MIDTERM

Huan Q. Bui

MA434: Algebraic Geometry
March 9-13, 2020

Problem	Earned	Total
1		20
2		20
5		20
6		20
8		20
10		20
11		20
Total	/100	120

Problem 1 (20 pts)

Suppose $f(X, Y, Z)$ is a homogeneous polynomial of degree n with coefficients in $\mathbb{R}$, so that we have $f(tX, tY, tZ) = t^n(X, Y, Z)$. Show that

$$X\frac{\partial f}{\partial X} + Y\frac{\partial f}{\partial Y} + Y\frac{\partial f}{\partial y} = nf.$$

(Hint: this is true for any differentiable function that satisfies the equation $f(tX, tY, tZ) = t^n f(X, Y, Z)$, not just for polynomials; use calculus.)

It's worth point out that this shows that if a point P satisfies

$$\left.\frac{\partial f}{\partial X}\right|_P = \left.\frac{\partial f}{\partial X}\right|_P = \left.\frac{\partial f}{\partial X}\right|_P = 0, \tag{1}$$

then P is automatically on the curve defined by $f(X, Y, Z) = 0$.

Solution: Let such a function f be given. Since f is a polynomial in X, Y, Z, it is an everywhere-differentiable function. This allows us to use calculus without "worries." Consider the change of variables $(X, Y, Z) \xrightarrow{t} (X', Y', Z')$ given by $X' = tX; Y' = tY, Z' = tZ$. We look at the following chain of implications

$$\begin{aligned}
f(X', Y', Z') &= t^n f(X, Y, Z), \quad \text{(hypothesis)}\\
\frac{\partial}{\partial t} f(X', Y', Z') &= \frac{\partial}{\partial t}[t^n f(X, Y, Z)]\\
\frac{\partial X'}{\partial t}\frac{\partial f}{\partial X'} + \frac{\partial Y'}{\partial t}\frac{\partial f}{\partial Y'} + \frac{\partial Z'}{\partial t}\frac{\partial f}{\partial Z'} &= nt^{n-1} f(X, Y, Z), \quad \text{(chain rule)}\\
X\frac{\partial f}{\partial X'} + Y\frac{\partial f}{\partial Y'} + Z\frac{\partial f}{\partial Z'} &= nt^{n-1} f(X, Y, Z)
\end{aligned}$$

This last equality holds for all t. Setting $t = 1$, we have $X' = tX = X, Y' = Y, Z' = Z$, and thus it follows that

$$X\frac{\partial f}{\partial X} + Y\frac{\partial f}{\partial Y} + Z\frac{\partial f}{\partial Z} = nf(X, Y, Z).$$

For any point $P = (\bar{X}, \bar{Y}, \bar{Z})$ such that Eq. (1) is satisfied, $nf(P) = 0$ automatically and thus $f(P) = 0$, i.e., P is on the curve defined by $f(X, Y, Z) = 0$.

$\square$

Problem 2 (20 pts)

The Proposition in section 1.13 of *Undergraduate Algebraic Geometry* says that in a pencil of conics *containing at least one non-degenerated conic* there will be at most 3 degenerate conics, and if $k = \mathbb{R}$ there will always be at least one degenerate conic. Find an example of a pencil of conics over $\mathbb{R}$ that does not contain any non-degenerate conics.

Solution: Call $C_{(\lambda,\mu)} : (\lambda Q_1 + \mu Q_2 = 0)$ the desired pencil of conics. The Proposition in 1.13 of Reid's says that if $C_{(\lambda,\mu)}$ contains at least one non-degenerate conic and if $k = \mathbb{R}$, then $C_{(\lambda,\mu)}$ contains *at least one* degenerate conic. This means we want our desired $C_{(\lambda,\mu)}$ to be degenerate.

The condition that $C_{(\lambda,\mu)}$ contains at least one non-degenerate conic is equivalent to $F_{(\lambda,\mu)}$ not identically zero where $F_{(\lambda,\mu)} = \det(\lambda Q_1 + \mu Q_2)$, with Q_1, Q_2 written as 3×3 symmetric matrices. So, our $C_{(\lambda,\mu)}$ must be such that $F_{(\lambda,\mu)}$ is identically zero. In fact, $C_{(\lambda,\mu)}$ degenerate $\iff$ $F_{(\lambda,\mu)} = \det(\lambda Q_1 + \mu Q_2) = 0 \;\forall\, \lambda, \mu \in \mathbb{R}$.

