot):
unprotect(O);
P1:=[0,1,-1];
P2:=[-1,0,1];
P3:=[-1,2,1];
P4:=[-7,-9,4];
f:=x^3+y^3+z^3+4*x*y*z;
O:=P1; A:=P2; B:=P4;
L1:=Determinant(Matrix([A,B,[x,y,z]]));
L1capC:=solve([f=0,L1=0,z=1],[x,y,z]);
solution:=L1capC[3];
P:=[eval(x,solution),eval(y,solution),eval(z,solution)];
L2:=Determinant(Matrix([P,O,[x,y,z]]));
L2capC:=solve([f=0,L2=0,z=1],[x,y,z]);
solution:=L2capC[2];
Q:=[eval(x,solution),eval(y,solution),eval(z,solution)];
AplusB:=Q;
l1:= subs(z=1,L1); l2:=subs(z=1,L2); g:=subs(z=1,f);
implicitplot([g=0,l1=0,l2=0],x=-4..4,y=-4..4);
```

Doubling points on $x^3 + y^3 + z^3 + 4xyz = 0$ (Algebra)

Let $\mathcal{C}_3$ be the cubic curve given by

$$x^3 + y^3 + x^3 + 4xyz = 0.$$

Let $\mathbf{O} = [0 : 1 : -1]$ and $A = [-1 : 2 : 1]$. Then

$$2A = A + A = \left[7 : 9 : -4\right].$$

Indeed, the tangent line to $\mathcal{C}_3$ at the point A is given by

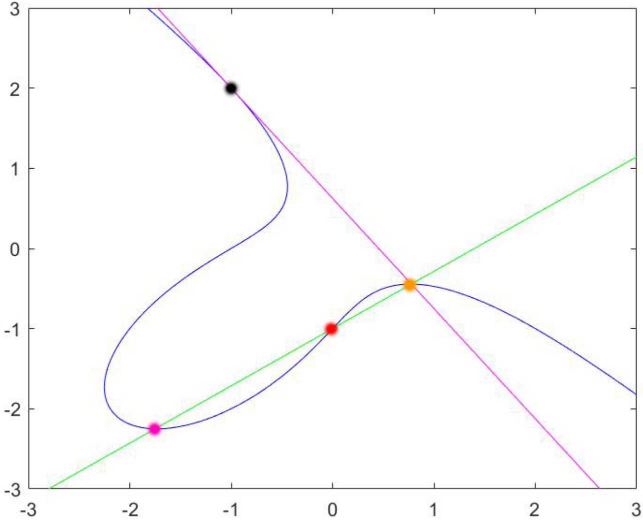
$$11x + 8y - 5z = 0.$$

It intersects the curve $\mathcal{C}_3$ at the point A and $[7 : -4 : 9]$.
The line L' containing $[7 : -4 : 9]$ and $\mathbf{O}$ is given by

$$5x - 7y - 7z = 0.$$

Then $L' \cap \mathcal{C}_3$ consists of $[7 : -4 : 9]$, $\mathbf{O}$ and $[7 : 9 : -4]$.

