MA434, Spring 2020 — Midterm Solutions

These solutions vary in detail. I decided not to give too much detail for problems that seemed easy or were basically computations. I gave more detail for the more theoretical problems.

1. [20 points] Suppose $f(X, Y, Z)$ is a homogeneous polynomial of degree n with coefficients in $\mathbb{R}$, so that we have $f(tX, tY, tZ) = t^n f(X, Y, Z)$. Show that

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

(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 pointing out that this shows that if a point satisfies

$$\frac{\partial f}{\partial X}(P) = \frac{\partial f}{\partial Y}(P) = \frac{\partial f}{\partial Z}(P) = 0,$$

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

The direct proof: let S_n be the vector space of all homogeneous polynomials of degree n in $k[X, Y, Z]$. Notice first that both sides are the result of linear transformations $S_n \longrightarrow S_n$ (this is obvious for multiplication by n, and it follows from the linearity of the derivative for the other transformation. So it suffices to show that they are equal on a basis. The basis of S_n is all monomials $X^iY^jZ^k$ with $i+j+k = n$. On the left, we just get $nX^iY^jZ^k$. On the right, we get

$$X(iX^{i-1}Y^jZ^k) + Y(jX^iY^{j-1}Z^k) + Z(kX^iY^jZ^{k-1}) = (i+j+k)X^iY^jZ^k = nZ^iY^jZ^k,$$

which proves the equality.

The calculus proof: Notice first that if we differentiate the equation $f(tX, tY, tZ) = t^n f(X, Y, Z)$ with respect to X we get

$$t\frac{\partial f}{\partial X}(tX, tY, tZ) = t^n \frac{\partial f}{\partial X}(X, Y, Z);$$

cancelling t shows that $\frac{\partial f}{\partial X}$ is homogeneous of degree $n - 1$. The same is true for the other partial derivatives.

For the next step, let's simplify notation by writing $P = (X, Y, Z)$ and $tP = (tZ, tY, tZ)$. Differentiating $f(tX, tY, tZ) = t^n f(X, Y, Z)$ with respect to t gives

$$X\frac{\partial f}{\partial X}(tP) + Y\frac{\partial f}{\partial Y}(tP) + Z\frac{\partial f}{\partial Z}(tP) = nt^{n-1}f(X, Y, Z).$$

Using the homogeneity and cancelling out t^{n-1} on both sides gives the result.

2. [20 **points**] The Proposition in section 1.13 of *Undergraduate Algebraic Geometry* says that in a pencil of conics *containing at least one non-degenerate 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.

It's enough to start with two (different) degenerate conics. For example, let $F = X^2 - Y^2$ and let $G = 2XY$, so that $F = 0$ gives the lines $y = \pm x$ and $G = 0$ gives the two axes in the affine plane. Then $uF + vG = uX^2 + 2vXY + uY^2$. When $u \neq 0$ the resulting conic is $X^2 + 2tXY + Y^2 = 0$, which is two lines crossing at the origin when $t^2 > 1$ and empty when $t^2 < 1$.

From the matrix point of view it's even clearer. We have

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

so $uA + vB$ will always have row of zeros.

3. [30 **points**] The Proposition in section 1.13 of *Undergraduate Algebraic Geometry* says that in a pencil of conics containing at least one non-degenerate conic there will be at most 3 degenerate conics, and if $k = \mathbb{R}$ *there will always be at least one degenerate conic*. In the examples we played with there were always at least two degenerate conics. Find an example with exactly one.

I vastly overthunk this one. Here's what I did. Each conic corresponds to a symmetric matrix, so let A and B be real symmetric matrices. Our goal is to choose them so that the equation $\det(uA + vB) = 0$ has a single real root $[u : v]$ (up to scaling, of course). If I make sure to choose A invertible, then setting $v = 0$ never gives a root, since $\det(uA) \neq 0$. So I can factor out v to make the equation be $v^3 \det(\frac{u}{v}A + B) = 0$. Setting $t = u/v$, I'm down to finding two symmetric matrices such that $\det(At + B) + 0$ has only one real root.