<u>Goal</u>: to find Q_1, Q_2 such that $F_{(\lambda,\mu)}$ is identically zero, i.e.,

$$\det\left[\lambda \underbrace{\begin{pmatrix} a & b & d \\ b & c & e \\ d & e & f \end{pmatrix}}_{Q_1} + \mu \underbrace{\begin{pmatrix} a' & b' & d' \\ b' & c' & e' \\ d' & e' & f' \end{pmatrix}}_{Q_2}\right] \equiv 0.$$

where

$$Q = aX^2 + 2bXY + cY^2 + 2dXZ + 2eYZ + fZ^2 \longleftrightarrow \begin{pmatrix} a & b & d \\ b & c & e \\ d & e & f \end{pmatrix}.$$

Consider $Q_1 = -X^2 + Y^2$ and $Q_2 = 2XY + 2YZ$, then

$$F_{(\lambda,\mu)} = \det\left[\lambda \underbrace{\begin{pmatrix} -1 & & \\ & 1 & \\ & & 0 \end{pmatrix}}_{Q_1} + \mu \underbrace{\begin{pmatrix} & 1 & \\ 1 & & 1 \\ & 1 & \end{pmatrix}}_{Q_2}\right] = \det\begin{pmatrix} -\lambda & \mu & 0 \\ \mu & \lambda & \mu \\ 0 & \mu & 0 \end{pmatrix} = \lambda\mu^2 - \mu^2\lambda = 0.$$

This holds for all λ, μ. So, $C_{(\lambda,\mu)}$ generated by the conics $C_1 : (Q_1 = -X^2 + Y^2 = 0)$ and $C_2 : (Q_2 = 2XY + 2YZ = 0)$ is degenerate $\iff$ $C_{(\lambda,\mu)}$ contains no non-degenerate conics. Not surprisingly, both C_1 and C_2 look like lines.

□

Problem 5 **(20 pts)**

This problem describes another way of thinking about the projective line $\mathbb{P}^1(k)$. Remember that the affine line $\mathbb{A}^1(k)$ is just another name for the field k. Any point in $\mathbb{P}^1(k)$ looks like $[u : v]$ with $u, v \in k$. Define the subsets $U = \left\{[u : v] \in \mathbb{P}^1(k) \,|\, v \neq 0\right\}$ and $V = \left\{[u : v] \in \mathbb{P}^1(k) \,|\, u \neq 0\right\}$.

(a) If $[u : v] \in U$, define $f([u : v]) = u/v$. Show: f is a bijection between U and $\mathbb{A}^1(k)$.

(b) If $[u : v] \in U$, define $g([u : v]) = v/u$. Show: g is a bijection between V and $\mathbb{A}^1(k)$.

(c) Suppose $t \in \mathbb{A}^1(k), t \neq 0$, What is $f(g^{-1}(t))$?

(d) Explain how this means we can think of $\mathbb{P}^1(k)$ as the result of gluing two copies of $\mathbb{A}^1(k)$ along the subsets $\mathbb{A}^1(k) \setminus \{0\}$ via the function $t \to 1/t$. (If you prefer to avoid the language of "gluing," you can express it as taking the disjoint union of two copies of $\mathbb{A}^1(k)$ and then passing to the quotient with respect to an equivalence relation.)

Solution:

(a)
- 1-to-1: Let $u/v = u'/v' \in \mathbb{A}^1(k)$ be given ($v, v' \neq 0$), then clearly $[u : v] = [u' : v'] \in U$, by definition. So f is injective.
- Onto: Any element of $\mathbb{A}^1(k)$ can be written as u/v for some $u, v \in \mathbb{A}^1(k)$ where $v \neq 0$. Then $[u : v] \in U$ is an element such that $f([u : v]) = u/v$.

(b)
- 1-to-1: Let $v/u = v'/u' \in \mathbb{A}^1(k)$ be given ($u, u' \neq 0$), then clearly $[u : v] = [u' : v'] \in V$, by definition. So g is injective.
- Onto: Any element of $\mathbb{A}^1(k)$ can be written as v/u for some $v, u \in \mathbb{A}^1(k)$ where $u \neq 0$. Then $[u : v] \in V$ is an element such that $g([u : v]) = v/u$.

(c) Let $t \in \mathbb{A}^1(k)$ be given. Then $g^{-1}(t) = [u : v] \in V$, where $u \neq 0$ and $v/u = t$. It follows that $f(g^{-1}(t)) = f([u : v]) = u/v = 1/t$.

