Lecture notes for PM 464/764 – Week Twelve

David McKinnon
Department of Pure Mathematics
University of Waterloo

Spring 2021

1 Playing with $\mathbf{Pic}^0(C)$

Now let's switch gears, and try to use all this Picard stuff to define a way of adding two points on a curve. That is, if P and Q are two points on a curve C, we want to find a point R such that $P+Q = R$. If we try to use divisors to do this in the obvious way, we're going to run into trouble, because $P + Q$ is a divisor of degree 2, and R is a divisor of degree 1, and there's no way those two divisors can be equal, even up to linear equivalence. So we'll try a different idea.

Let C be a smooth curve, and let O be any point on C. We can define a function from C to $\mathrm{Pic}^0(C)$ as follows:

$$\phi_C(P) = |P - O|$$

This solves the degree problem – $\phi_C(P)$ is always a divisor of degree 0. So what we want now is to define an addition on C by setting:

$$P + Q = R \text{ if and only if } \phi_C(P) + \phi_C(Q) = \phi_C(R)$$

So what we're hoping for is that for any P and Q on C, we can find a unique point R such that:

$$(P - O) + (Q - O) \equiv (R - O)$$

In general, this will not be possible for most curves C. But if it is, the map ϕ_C will provide a means for defining an addition law on C.

So let's try looking for such curves C. If C is a curve of degree 1 in the plane, then it's a line. In this case, the map ϕ_C is trivial, for the simple reason that $\mathrm{Pic}^0(C)$ is a single equivalence class. Let's prove that now.

Theorem 1.1. *Let C be a line in the plane. Then $Pic^0(C)$ has exactly one element.*

Proof: Say we could prove that if P and Q are any two points on C, then $P \equiv Q$. Then if D is any divisor of degree 0, we can write $D = (P_1 - Q_1) + (P_2 - Q_2) + \ldots + (P_r - Q_r) \equiv 0$, since each $P_i - Q_i \equiv 0$, and we'd have proven that $\mathrm{Pic}^0(C)$ contains only one equivalence class.

So, let P and Q be any two points on C. Let L be any line through P (except C), and let L' be any line through Q (except C). Then we have $\mathrm{div}(L) = P$ and $\mathrm{div}(L') = Q$, so $P - Q = \mathrm{div}(L) - \mathrm{div}(L') = \mathrm{div}(L/L')$. Since L and L' have the same degree, L/L' is a rational function on C, and hence is linearly equivalent to 0 by definition. Thus, $P \equiv Q$, as desired.

♣

This is no good for defining an addition, because every point is linearly equivalent to every other point – the "addition" will be trivial.

Darn. Well, let's try the next degree up. Another disappointment:

Theorem 1.2. *Let C be a smooth plane curve of degree 2. Then $Pic^0(C)$ has exactly one element.*

Proof: As before, it suffices to show that any two points P and Q are linearly equivalent. Let L be any line through P but not Q. Then by Bezout's Theorem, $\mathrm{div}(L) = P + R$ for some point R on C (possibly $R = P$ – that's OK). Let L' be the line through Q and R, so $\mathrm{div}(L') = Q + R$. Then we can define a rational function L/L' with:

$$\mathrm{div}(L/L') = P + R - Q - R = P - Q$$

and so $P \equiv Q$, as desired. ♣

So for curves of degree 1 and 2 both, the map ϕ_C is trivial for the simple reason that $\mathrm{Pic}^0(C)$ is a one-element set. At this point, we should remark that all smooth plane curves of degree 1 and 2 are isomorphic to $\mathbb{P}^1$. In fact, we can prove a stronger theorem:

Theorem 1.3. *Let C be a smooth curve with two points P and Q satisfying $P \equiv Q$. Then C is isomorphic to $\mathbb{P}^1$.*

Proof: We proved this on the homework. ♣

So much for the first two cases. In the next section, we'll finally find some curves for which Pic^0 is not trivial.

2 Smooth Plane Cubics

Let's now turn our attention to the case $\deg(C) = 3$. Before we start analyzing $\mathrm{Pic}^0(C)$, let's perform some coordinate changes on our curve, so that the equation defining C will look presentable.

Choose a point $O \in C$. Apply a change of coordinates so that O is mapped to the point $[1 : 0 : 0]$, and the tangent line L to O is mapped to the line $z = 0$. Write $\mathrm{div}(L) = 2O + P$ for some point $P \in C$, and let L' be the tangent line to C at P. Keeping O and L fixed, apply another change of coordinates to move L' to the line $x = 0$. (This might not be possible if $P = O$ and $L = L'$, which happens when $\mathrm{div}(L) = 3O$. If this happens, we say that O is a flex of C, and you have to go through a similar but separate procedure. We'll assume O is not a flex of C for now.)