Doubling points on $x^3 + y^3 + z^3 + 4xyz = 0$ (Geometry)



Doubling points on $x^3 + y^3 + z^3 + 4xyz = 0$ (Maple)

```
with(LinearAlgebra): with(plots,implicitplot): unprotect(O);
P1:=[0,1,-1]; P2:=[-1,0,1]; P3:=[-1,2,1]; P4:=[-7,-9,4];
f:=x^3+y^3+z^3+4*x*y*z;
fx:=diff(f,x); fy:=diff(f,y); fz:=diff(f,z);
a:=subs({x=P3[1],y=P3[2],z=P3[3]},fx);
b:=subs({x=P3[1],y=P3[2],z=P3[3]},fy);
c:=subs({x=P3[1],y=P3[2],z=P3[3]},fz);
TP3:=a*x+b*y+c*z;
O:=P1; A:=P3;
L1:=TP3;
L1capC:=solve([f=0,L1=0,y=1],[x,y,z]);
solution:=L1capC[1];
P:=[eval(x,solution),eval(y,solution),eval(z,solution)];
L2:=Determinant(Matrix([P,O,[x,y,z]]));
L2capC:=solve([f=0,L2=0,y=1],[x,y,z]);
solution:=L2capC[3];
Q:=[eval(x,solution),eval(y,solution),eval(z,solution)];
AplusA:=Q;
l1:= subs(z=1,L1); l2:=subs(z=1,L2); g:=subs(z=1,f);
implicitplot([g=0,l1=0,l2=0],x=-4..4,y=-4..4);
```

Subtracting points on $x^3 + y^3 + z^3 + 4xyz = 0$ (Algebra)

Let $\mathcal{C}_3$ be the cubic curve given by

$$x^3 + y^3 + x^3 + 4xyz = 0.$$

Let $\mathbf{O} = [-1 : 2 : 1]$ and $A = [7 : 9 : -4]$.

Question

How to find $-A$?

The tangent line to $\mathcal{C}_3$ at the point $\mathbf{O}$ is given by

$$11x + 8y - 5z = 0.$$

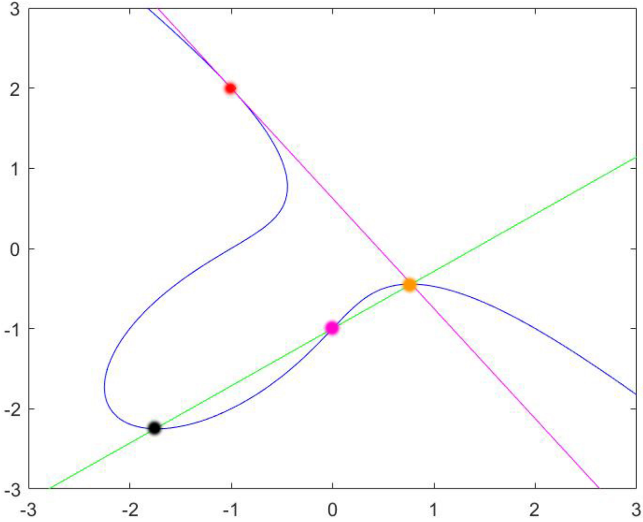
It intersects the curve $\mathcal{C}_3$ at the point $\mathbf{O}$ and $[7 : -4 : 9]$.
The line L' containing $[7 : -4 : 9]$ and A is given by

$$5x - 7y - 7z = 0.$$

Then $L' \cap \mathcal{C}_3$ consists of $[7 : -4 : 9]$, A and $[0 : -1 : 1]$. This gives

$$-A = \big[0 : -1 : 1\big].$$

Subtracting points on $x^3 + y^3 + z^3 + 4xyz = 0$ (Geometry)



Subtracting points on $x^3 + y^3 + z^3 + 4xyz = 0$ (Maple)

```
with(LinearAlgebra): with(plots,implicitplot): unprotect(O);
P1:=[0,1,-1]; P2:=[-1,0,1]; P3:=[-1,2,1]; P4:=[-7,-9,4];
f:=x^3+y^3+z^3+4*x*y*z;
fx:=diff(f,x); fy:=diff(f,y); fz:=diff(f,z);
a:=subs({x=P3[1],y=P3[2],z=P3[3]},fx);
b:=subs({x=P3[1],y=P3[2],z=P3[3]},fy);
c:=subs({x=P3[1],y=P3[2],z=P3[3]},fz);
TP3:=a*x+b*y+c*z;
O:=P3; TO:=TP3; A:=[7,9,-4];
L1:=TO;
L1capC:=solve([f=0,L1=0,y=1],[x,y,z]);
solution:=L1capC[1];
P:=[eval(x,solution),eval(y,solution),eval(z,solution)];
L2:=Determinant(Matrix([P,A,[x,y,z]]));
L2capC:=solve([f=0,L2=0,y=1],[x,y,z]);
solution:=L2capC[3];
Q:=[eval(x,solution),eval(y,solution),eval(z,solution)];
minusA:=Q;
l1:= subs(z=1,L1); l2:=subs(z=1,L2); g:=subs(z=1,f);
implicitplot([g=0,l1=0,l2=0],x=-4..4,y=-4..4);
```

The group law

- Let $\mathcal{C}_3$ be a smooth cubic curve in $\mathbb{P}^2_{\mathbb{C}}$
- Fix a point $\mathbf{O} = [a : b : c]$ in the curve $\mathcal{C}_3$.