(d) Here's how we can think of $\mathbb{P}^1(k)$ as the result of gluing two copies of $\mathbb{A}^1(k)$ along the subsets $\mathbb{A}^1(k) \setminus \{0\}$ via the function $t \to 1/t$ given by $f \circ g^{-1} : \mathbb{A}^1(k) \setminus \{0\} \to \mathbb{A}^1(k) \setminus \{0\}$ (which is bijective). Pictorially, the "gluing" action looks like this:

With f, we can identify almost all points (except for those with $v = 0$) in $\mathbb{P}^1(k)$ with points in $\mathbb{A}^1(k)$. With g, we can identify almost all points (except for those with $u = 0$) in $\mathbb{P}^1(k)$ with points in $\mathbb{A}^1(k)$. To identify *every* point in $\mathbb{P}^1(k)$ using $\mathbb{A}^1(k)$ we can "glue" (parts of) the images of f and g together. We do this using $f \circ g^{-1}$ to identify (i.e. defining an equivalence relation between) $t \in \mathbb{A}^1(k)$ with $1/t \in \mathbb{A}^1(k)$, $t \neq 0$. This way, we can "cover" the entire $\mathbb{P}^1(k)$ with two copies of $\mathbb{A}^1(k) \setminus \{0\}$. $\square$

Problem 6 **(20 pts)**

Let E be the cubic in $\mathbb{P}^2(\mathbb{Q})$ defined by the affine equation in Weierstrass form

$$y^2 = x^3 + x + 1.$$

The point $P = (0,1)$ is on E. Use the group law to compute $2P$, $3P$, and $4P$. (The numbers will get ugly, so use software. It's ok to use *Sage*'s built-in functions if you can figure out how to do it.)

Solution:

$\boxed{2P}$ To find $2P$, we want to find the inverse of the third intersection of the tangent line to E through $P = (0,1)$. Let $f(x,y) = y^2 - x^3 - x - 1$. This tangent line is given by

$$\frac{\partial f}{\partial x}(P)(x-0) + \frac{\partial f}{\partial y}(P)(y-1) = 0$$

$$(-3 \cdot 0^2 - 1)x + 2(y-1) = 0 \implies y = \frac{1}{2}x + 1$$

The third intersection (since P is a double intersection) of the tangent line and E:

$$\left(\frac{1}{2}x + 1\right)^2 = x^3 + x + 1, \quad \text{with } x \neq 0 \iff x = \frac{1}{4} \implies y = \frac{1}{2} \cdot \frac{1}{4} + 1 = \frac{9}{8}.$$

$2P$ is the inverse of this point (obtained by flipping the sign of the y-coordinate):

$$\boxed{2P = \left(\frac{1}{4}, \frac{-9}{8}\right)}$$

Mathematica code:

```
Solve[((1/2) x + 1)^2 == x^3 + x + 1, x]
{{x -> 0}, {x -> 0}, {x -> 1/4}}
```

$\boxed{3P}$ We repeat this process for $3P$. The line through P and $2P$ is given by

$$y = -\frac{17}{2}x + 1.$$

We rely on Mathematica to find the third intersection of this line with E. Taking the inverse of this third point, we get $3P$:

$$\boxed{3P = (72, +611)}$$

Mathematic code:

```
Solve[(-(17/2) x + 1)^2 == x^3 + x + 1, x]
{{x -> 0}, {x -> 1/4}, {x -> 72}}

-(17/2) 72 + 1
-611
```

$\boxed{4P}$ We do this once again to find $4P$. The line through $3P$ and P is given by

$$y = \frac{610}{72}x + 1.$$

(where I'm leaving the fraction unsimplified to make checking easier). Using Mathematica, we find the third intersection of this line with E. Taking the inverse of this third point, we get $4P$:

$$\boxed{4P = \left(\frac{-287}{1296}, \frac{40879}{46656}\right)}$$

Mathematica code:

```
Solve[((610/72) x + 1)^2 == x^3 + x + 1, x]
{{x -> -(287/1296)}, {x -> 0}, {x -> 72}}

(610/72) (-(287/1296)) + 1
-(40879/46656)
```

$\boxed{4P\text{, bis}}$ As a check, we can find $4P$ via $2P + 2P$ as well. In this case, we consider the line through $2P$ tangent to E. This line is given by

$$\left(-3 \cdot \left[\frac{1}{4}\right]^2 - 1\right)\left(x - \frac{1}{4}\right) + 2\left(\frac{-9}{8}\right)\left(y + \frac{9}{8}\right) = 0 \implies y = -\frac{19}{36}x - \frac{143}{144}.$$

We find the third intersection of this line and E and invert it to get the same $4P$, as expected.