But I chose A to be invertible, so I can factor it out too: $\det(At+B) = \det(A)\det(It+A^{-1}B)$. Since $\det(A) \neq 0$, what I need is to make sure that $\det(It + A^{-1}B) = 0$ has a single real root, which boils down to making sure that $A^{-1}B$ has only one real eigenvalue.

There are lots of matrices with only one real eigenvalue; something like this will work:

$$A^{-1}B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix}.$$

So I set out to find two symmetric matrices that satisfied that equation (or something close). I ended up with

$$F = 2XY + Y^2 - 2X + 4Y - 1, \qquad G = 2XY - 2Y^2 + 2Y + 2,$$

and checked that $tF + G = 0$ is singular only when $t = -1/2$.

Here's the code for a pretty picture of the pencil:

```
var('x y t')
Q(t)=t*(2*x*y + y^2 - 2*x + 4*y - 1)+(2*x*y - 2*y^2 + 2*y + 2)
G=implicit_plot(2*x*y + y^2 - 2*x + 4*y - 1==0,(x,-10,10),(y,-10,10))
for c in range(-5,5):
    G += implicit_plot(Q(c/2)==0,(x,-10,10),(y,-10,10),
        color=sorted(colors)[10*c%147])
show(G)
```

Maybe you found a simpler example.

4. [20 **points**] Let $f(x, y)$ be a polynomial in two variables with coefficients in $\mathbb{R}$ such that $f(0, 0) = 0$. We want to look at the point $P = (0, 0)$ on the affine curve C defined by $f(x, y) = 0$.

a. The line $y = 0$ passes through P. Under what condition on f is it the tangent line to C at P?

Write the polynomial in order of increasing degree:

$$f(x, y) = a + bx + cy + dx^2 + exy + fy^2 + \dots$$

The fact that $f(0, 0) = 0$ tells us $a = 0$. Plugging in $y = 0$ gives

$$f(x, 0) = bx + dx^2 + \dots,$$

So $f(x, 0) = 0$ has a double root at $x = 0$ if and only if $b = 0$.

For a fancier version, notice that $b = \frac{\partial f}{\partial x}(0, 0)$.

b. Under what conditions on f is the point P an inflection point with tangent line $y = 0$?

Exactly as before, the condition becomes $b = d = 0$, that is, we need both

$$\frac{\partial f}{\partial x}(0, 0) = 0 \qquad \text{and} \qquad \frac{\partial^2 f}{\partial x^2}(0, 0) = 0.$$

Can you generalize to other lines? Other points?

Generalizing to other points is easy: take the Taylor expansion around that point instead.

For other lines, plug in $y = mx$ and try to find the right condition on the partial derivatives. It's not hard, but can you write the condition in a nice way?

5. [20 **points**] 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

$$U = \{[u : v] \in \mathbb{P}^1(k) \mid v \neq 0\}$$

and

$$V = \{[u : v] \in \mathbb{P}^1(k) \mid u \neq 0\}.$$

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

   This should have been very easy. The inverse function sends t to $[t : 1]$.

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

   Identical to the first one, except now send s to $[1 : s]$.

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

   This is easy too: $f(g^{-1}(t)) = 1/t$, because when $t \neq 0$ we have $[t : 1] = [1 : 1/t]$.

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

   It's all said already... A few pictures might clarify what is going on. We can think as $t = u/v$ as a local coordinate on the set U and $s = v/u$ as a local coordinate on the set V. (Both U and V are just lines, so one-dimensional.) At any point that belongs to both sets, the two coordinates are related by $s = 1/t$.

6. [20 points] 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.)

$P = (0, 1)$, $2P = (\frac{1}{4}, -\frac{9}{8})$, $3P = (72, 611)$, $4P = (-\frac{287}{1296}, \frac{40879}{46656})$. I did it with *Sage*, of course. To set up the curve the command is `E=EllipticCurve([1,1])`. Then you can set `P=E(0,1)` and ask for `2*P`, etc.