Let's look at what our equation looks like now. In principle, we have a homogeneous cubic equation $f(x, y, z) = 0$ for C:

$$c_1x^3+c_2x^2y+c_3x^2z+c_4xy^2+c_5xyz+c_6xz^2+c_7y^3+c_8y^2z+c_9yz^2+c_{10}z^3 = 0$$

We know that C contains the points $O = [1 : 0 : 0]$ and $P = [0 : 1 : 0]$ (remember that P is the intersection of the lines $x = 0$ and $z = 0$), so $c_1 = c_7 = 0$. We further know that $z = 0$ is the tangent line at O and $x = 0$ is the tangent line P, so we can

compute some values of partial derivatives:

$$\begin{aligned} f_x(1,0,0) &= 0 \\ f_y(1,0,0) &= c_2 = 0 \\ f_z(1,0,0) &= c_3 \neq 0 \\ f_x(0,1,0) &= c_4 \neq 0 \\ f_y(0,1,0) &= 0 \\ f_z(0,1,0) &= c_8 = 0 \end{aligned}$$

If we divide through by c_4 and relabel our variables, our equation for C now looks like:

$$xy^2 + axyz + byz^2 + cx^2z + dxz^2 + ez^3 = 0$$

for some constants a through e. Multiplying through by x gives:

$$(xy)^2 + ax(xy)z + b(xy)z^2 + cx^3z + dx^2z^2 + exz^3 = 0$$

We now restrict to the affine piece $z = 1$ and apply the birational transformation $(x, y) \mapsto (x, y/x)$. Rehomogenizing gives:

$$y^2z + axyz + byz^2 + cx^3 + dx^2z + exz^2 = 0$$

However, this is all contingent on the fact that the tangent line L to C at O is not a flex. If it is a flex, then this procedure remains essentially the same, except that the point $[0 : 1 : 0]$ might not lie on the curve C. The upshot of this is that we have to add a z^3 term to the previous equation. Of course, this term isn't really necessary, since over an algebraically closed field we can always do a linear change of coordinates in x to get rid of it, but later on we will be dealing with fields that are not algebraically closed, so we'll leave the term in for now.

Thus, with a trivial rearrangement, we have put our cubic C into the following standard form:

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

(The reason why a_5 does not appear, but a_4 and a_6 both do is stylistic: if you imagine that x has weight 2 and y has weight 3, then adding the index of the coefficient to the sum of the weights of each term always gives you 6.)

This form of equation is called Weierstrass form. We will largely make use of the $z = 1$ affine piece of this curve:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Remark: We can make a change of coordinates $x \mapsto x$, $z \mapsto z$ and $y \mapsto y - (a_1xz - a_3z^2)/2$, to get:

$$y^2z = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

We can make a further change of coordinates $x \mapsto x - (a_2/3)z$, $y \mapsto y$, and $z \mapsto z$ to get:

$$y^2z = x^3 + axz^2 + bz^3$$

where the a and b are the standard labels for the reduced Weierstrass form of C. In these notes, however, we'll stick with the general Weierstrass form, because in characteristic 2 these changes of coordinates don't work, and characteristic 2 is particularly useful for cryptographic applications. (In characteristic 2, there are a lot of zeroes and ones. Computers like that.)

Thus, let's assume that C is given in Weierstrass form, as above. We can see that the point $[0 : 1 : 0]$ lies on C – call this

point O. (It is the image of the original point O under all the various transformations we performed on C before.) Note that the tangent line to C at O is the line $z = 0$, and that the only intersection point of $z = 0$ with C is O (if $z = 0$ on C, then $x^3 = 0$). Therefore, $z = 0$ is a flex of C, so $\mathrm{div}(L) = 3O$. (The coefficient has to be 3 because of Bezout's Theorem.)

Back to $\mathrm{Pic}^0(C)$. We are now in a position to prove that ϕ_C is surjective. To do this, we need to show that an arbitrary divisor D of degree 0 is linearly equivalent to $\phi_C(P) = P - O$ for some point $P \in C$. Thus, write:

$$D = a_1 P_1 + \ldots + a_n P_n$$

with $a_1 + \ldots + a_n = 0$. Then we can rewrite:

$$D = a_1(P_1 - O) + \ldots + a_n(P_n - O)$$

We want to show that D is linearly equivalent to $P - O$ for some point P. Since the a_i are integers, it suffices to prove the following two facts:

- For any P and Q on C, that there is some $R \in C$ such that $|P - O| + |Q - O| = |R - O|$.
- For any $P \in C$, that there is some $R \in C$ such that $-|P - O| = |R - O|$.