Mathematica code:

```
Solve[(-(143/144) - (19 x)/36)^2 == x^3 + x + 1, x]
{{x -> -(287/1296)}, {x -> 1/4}, {x -> 1/4}}

-(143/144) - (19 (-(287/1296)))/36
-(40879/46656)
```

Problem 8 (20 pts)

(Gauss's Lemma) Suppose R is a UFD and K is its field of fractions. We want to compare factorizations in $R[x]$ and in $K[x]$. Let $f(x) \in R[x]$ and suppose we have $g(x), h(x) \in K[x]$ such that $f(x) = g(x)h(x)$. Show that there exists $a \in K$ such that $\tilde{g}(x) = ag(x) \in R[x]$, and $\tilde{h}(x) = \frac{1}{a}h(x) \in R[x]$, and so $f(x) = \tilde{g}(x)\tilde{h}(x)$ is a factorization in $R[x]$. (It's useful to remember that in a UFD every irreducible element is prime and that if D is a domain so is $D[x]$.)

Solution: (*inspired by the proofs of Gauss's Lemma & reducibility over* $\mathbb{Q}[x] \implies$ *reducibility over* $\mathbb{Z}[x]$ *by Gallian*) Let any $f(x) \in R[x]$ be given. We can factor out the content $c \in R$ of $f(x)$ so that $f(x) = cf_1(x)$ where f_1 is *primitive* (i.e., the coefficients of $f_1(x)$ have no irreducible factors in common). We first want to show that the product of two primitive polynomials is primitive.

To prove: The product of two primitive polynomials is primitive.

Let $\mathfrak{f}(x), \mathfrak{g}(x) \in R[x]$ be primitive polynomials. Suppose (to get a contradiction) that $\mathfrak{f}(x)\mathfrak{g}(x)$ is not primitive. Let p be an irreducible element of R (hence prime because R is a UFD) such that p divides the "gcd" of the coefficients of $\mathfrak{f}(x)\mathfrak{g}(x)$. Let $\bar{\mathfrak{f}}(x)$, $\bar{\mathfrak{g}}(x)$, and $\overline{\mathfrak{f}(x)\mathfrak{g}(x)}$ be the polynomials obtained from $\mathfrak{f}(x)$, $\mathfrak{g}(x)$, and $\mathfrak{f}(x)\mathfrak{g}(x)$ by reducing the coefficients "mod" p.

We consider the function $\phi : R[x] \to R_p[x]$ defined by

$$\phi\left(\sum_{i=1}^{n} a_i x^i\right) = \sum_{i=1}^{n} \bar{a}_i x^i$$

where $\bar{a} = a \mod p$. This is a ring homomorphism:

- $\phi(\mathfrak{f} + \mathfrak{g}) = \phi(\mathfrak{f} + \mathfrak{g})$:

$$\phi\left(\sum_{i=1}^{n} a_i x^i + \sum_{i=1}^{m} b_i x^i\right) = \sum_{i=1}^{n} \bar{a}_i x^i + \sum_{i=1}^{m} \bar{b}_i x^i = \phi\left(\sum_{i=1}^{n} a_i x^i\right) + \phi\left(\sum_{i=1}^{m} b_i x^i\right).$$

- $\phi(\mathfrak{f}\mathfrak{g}) = \phi(\mathfrak{f})\phi(\mathfrak{g})$:

$$\phi\left(\sum_{i=1}^{n} a_i x^i \cdot \sum_{i=1}^{m} b_i x^i\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} \bar{a}_i \bar{b}_j x^{i+j} = \phi\left(\sum_{i=1}^{n} a_i x^i\right)\phi\left(\sum_{i=1}^{m} b_i x^i\right).$$