- Equip $\mathcal{C}_3$ with the addition $+$ as above.

Theorem

The curve $\mathcal{C}_3$ equipped with $+$ is an abelian group.

- Let $\mathbb{F}$ be a subfield of the field $\mathbb{C}$.
- Suppose that the curve $\mathcal{C}_3$ is defined by

$$f_3(x, y, z) = 0$$

  for a cubic homogeneous polynomial $f_3(x, y, z) \in \mathbb{F}[x, y, z]$.
- Suppose that a, b and c are contained in $\mathbb{F}$.
- We say that $\mathcal{C}_3$ and $\mathbf{O}$ are defined over $\mathbb{F}$.

Denote by $\mathcal{C}_3(\mathbb{F})$ the set of all points in $\mathcal{C}_3$ defined over $\mathbb{F}$.

Theorem

The set $\mathcal{C}_3(\mathbb{F})$ equipped with $+$ is a subgroup of the group $\mathcal{C}_3$.

Identity, commutativity and inverses

Let $\mathcal{C}_3$ be a smooth cubic curve in $\mathbb{P}^2_{\mathbb{C}}$
Fix a point $\mathbf{O} = [a : b : c]$ in the curve $\mathcal{C}_3$.

- Let $\mathbb{F}$ be a subfield of the field $\mathbb{C}$.
- Suppose that $\mathcal{C}_3$ and $\mathbf{O}$ are defined over $\mathbb{F}$.

Equip $\mathcal{C}_3(\mathbb{F})$ with the addition $+$.

Lemma
For every A in $\mathcal{C}_3(\mathbb{F})$, one has $\boxed{\mathbf{O}+A = A+\mathbf{O} = A}$.

Lemma
For every A and B in $\mathcal{C}_3(\mathbb{F})$, one has $\boxed{A+B = B+A}$.

Lemma
For every $A \in \mathcal{C}_3(\mathbb{F})$ there is $B \in \mathcal{C}_3(\mathbb{F})$ such that

$$\boxed{A+B = B+A = \mathbf{O}.}$$

Associativity

Take three points A, B and C in $\mathcal{C}_3$.

- Let L be the line in $\mathbb{P}^2_{\mathbb{C}}$ that passes through A and B.
- Let P be the third point of the intersection $L \cap \mathcal{C}_3$.
- Let L' be the line in $\mathbb{P}^2_{\mathbb{C}}$ that passes through P and $\mathbf{O}$.

Then $A+B$ is the third point of the intersection $L' \cap \mathcal{C}_3$.