One can show that the point P is of infinite order, i.e., we have $nP \neq 0$ for all n. One way to prove this is to prove that the denominators that appear in points of finite order can be determined.

I presume it's possible to do this by hand (I managed to do $2P$ by hand), but the equations are going to get more and more complicated.

If classrooms were 3-tori, looking out the windows would mean looking at the board. – Chris Tuffley, Mathcamp 2004

7. [20 points] The curve $y^2 = x^3 + x + 1$ also makes sense over $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$. Of course, in that case there will be finitely many points on the curve.

a. Find all the points of E in $\mathbb{P}^2(\mathbb{F}_7)$. (Don't forget the point at infinity.)

   The most straighforward way (short of just asking *Sage*) is to compute $x^3 + x + 1$ for $x = 0, 1, 2, \dots, 6$ and check which of the answers are squares mod 7. There are five points: 0, $(0, 1)$, $(0, 6)$ $(2, 2)$, $(2, 5)$.

b. The set of all points with coordinates in $\mathbb{F}_7$ is a group. What group is it?

   Of course, any group of order 5 is cyclic, and indeed any nonzero element will be a generator. If we take $P = (0, 1)$ as before, then $2P = (2, 5)$, $3P = (2, 2)$ $4P = (0, 6)$, $5P = 0$. (The only one that needs to be computed is $2P$, since $3P = -2P$ and $4P = -P$ can be computed just by changing the sign of the y-coordinate.)

   Challenge: compare $2P$, $3P$, and $4P$ over $\mathbb{Q}$, which you found above, with the results over $\mathbb{F}_7$. Do they agree?

8. [20 points] (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 $\tilde{g}(x) = ag(x) \in R[x]$, $\tilde{h}(x) = \frac{1}{a}h(x) \in R[x]$, and so $f(x) = \tilde{g}(x)\tilde{h}(x)$ is a factorization in $R[x]$.

Writing (x) after every polynomial is a pain, so I won't do it. Below, f, g, h always stand for polynomials in x.

Given a polynomial $g \in K[x]$, there is clearly an element $r \in R$ such that $rg \in R[x]$ (for example, we could take r to be the product of all the denominators of the coefficients of g). For every polynomial $f \in R[x]$, if there is an irreducible element that divides all the coefficients we can factor it out to get $f = \pi f_1$. We can clearly keep doing this until the coefficients do not share any irreducible factors. So:

- A polynomial $f \in R[x]$ is *primitive* if its coefficients do not have an irreducible common factor.

- If $f \in K[x]$ is a polynomial, there exists $c \in K$ such that $f = cf_1$, $f_1 \in R[x]$, f_1 primitive. Any two such c differ by a unit in R.

  (To prove this, first clear denominators to get $rf \in R[x]$. Then consider the factorizations of the coefficients of rf and let d be the product of their common irreducible factors. Then $c = d/r$ will work.)

- The number c in the previous item is called the *content* of f. It is defined up to multiplication by a unit in R. (This is because any non-unit is a product of irreducibles.)

Lemma: *If* f *and* g *are primitive, so is* fg.

Proof: We prove the contrapositive. Suppose fg is not primitive, and let $\pi \in R$ be an irreducible element that divides all of its coefficients. Let $D = R/R\pi$. Since π is irreducible and R is a UFD, π is prime, so $R\pi$ is a prime ideal, so D is a domain, which means $D[x]$ is a domain as well. We have $\overline{fg} = 0$ in $D[x]$; this forces either $\overline{f} = 0$ or $\overline{g} = 0$ in $D[x]$. We can suppose, without loss of generality, that $\overline{f}$=0 (otherwise just switch f and g). But $\overline{f} = 0$ in $D[x]$ if and only if all the coefficients of f are divisible by π, so f is not primitive.