So, $\bar{\mathfrak{f}}(x)$ and $\bar{\mathfrak{g}}(x)$ belong to $R_p[x]$, which we can see is an integral domain. Further, because the coefficients of $\mathfrak{f}(x)\mathfrak{g}(x)$ have p as a common factor (assumption), $\bar{\mathfrak{f}}(x)\bar{\mathfrak{g}}(x) = \overline{\mathfrak{f}(x)\mathfrak{g}(x)} = 0$, the zero element of $R_p[x]$. Therefore, $\bar{\mathfrak{f}}(x) = 0$ or $\bar{\mathfrak{g}}(x) = 0$, and so p divides every coefficient of $\mathfrak{f}(x)$ or p divides every coefficient of $\mathfrak{g}(x)$. This implies that either $\mathfrak{f}(x)$ is not primitive or $\mathfrak{g}(x)$ is not primitive. This contradicts our initial assumption. So $\mathfrak{f}(x)\mathfrak{g}(x)$ must be primitive. △

Back to our proof. Suppose we have $g(x), h(x) \in K[x]$ such that

$$f_1(x) = g(x)h(x) \in R[x]$$

(remember that $f_1(x)$ is the primitive polynomial constructed from $f(x)$). Let γ be the "lcm" of the denominators of the coefficients of $g(x)$, and η the "lcm" of the denominators of the coefficients of $h(x)$. Then we have $\gamma\eta f_1(x) = \gamma g(x) \cdot \eta h(x)$, where $\gamma g(x), \eta h(x) \in R[x]$. Let c_1 be the content of $\gamma g(x)$ and c_2 the content of $\eta h(x)$. Then,

$$\gamma g(x) = c_1 \tilde{g}(x)$$
$$\eta h(x) = c_2 \tilde{h}(x)$$

where both $\tilde{g}, \tilde{h}$ are primitive polynomials in $R[x]$. With this, we have

$$\gamma\eta f_1(x) = c_1 c_2 \tilde{g}(x)\tilde{h}(x). \tag{2}$$

Now, $f_1(x)$ is primitive, so the content of $\gamma\eta f_1(x)$ is $\gamma\eta$. $\tilde{g}(x)\tilde{h}(x)$ is primitive (because $\tilde{g}(x), \tilde{h}(x)$ are primitive), so the content of $\gamma\eta\tilde{g}(x)\tilde{h}(x)$ is $\gamma\eta$. From here, we see that $\gamma\eta = c_1c_2$, and thus $f_1(x) = \tilde{g}(x)\tilde{h}(x) \in R[x]$. In particular, because $\gamma\eta = c_1c_2$, we can call

$$a = \frac{\gamma}{c_1} = \frac{c_2}{\eta} \in K,$$

so that we can write, from Eq. (2),

$$f_1(x) = \tilde{g}(x)\tilde{h}(x) = \frac{\gamma}{c_1}\tilde{g}(x)\frac{c_2}{\eta}\tilde{h}(x) = a g(x)\frac{1}{a}h(x).$$

Obviously,

$$a g(x) = \frac{\gamma}{c_1} g(x) = \tilde{g}(x) \in R[x]$$
$$\frac{1}{a}h(x) = \frac{\eta}{c_2}h(x) = \tilde{h}(x) \in R[x].$$

So, we have shown that there exists $a \in K$ such that $\tilde{g}(x) = a g(x) \in R[x]$, $\tilde{h}(x) = \frac{1}{a}h(x) \in R[x]$, and thus $f_1(x) = \tilde{g}(x)\tilde{h}(x)$ is a factorization in $R[x]$. To recover $f(x)$ from $f_1(x)$ we can just let $\tilde{g}(x)$ absorb the content c of $f(x)$. Because $\tilde{g} \to c\tilde{g}$ must still be in $R[x]$, we get the factorization $f(x) = \tilde{g}(x)\tilde{h}(x)$ in $R[x]$.

$\square$

Problem 10 (20 pts)

Let $\mathcal{C}$ be the curve in $\mathbb{P}^2$ whose affine equation is $y^2 = x^3 + x^2$. This is the modal cubic we studied in section 2.1. Show that the line $y = tx$ has a double intersection with $\mathcal{C}$ at $(0,0)$ and find the third point of intersection. Check that this gives the parameterization in 2.1. What happens when $t = \pm 1$?

Solution: The x–coordinate of any intersection of the line $y = tx$ and the nodal cubic $y^2 = x^3 + x^2$ satisfies the equation:

$$\begin{aligned}(tx)^2 = x^3 + x^2 &\iff x^3 + (1 - t^2)x^2 = 0 \\ &\iff x^2(x + 1 - t^2) = 0. \qquad (3)\end{aligned}$$

Clearly, there is a double root at $x = 0$. Thus, the point $(x, tx) = (0,0)$ is a double intersection.