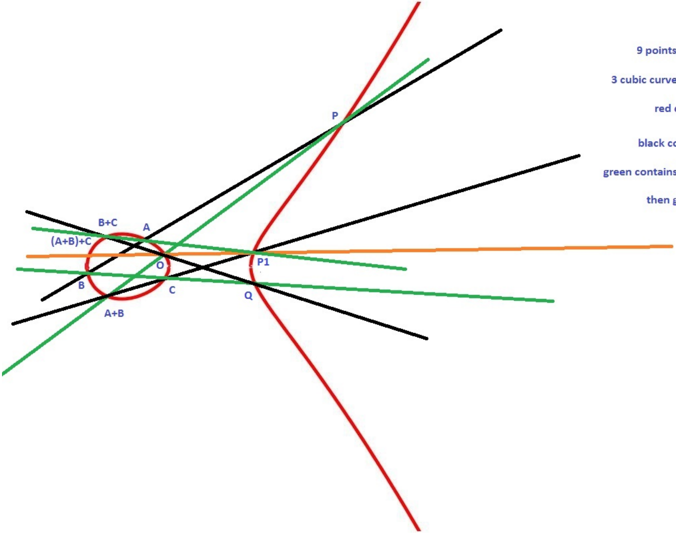
- Let $\overline{L}$ be the line in $\mathbb{P}^2_{\mathbb{C}}$ that passes through B and C.
- Let $\overline{P}$ be the third point of the intersection $\overline{L} \cap \mathcal{C}_3$.
- Let $\overline{L}'$ be the line in $\mathbb{P}^2_{\mathbb{C}}$ that passes through $\overline{P}$ and $\mathbf{O}$.

Then $B+C$ is the third point of the intersection $\overline{L}' \cap \mathcal{C}_3$.

- Let $\widehat{L}$ be the line in $\mathbb{P}^2_{\mathbb{C}}$ that passes through $A+B$ and C.
- Let $\widetilde{L}$ be the line in $\mathbb{P}^2_{\mathbb{C}}$ that passes through $B+C$ and A.
- Let $\widehat{P}$ be the third point of the intersection $\widehat{L} \cap \mathcal{C}_3$.
- If $\widehat{P} \in \widetilde{L}$, then $\boxed{(A+B)+C = A+(B+C)}$.

But $\mathcal{C}_3$ intersect $L + \overline{L}' + \widehat{L}$ by $\mathbf{O}$, A, B, C, P, $\overline{P}$, $\widehat{P}$, $A+B$, $B+C$.
And $L' + \overline{L} + \widetilde{L}$ contains $\mathbf{O}$, A, B, C, P, $\overline{P}$, $A+B$, $B+C$.
Then $\widehat{P} \in L' + \overline{L} + \widetilde{L}$ by Chasles's theorem, so that $\widehat{P} \in \widetilde{L}$.

Associativity on the cubic curve $zy^2 = x(x-z)(x-2z)$



9 points: O, A, B, C, P, A+B, P1, B+C, Q

3 cubic curve: red, black, green

red containe all 9 points

black contains all nine points

green contains O, A, B, C, P, A+B, B+C, Q

then green must contain P1

Adding points on $zy^2 = x^3 - zx^2 - 4xz^2 + 4z^3$

Let $\mathcal{C}_3$ be the cubic curve in $\mathbb{P}^2_{\mathbb{C}}$ given by

$$\boxed{zy^2 = x^3 - zx^2 - 4xz^2 + 4z^3.}$$

- Put $\mathbf{O} = [0 : 1 : 0]$.
- Let $\mathbf{O}$ be the zero in $\mathcal{C}_3$.

Put $A = [1 : 0 : 1]$ and $B = [0 : 2 : 1]$. Let us find $A+B$.

- The line that contains A and B is given by

$$\boxed{2x + y - 2z = 0.}$$

- It intersects $\mathcal{C}_3$ by A, B and $[4 : -6 : 1]$.
- The line that contains $[4 : -6 : 1]$ and $\mathbf{O}$ is given by

$$\boxed{x - 4z = 0.}$$

- It intersects $\mathcal{C}_3$ by $\mathbf{O}$, $[4 : -6 : 1]$ and $[4 : 6 : 1]$.

Thus, the point $A+B$ is $[4 : 6 : 1]$.

Orders of points on $zy^2 = x^3 - zx^2 - 4xz^2 + 4z^3$

- Let $\mathcal{C}_3$ be the cubic in $\mathbb{P}^2_{\mathbb{C}}$ given by

$$\boxed{zy^2 = x^3 - zx^2 - 4xz^2 + 4z^3.}$$

- Let $\mathbf{O} = [0 : 1 : 0]$. Then $\mathbf{O} \in \mathcal{C}_3$.