Proof of the theorem: Now suppose $f \in R[x]$, $g, h \in K[x]$, $f = gh$. Write $f = cf_1$, $g = ag_1$, $h = dh_1$ with $f_1, g_1, h_1 \in R[x]$ all primitive. Notice that $c \in R$ but all we know is that $d, a \in K$. Then $cf_1 = adg_1h_1$. Since g_1h_1 and f_1 are primitive, it follows that $c = adu$ for some invertible $u \in R^\times$. Hence $adu = c \in R$. So

$$f = cf_1 = (adu)(gh) = (ag)(udh) = (g_1)(uh_1) = \tilde{g}\tilde{h}.$$

Since $\tilde{g} = g_1 \in R[x]$ and $\tilde{h} = uh_1 \in R[x]$, we are done. Notice that $f = gh = \tilde{g}\tilde{h}$ implies that $uda = 1$, so $ud = 1/a$.

9. **[30 points]** Let V be the variety in $\mathbb{A}^3(k)$ defined by the equations $xy = 0$, $xz = 0$, $yz = 0$ (points on V are those for which all three equations hold).

a. Describe V. In particular, explain why it is a curve in $\mathbb{A}^3(k)$.

V consists of three lines. Specifically, it is the three axes in $\mathbb{A}^3(k)$. Since lines are one-dimensional, this is a curve, a degenerate cubic.

b. Show that the set

$$I = \{f \in k[x, y, z] \mid f(P) = 0 \text{ for all } P \in V\}$$

of polynomials that vanish on V is an ideal in $k[x, y, z]$.

Easy and pretty much done in class. This is just $I(V)$.

c. Show that I is generated by xy, xz, yz.

We already know that $xy, xz, yz \in I$. So what we need to prove is that if a polynomial vanishes on all points on the three axes then it must be a linear combination of these three. So take a polynomial $f(x, y, z)$ and suppose it vanishes on V. Notice first that $f(0, 0, 0) = 0$ tells us that there is no degree zero coefficient.

Knowing $f(x, 0, 0) = 0$ for all x shows that there is no term of the form ax^k. Similarly there is no term by^n or cz^m. So all the terms in f involve at least two of the variables. Splitting the terms into those that involve x and y, then those that involve x and z, then those that involve y and z, we get

$$f(x, y, z) = f_1(x, y, z)xy + f_2(x, y, x)xz + f_3(x, y, z)yz,$$

so I is generated by xy, xz, yz.

Notice that the decomposition is far from unique, because terms involving all three variables can be put into any group.

d. Intuitively, we would expect that a curve in $\mathbb{A}^3(k)$ is determined by two polynomial equations. Do there exist polynomials f and g such that I is generated by f and g?

No, but this may be the hardest part to prove. Here's a rough-and-ready attempt.

Some possibilities are easy to eliminate: I does not contain any polynomials of degree one, but it does contain polynomials of degree two. So if it could be generated by two polynomials at least one must be of degree two.

If only one generator is of degree two, all three of xy, xz and yz would be scalar multiples of that generator, which is impossible since $\gcd(xy, xz, yz) = 1$. So there must be two generators of degree two; call them g_1 and g_2. By the discussion above, each must look like

$$g_1 = c_1xy + c_2xz + c_3yz \text{ and } g_2 = d_1xy + d_2xz + d_3yz.$$

Since $\deg(xy) = 2$ we must have $xy = \alpha g_1 + \beta g_2$ with $\alpha, \beta \in k$, which gives three equations in the two unknowns α and β. For those to have a solution imposes a constraint on the c_i and d_i. Work that out, then do the same for the other monomials xz and yz to get a contradiction.

Maybe there is an easier way to do it. Do you know how?

10. [20 **points**] Let C be the curve in $\mathbb{P}^2$ whose affine equation is $y^2 = x^3 + x^2$. This is the nodal cubic we studied in section 2.1. Show that the line $y = tx$ has a double intersection with C at $(0, 0)$ and find the third point of intersection. Check that this gives the parametrization in 2.1. What happens when $t = \pm 1$?

Plugging $y = tx$ into $y^2 = x^3 + x^2$ gives $t^2x^2 = x^3 + x^2$, which has at least a double zero at $(0, 0)$. It is a triple zero ($x^3 = 0$) when $t^2 = 1$.