The x–coordinate of the third point of intersection solves the equation $x + 1 - t^2 = 0 \iff x = t^2 - 1$. Plugging this into the equation for the line, we get the third point of intersection:

$$(x, y) = (t^2 - 1, t^3 - t).$$

This is exactly the parameterization in 2.1. of Reid's.

When $t = \pm 1$, the third point of intersection is once again $(0,0)$, making $(0,0)$ a triple intersection (since Eq. (3) now becomes $x^3 = 0$). Both the lines $y = x$ and $y = -x$ are tangents to E at $(0,0)$. Intuitively, we can think about the triple intersection as three intersections, one of which due to one "branch" of the cubic and the other two is a double root on the other "branch." If we associate each line $y = \pm x$ to the correct "branch" of the cubic, we see that they are both tangent lines.

To see this more explicitly, we can consider the "branch" given by the parameterization:

$$t \to \begin{cases} (t, \sqrt{t^3 + t^2}), & t \geq 0 \\ (t, -\sqrt{t^3 + t^2}), & t < 0 \end{cases}$$

The line $y = x$ is tangent to this branch of $\mathcal{C}$ at $(0,0)$. We can see that

$$\lim_{h \downarrow 0} \frac{\sqrt{h^3 + h^2} - 0}{h} = 1 = \lim_{h \uparrow 0} \frac{-\sqrt{h^3 + h^2} - 0}{h},$$

which implies the slope of this branch at $(0,0)$ is 1, and so we see that $y = x$ is tangent to $\mathcal{C}$ here. Following a similar argument, we can see that $y = -x$ is tangent to the other branch of this cubic, again at $(0,0)$.

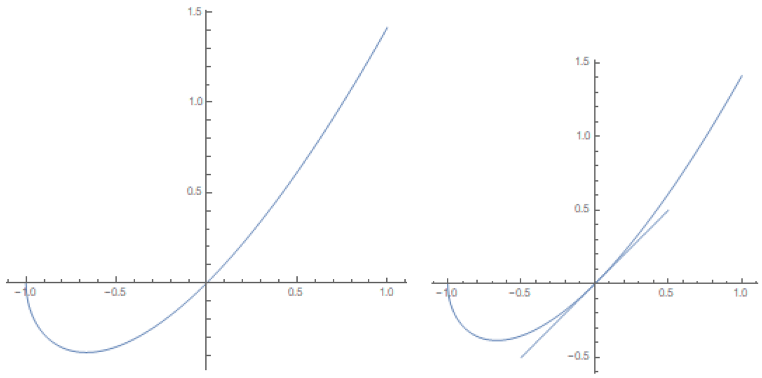

Figure 1: A "branch" of the nodal cubic and the tangent line $y = x$

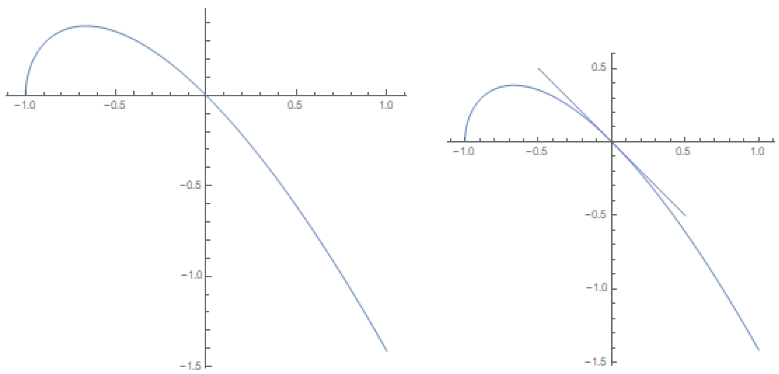

Figure 2: Another "branch" of the nodal cubic and the tangent line $y = -x$

Putting these pictures together we get two distinct tangents at $(0, 0)$:

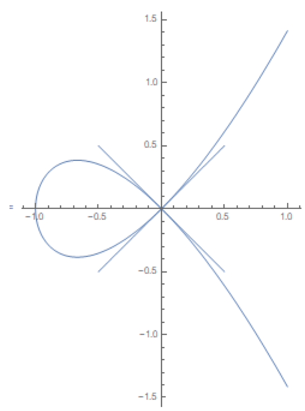

Figure 3: Another "branch" of the nodal cubic and the tangent line $y = -x$

$\square$

Problem 11 (20 pts)

With $\mathcal{C}$ as in the previous problem, let $\mathcal{C}(k)$ be the set of points on $\mathcal{C}$ with coefficients in k (including the point at infinity), and let $\mathcal{C}'(k) = \mathcal{C}(k) \setminus \{(0,0)\}$. (So $\mathcal{C}'(k)$ is the set of points on $\mathcal{C}$ where there is a unique tangent.) We want to try to define a group structure using the same method as for nonsingular cubics.