- Equip $\mathcal{C}_3$ with $+$ such that $\mathbf{O}$ is zero.

Put $A = [4 : 6 : 1]$. Let us find nA for small n.

- The tangent line to $\mathcal{C}_3$ at A is $\boxed{3x - y - 6z = 0}$.
- It intersects $\mathcal{C}_3$ by A and $[2 : 0 : 1]$.
- The line that contains $[2 : 0 : 1]$ and $\mathbf{O}$ is $\boxed{x - 2z = 0}$.
- It contains $\mathbf{O}$ and tangents $\mathcal{C}_3$ at $[2 : 0 : 1]$.
- This shows that $2A = [2 : 0 : 1]$.
- But the line that contains A and $2A$ is $\boxed{3x - y - 6z = 0}$.
- We already know that it tangents $\mathcal{C}_3$ at A.
- This shows that $3A = 2A + A = [4 : -6 : 1]$.
- Finally, we compute that $4A = \mathbf{O}$.

Therefore, the order of the point A is 4.

Points of order two

- Let $\mathcal{C}_3$ be a smooth cubic in $\mathbb{P}^2_{\mathbb{C}}$.
- Let $\mathbf{O}$ be a point in $\mathbb{P}^2_{\mathbb{C}}$ that is contained in $\mathcal{C}_3$.

Equip $\mathcal{C}_3$ with $+$ such that $\mathbf{O}$ is zero.

- Let L be the line in $\mathbb{P}^2_{\mathbb{C}}$ that is tangent to $\mathcal{C}_3$ at $\mathbf{O}$.
- Let $\widehat{O}$ be the remaining point in $L \cap \mathcal{C}_3$
- Let $\widehat{L}$ be the line in $\mathbb{P}^2_{\mathbb{C}}$ that is tangent to $\mathcal{C}_3$ at $\widehat{O}$.

Suppose that $\widehat{O} = [0 : 1 : 0]$ and $\widehat{L}$ is $z = 0$. Then $\mathcal{C}_3$ is given by

$$zy^2 = \left(Ax^2 + Bxz + Cz^2\right)y + Dx^3 + Ex^2z + Gxz^2 + Hz^3$$

for some A, B, C, D, E, F, G, H, I, J in $\mathbb{C}$.
Then the points of order 2 in $\mathcal{C}_3(\mathbb{F})$ are given by

$$\left[2\lambda : A\lambda^2 + B\lambda + C : 2\right]$$

for $\lambda \in \mathbb{C}$ such that

$$\left(A\lambda^2 + B\lambda + C\right)^2 + 4\left(D\lambda^3 + E\lambda^2 + G\lambda + H\right) = 0$$

and the line $x = \lambda z$ does not contain $\mathbf{O}$.

Simplified group law

- Let $\mathcal{C}_3$ be a smooth cubic in $\mathbb{P}^2_{\mathbb{C}}$ given by

$$zy^2 = Ax^3 + Bx^2z + Cxz^2 + Dz^3$$

for some complex numbers A, B, C, D.

Put $\mathbf{O} = [0 : 1 : 0]$ and equip $\mathcal{C}_3$ with $+$ such that $\mathbf{O}$ is zero.

Lemma

For any $A = [a : b : c] \in \mathcal{C}_3$, one has $\boxed{-A = [a : -b : c]}$.

Lemma

Let A, B, C be points in $\mathcal{C}_3$. Then

$$\boxed{A + B + C = \mathbf{O} \iff A, B, C \text{ are collinear.}}$$

Then points of order 2 are $[\alpha : 0 : 1]$ for $\alpha \in \mathbb{C}$ such that

$$A\alpha^3 + B\alpha^2 + C\alpha + D = 0.$$