A simple induction will then show that D is linearly equivalent to $P - O$ for some point $P \in C$.

Both of these facts will follow from the following lemma, which will also be very useful for calculations later on:

Lemma 2.1. *Let L be a line in $\mathbb{P}^2$. Then if div$(L) = P+Q+R$, then $|P-O|+|Q-O|+|R-O| = |0|$; that is, there is a rational function $\alpha \in K(C)$ satisfying div$(\alpha) = P + Q + R - 3O$.*

Proof: Say L is a line with $\mathrm{div}(L) = P + Q + R$ for points P, Q, and R on C. (Note that P, Q, and R might not all be different.) Let T be the line $z = 0$. Then $\mathrm{div}(T) = 3O$, so define $\alpha = L/T$. We have:

$$\mathrm{div}(\alpha) = \mathrm{div}(L) - \mathrm{div}(T) = P + Q + R - 3O$$

and hence the lemma follows. ♣

Let's now prove those two facts. We'll prove the second one first. Let $P \in C$ be any point, and let L be the line joining P to O. (If $P = O$, let L be the tangent line $z = 0$ to C at P.) Then we have:

$$\mathrm{div}(L) = P + O + R$$

for some point $R \in C$. By the lemma, that means:

$$|P - O| + |O - O| + |R - O| = |0|$$

and hence $-|P - O| = |R - O|$, as desired.

Now for the first fact. Let P and Q be two points on C (not necessarily different), and let L be the line joining P to Q. (If $P = Q$, let L be the tangent line to C at P.) Then we have:

$$\mathrm{div}(L) = P + Q + R$$

for some point $R \in C$. By the lemma, that means:

$$|P - O| + |Q - O| + |R - O| = |0|$$

and hence that $|P - O| + |Q - O| = -|R - O| = |R' - O|$ for some point $R' \in C$.

Thus, we have now proven that any element $D \in \mathrm{Pic}^0(C)$ is linearly equivalent to $|P - O|$ for some point $P \in C$. We can use this to define an addition on C: if P and Q are two points on C, define $P + Q$ to be the point R satisfying $|R - O| = |P - O| + |Q - O|$ – the existence of this point is guaranteed by the preceding discussion.

The only problem with this definition is that the point R might not be unique. For example, if C were birational to $\mathbb{P}^1$ (it isn't), then R would be birational to every other point of C, and therefore every point of C would be a candidate for $P+Q$ according to the preceding criterion! Luckily, this doesn't happen:

Theorem 2.2. *The map ϕ_C is injective. That is, if $|P - O| = |Q - O|$, then $P = Q$.*

Proof: Assume that $\phi_C(P) = \phi_C(Q)$. Then we have $|P - O| = |Q - O|$, in which case $P \equiv Q$. Thus, we can find plane curves g and h of the same degree satisfying:

$$P + \mathrm{div}(g) = Q + \mathrm{div}(h)$$

By changing coordinates, we may assume that g and h do not meet f at infinity – that is, that $g \cap f \cap z = h \cap f \cap z = \emptyset$. Let ℓ be any line through P which does not meet h at infinity. Then we have:

$$\mathrm{div}(\ell) = P + R_1 + R_2$$

for some points $R_i \in C$, not necessarily different from P or Q.

We compute:

$$\begin{aligned}\operatorname{div}(g\ell) &= \operatorname{div}(g) + \operatorname{div}(\ell) \\ &= Q - P + \operatorname{div}(h) + P + R_1 + R_2 \\ &= \operatorname{div}(h) + (Q + R_1 + R_2)\end{aligned}$$

Thus, we have $\operatorname{div}(g\ell) \geq \operatorname{div}(h)$, which means that for every point $R \in C$, we have $\operatorname{ord}_R(g\ell) \geq \operatorname{ord}_R(h)$.

Fix any point $R \in C$, and let t be a uniformizer for $\mathcal{O}_R(C)$. After dehomogenizing g, ℓ, and h to G, L, and H, respectively, we can write $GL = ut^n$ and $H = vt^m$ for units u and v of $\mathcal{O}_R(C)$, with $n \geq m$. Thus:

$$GL = uv^{-1}t^{n-m}H$$

as elements of $\mathcal{O}_R(C)$. Note that $uv^{-1}t^{n-m} \in \mathcal{O}_R(C)$ because $n - m \geq 0$. Lifting this to $O_R(\mathbb{A}^2)$, we get:

$$GL = AF + BH$$

where A and B are rational functions in X and Y, and $F(X, Y) = f(X, Y, 1)$ is the dehomogenization of f. (Recall that $f(x, y, z) = 0$ is the defining equation for C.)