(a) Let A be a point in $\mathcal{C}(k)$ and let $P = (0,0)$. Let $\mathcal{L}$ be the line through A and P. What is the third intersection of $\mathcal{L}$ and $\mathcal{C}$?

(b) Explain why the point P is problematic if we want a group structure.

(c) Suppose $A, B \in \mathcal{C}'(k)$, and let $\mathcal{L}$ be the line through A and B. Show that the third intersection of $\mathcal{L}$ with $\mathcal{C}$ is in $\mathcal{C}'(k)$.

(d) Explain why this gives a group law on $\mathcal{C}'(k)$.

(It turns out that this group law $\mathcal{C}'(k) \cong k^\times$, but this is a little hard to prove.)

Solution: Here, we remove the "bad" point $(0,0)$ at which there exist distinct tangent lines. We hope to (and we do) get a group law on $\mathcal{C}'(k) = \mathcal{C}(k) \setminus \{(0,0)\}$ by doing this.

(a) The line L through P is a line through the origin $P = (0,0)$, so it must have the form $y = tx$. If $A \neq P = (0,0)$ then the third point of intersection is once again P, since (by Problem 10) the line $y = tx$ has a double intersection with $\mathcal{C}$. If $A = P$ then the third point of intersection has the coordinates $(t^2 - 1, t^3 - t)$. If $t = \pm 1$ then this third point is once again P (triple intersection).

(b) Essentially, the point P is problematic because there isn't a unique tangent line to $\mathcal{C}$ at P. When $P = (0,0)$ is included, addition in the group law is no longer well-defined—exactly because (as we have seen in Problem 10) there are two distinct tangent lines to $\mathcal{C}$ through P.

(c) Let $A, B \in \mathcal{C}'(k)$ be given. If $A \neq B$, we can write down the equation for the line $\mathcal{L}$ going through A and B. This equation has some form $y = \alpha x + \beta$ where $\alpha, \beta \in k$. After plugging this into $y^2 = x^3 + x^2$, we can simplify and have the factorization $(x - x_A)(x - x_B)(x - x_G) = 0$ for some x_G since we know x_A and x_B solve this equation. Expanding this equation, we have

$$0 = (x - x_A)(x - x_B)(x - x_G) = x^3 - x^2(x_A + x_B + x_G) + \dots \tag{4}$$

We know that $x_A + x_B + x_G \in k$ necessarily. Further, because $A, B \in \mathcal{C}'(k)$, $x_A + x_B \in k$. Thus, $x_G \in k$. With this, we see that $y_G = \alpha x_G + \beta \in k$ as well. So, the coordinates of the third intersection G of $\mathcal{L}$ with $\mathcal{C}$ are elements of k, i.e., $G \in \mathcal{C}'(k)$.

If $A = B$, then because $A, B \neq (0,0)$, there exists a unique tangent line which contains a third unique intersection with $\mathcal{C}$. Following a similar argument, but with $(x - x_A)^2(x - x_G = 0)$ (double intersection at $A = B$), we once again see that $G \in \mathcal{C}'(k)$.

(d) If we let the identity element be the point at infinity and construct a similar group operation to what we did with nonsingular cubics, we get a group law on $\mathcal{C}'(k)$. Here's why: in the previous items we have shown that the group operation is well-defined by disregarding $(0,0)$. The zero element is once again the point at infinity, which allows us to find, for each point in $\mathcal{C}'(k)$, an additive inverse by flipping the sign of the y–coordinate. Commutativity and associativity follows in the same manner as in the (simplified) group law. Clearly, if we have two points A, B, then $A+B$ is defined as the inverse of the (unique) intersection of the line through A, B and $\mathcal{C}$. So $A+B=B+A$. Associativity is harder to show, but it is just a special case of showing associativity in the general group law.

Acknowledgments/References

I’ve referred to...