So we see that when $t \neq \pm 1$, the line $y = tx$ always has a double intersection with the curve, and so will intersect the curve at one more point, which we cand find by cancelling x^2 to get $x = t^2 - 1$. Then $y = tx = t^3 - t$, which gives the parametrization we want: except for $t = \pm 1$ the function $t \mapsto (t^2 - 1, t^3 - t)$ is a bijection.

When $t = \pm 1$ the line is actually tangent to one of the branches of the curve going through $(0, 0)$, which explains the triple intersection: the tangent means a double intersection with one branch, and then you need to count the other branch as well. Unsurprisingly, the parametrization is 2-to-1 at the double point.

11. [20 **points**] With C as in the previous problem, let $C(k)$ be the set of points on C with coefficients in k (including the point at infinity), and let $C'(k) = C(k) - \{(0, 0)\}$.

(So $C'(k)$ is the set of points on 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 $C(k)$ and let $P = (0, 0)$. Let L be the line through A and P. What is the third intersection of L and C?

Since any line has at least a double intersection with P and L goes through A and P, the "third" intersection point will be P.

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

The previous item shows that we would have $A + P = P$ for all A, which is impossible in a group. (It would imply $A = 0$ for all A, for example.) The point P "wants" to behave like 0 under multiplication.

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

Since P always counts at least twice, the line that cuts C twice, at A and B, cannot go through P, because that would give four intersection points.

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

The proofs we did never required the cubic to be nonsingular, so everything still works.

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

It's worth a try, though! The isomorphism can't send t to t, since the identity is the point at infinity and that has to correspond to 1 in $k^\times$. So the first thing to do is to change parameters somehow. We want the new parameter to be nonzero at the nonsingular points, i.e., it should be zero only when $t = 0$. Does something like $s = t/(t-1)$ work?

12. [30 **points**] Suppose $f, g \in k[x, y]$ are polynomials in two variables with coefficients in a field k. Suppose $f(x, y)$ is irreducible and does not divide $g(x, y)$. Show that there are at most finitely many solutions to $f(x, y) = g(x, y) = 0$.

Since $f(x, y)$ is not a constant, we may suppose without loss of generality that x appears in $f(x, y)$ with positive degree. (Otherwise switch x and y.)

We want to consider $f \in k(y)[x]$. We know the x-degree of f is not zero. By Gauss's Lemma, f is still irreducible as an element of this ring (because we know $k[y]$ is a UFD and $k(y)$ is its field of fractions). In particular, the ideal in $k(y)[x]$ generated by f is maximal.

Suppose we had $g = fh$ with $h \in k(y)[x]$. Using Gauss's Lemma again we get $g = f\tilde{h}$ with $\tilde{h} \in k[y, x]$, and then f divides g in $k[x, y]$. So f cannot be a divisor of g in $k[x, y]$.

Consider the ideal in $k(y)[x]$ generated by f and g. It clearly contains all the multiples of f, but it also contains g, so it is strictly bigger than the ideal generated by f. Since the latter is maximal, the ideal generated by f and g must be all of $k(y)[x]$. In particular, we can write $1 \in k(y)[x]$ as a linear combination: $rf + sg = 1$ for some $r, s \in k(y)[x]$. Of course, r and s may have denominators that are polynomials in y. Clearing denominators, we end up with

$$d(x,y)f(x,y) + c(x,y)g(x,y) = h(y).$$

Hence any solution to $f(x,y) = g(x,y) = 0$ gives a solution to $h(y) = 0$. Polynomials in one variable have finitely many roots, so we have finitely many choices for y. If we fix a value for y the equation $f(x,y) = 0$ becomes a polynomial in x, with again only finitely many roots. So we have finitely many choices for y, and for each y finitely many choices for x, so finitely many solutions in all.

Notice that we do *not* need to assume k is infinite anywhere, but the result seems silly if k is finite, since there are only finitely many pairs (x,y). But the claims about the number of roots are true even if we pass to the algebraic closure of k. So, for example, if $k = \mathbb{F}_p$ we can still conclude that there are finitely many common points even if we go to $\overline{\mathbb{F}}_p$.