It would be nice if we could change our rational functions A and B into polynomials. So let's try to do that.

By hypothesis, g and ℓ do not meet h at infinity, so *a fortiori*, $g\ell$, f, and h also do not simultaneously meet at infinity. From the preceding discussion, we know that $GL = 0$ as an element of $\mathcal{O}_R(\mathbb{A}^2)/(F, H)$, for every point $R \in \mathbb{A}^2$. We know that:

$$\prod_{R \in F \cap H} \mathcal{O}_R(\mathbb{A}^2)/(F, H) \cong \mathbb{C}[X, Y]/(F, H)$$

Since $GL = 0$ in all the rings in the product on the left, it follows that $GL = 0$ in $\mathbb{C}[X, Y]/(F, H)$, and hence we have:

$$GL = A'F + B'H$$

for polynomials A' and B' in two variables. Rehomogenizing, we find:

$$z^r g\ell = a'f + b'h$$

for some nonnegative integer r. (We have to rehomogenize the whole equation, not just each polynomial individually. In particular, a' and b' might differ from the homogenizations of A' and B' by a power of z as well ... but that doesn't matter.)

Now notice that z is not a zero divisor in $\mathbb{C}[x, y, z]/(f, h)$, because $V(f, h, z) = \emptyset$ and so we get $(1) = (f, h, z) = (z)$ in $\mathbb{C}[x, y, z]/(f, h)$. (Note that we're thinking of f and g as defining algebraic subsets of $\mathbb{A}^3$ here, not $\mathbb{P}^2$.)

Thus, multiplication by z is injective on $\mathbb{C}[x, y, z]/(f, h)$, so we can find polynomials a'' and b'' satisfying:

$$g\ell = a''f + b''h$$

We've got our polynomials! Now we can reduce modulo f once more, and write:

$$\begin{aligned} \operatorname{div}(b'') &= \operatorname{div}(g) + \operatorname{div}(\ell) - \operatorname{div}(h) \\ &= Q - P + \operatorname{div}(\ell) \\ &= Q + R_1 + R_2 \end{aligned}$$

Since $\operatorname{div}(b'')$ has degree 3, it follows that b'' is a line. In fact, it's the same line as ℓ, since it passes through R_1 and R_2 – even if $R_1 = R_2$, ℓ and b'' both have to be the tangent line to C at

$R_1 = R_2$. But if ℓ and b'' are the same line, then they have the same divisor, so $P + R_1 + R_2 = Q + R_1 + R_2$, and hence $P = Q$.

♣

At this point, we have shown that ϕ_C is a bijection between C and $\mathrm{Pic}^0(C)$, so we can use this bijection to define an addition law on C, by defining $P+Q$ to be the unique point R of C which satisfies $\phi_C(R) = \phi_C(P) + \phi_C(Q)$. Let's now try to answer the question: given two points P and Q on C, how can we compute the point $P + Q$?

To do this, we'll use Lemma 2.1. Let P and Q be points on C, possibly the same point, and let L be the line joining them. (If $P = Q$, let L be the tangent line to C at P.) We can write

$$\mathrm{div}(L) = P + Q + R$$

where R is the third point of intersection of L with C. By Lemma 2.1, it follows that $\phi_C(P) + \phi_C(Q) + \phi_C(R) = |0|$ in $\mathrm{Pic}^0(C)$, or in other words, $P + Q + R = O$.

So this R isn't quite what we want, because $R = -P - Q$. If we compute $-R$, we'll be in business. Thus, let L' be the line connecting R to O (tangent line if $R = O$). Then:

$$\mathrm{div}(L') = R + O + R'$$

where R' is the third intersection point of L' with C. By Lemma 2.1, we have $R + O + R' = O$, or $R' = -R = P + Q$. So we've found the point we want!

Let's do an example. Say C is the curve $y^2z = x^3 + 3xz^2$ over the field of complex numbers, and let $P = [0 : 0 : 1]$, $Q = [1 : 2 : 1]$. The line L through P and Q is the line $2x - y = 0$,

and if we plug this into the equation defining C, we get:

$$(2x)^2 z = x^3 + 3xz^2$$
$$x^3 + 4x^2 z + 3xz^2 = 0$$

This equation is easy enough to factor, but there's a shortcut which is often very helpful. Dehomogenizing the equation gives:

$$x^3 - 4x^2 + 3x = 0$$

This equation has (with multiplicity) three roots, and their sum is $-b/a$, where a is the leading coefficient and b is the coefficient of x^2. But we already know two of the roots of this equation, corresponding to the values of x/z for the points P and Q which are, after all, two of the three intersection points of L and C. Thus, if α is the mysterious third root, we have:

$$\alpha + 0 + 1 = 4$$

so $\alpha = 3$ and hence our third point $R = [a : b : c]$ satisfies $a/c = 3$. Normalizing $c = 1$ gives $a = 3$, and $b = 2a = 6$ (R lies on the line $y = 2x$), so our third point is $R = [3 : 6 : 1]$.

There's one step to go: we have to calculate $-R$. The line joining $R = [3 : 6 : 1]$ to $O = [0 : 1 : 0]$ has equation $x - 3z = 0$. Plugging this into the equation defining C gives:

$$y^2 z = (3z)^3 + 3(3z)z^2$$
$$y^2 z = 36z^3$$

which gives $z = 0$ or $y = \pm 6z$. Since $z = 0$ corresponds to O and $y = 6z$ corresponds to R, it follows that $y = -6z$ corresponds to $-R = P + Q$. Thus, noting along the way that $x = 3z$ and normalizing $z = 1$, we find that $P + Q$ is the point $[3 : -6 : 1]$.

As a further example, let's compute $2Q = Q + Q$, where $Q = [1 : 2 : 1]$ is as above. Following the program outlined above, we let L be the tangent line to C at Q, compute the third point R of intersection of C and L, and then compute $-R$ as the third point of intersection of C and the line L' joining R to O.

The tangent line to C at Q is the line $3x - 2y + z = 0$. Plugging this into the equation defining C gives:

$$y^2(2y - 3x) = x^3 + 3x(2y - 3x)^2$$
$$2y^3 - 15y^2x + 36yx^2 - x^3 = 0$$

Normalizing to $x = 1$ (or, more accurately, dividing through by x and relabeling $y = y/x$), we get:

$$2y^3 - 15y^2 + 36y - 1 = 0$$

Using the nifty trick from the previous example, we note that $y = 2$ is a double root of this polynomial (since the line is tangent to the curve at Q), so if α is the mysterious third root, we have:

$$2 + 2 + \alpha = 15/2$$

and hence $\alpha = 7/2$. Thus, we get $x = 1$, $y = 7/2$, and $z = 2y - 3x = 4$, so $-2Q = [2 : 7 : 8]$. To compute $2Q$, we need to find $-[2 : 7 : 8]$.

The line joining $[2 : 7 : 8]$ to $O = [0 : 1 : 0]$ is $4x - z = 0$. Plugging this into the equation defining C gives:

$$y^2(4x) = x^3 + 3x(4x)^2$$

so $4y^2x = 49x^3$, and hence $x = 0$, $y = 7/2x$, or $y = -7/2x$. The first two of these correspond to $[0 : 1 : 0]$ and $[2 : 7 : 8]$,

respectively, so $y = -7/2x$ must correspond to the third point of intersection, which is $2Q = [2 : -7 : 8]$.

Finally, note that it is possible for these calculations to have slightly strange-looking results. For instance, let's compute $2P$ on the curve C as above, where $P = [0 : 0 : 1]$ as above. The tangent line to C at P is the line $x = 0$. Plugging this into the equation defining C gives $y^2z = 0$. The double root $y = 0$ corresponds to the tangency at P, so the third intersection point has $z = 0$, and is thus $[0 : 1 : 0]$ (since $x = 0$ already). Thus, $-2P = O$, so $2P = -O$. But $-O = O$, so $2P = O$! This point P is called a 2-torsion point of C. More generally, we have the following definition:

Definition 2.3. *Let C be an elliptic curve in Weierstrass form, and let n be an integer. A point $P \in C$ is said to be an n-torsion point (or an n-division point) of C if $nP = O$.*

As it turns out, there are exactly n^2 n-torsion points on any elliptic curve C. This is because (over the complex numbers), an elliptic curve is the same topological group as a torus, which is a product of two circles. There are n points of order dividing n on a circle (the roots of $x^n = 1$!), so there are n^2 points of order dividing n on a torus.

Incidentally, these results can be used to classify embeddings of an elliptic curve in projective space, in a similar fashion to how we classified embeddings of $\mathbb{P}^1$ in projective space. We will not do this here, because the answer is somewhat more complicated, but the techniques used are essentially the same.