A Brief Introduction to Divisors and the Picard Group

Justin French

June 17, 2017

1 Introduction

The Picard group is a group that can be derived from a variety, or more generally a scheme. It is a generalization of the ideal class group, and it encodes useful information about the structure from which it is derived. In general, the definition of the Picard group is scary. It is "the group of isomorphism classes of invertible sheafs, or equivalently of line bundles, on a ringed space, with the group operation being the tensor product." Fortunately, for smooth curves, there is another definition, based on divisors, that is much easier to understand.

2 Divisors

Before defining divisors we must first define prime divisors. A **prime divisor** Z on a smooth variety X is a subvariety satisfying the following conditions:

- It is closed, with respect to the Zariski topology.
- It is **irreducible**— that is it is not the union of smaller subvarieties
- It has **codimension one**— this means that if D is a closed, irreducible subvariety of X containing Z, then either $D = Z$ or $D = X$. This is analogous to the concept of a maximal ideal.

As an example, on a line each distinct point is a prime divisor.

From prime divisors we can define an arbitrary divisor: a **divisor** of a variety X is a finite formal sum of prime divisors on X with integer coefficients. For example, if Z_1, Z_2, and Z_3 are prime divisors of X, then the sum $Z_1 + 2Z_2 - 5Z_3$ would be a divisor. This sum does not have any geometric meaning; it is a purely formal construction. All these divisors form an abelian group, denoted $Div(X)$, where the group addition is just adding corresponding coefficients. Note that this group is not the Picard group—the Picard group is a quotient of the divisor group.

It is convenient to associate a divisor to each rational function on X. The divisor of some rational function f on X is defined as follows:

$$div(f) = (f) = \sum_Z ord_Z(f)Z$$

The sum is over every prime divisor, and $ord_Z(f)$ is (essentially) the multiplicity of the zero of f on Z, negative if it has a pole. (The rigorous definition of the vanishing order is somewhat unintuitive and isn't really necessary for this sort of general description of divisors.) Note that this sum is finite, though we won't prove it. Any divisor of the form (f) for some function is called a **principal divisor**. This is clearly analogous with principal ideals. The principal divisors form a (normal) subgroup of the divisor group, as $(f) + (g) = (fg)$ and $-(f) = (\frac{1}{f})$. That group is denoted $Princ(x)$.

3 The Picard Group

Finally, we have enough resources to define the Picard group. In terms of the groups described above, the definition is simple:

$$Pic(X) = \frac{Div(X)}{Princ(x)}$$

Again, there is a clear analogy with the ideal class group, not surprisingly as the Picard group is in many senses a broader definition of the ideal class group. From the definition we can derive the Picard group of some basic varieties:

Example: $Pic(\mathbb{A}^n) = 0$ for $n \geq 1$. This result is due to the fact that every subvariety of codimension one can be defined by a single polynomial. Strictly speaking it takes more ring theory than we covered to prove that.

Example: From knowing the Picard groups of affine space we can find the Picard groups of projective space as well. Consider the general sequence

$$\mathbb{Z} \to Pic(X) \to Pic(X \backslash Z)$$

where Z is some prime divisor. The first map is given by $1 \mapsto Z$. The second map is given by $D \mapsto D \cap (X \backslash Z)$. (If D is not a prime divisor then the intersection is distributed to each prime divisor in the formal sum for D so that the map is well-defined.) It is not difficult to check that each map is a homomorphism. Furthermore, one can show that the map is **exact**, meaning that the image of each map is the kernel of the succeeding one: the image of the first map is just everything of the form kZ for some integer k. That is also the kernel of the second map, since clearly $Z \cap (X \backslash Z) = \emptyset$, and any other prime divisor must not be affected much by the mapping $X \backslash Z$ or else it would intersect too much with Z and hence not be prime. At this point it is not clear how this sequence tells us the Picard group of projective space. To do that, take $X = \mathbb{P}^n$ and $Z = \mathbb{P}^{n-1}$. $\mathbb{P}^{n-1}$ is a subvariety because of the decomposition $\mathbb{P}^n = \mathbb{A}^n \sqcup \mathbb{P}^{n-1}$, and it a prime divisor because it is irreducible, has codimension one, and, since it is the vanishing set of the homogenous polynomial $f(x_0 : x_1 : ... : x_n) = x_0$, it is closed. (When writing $\mathbb{P}^n = \mathbb{A}^n \sqcup \mathbb{P}^{n-1}$, the patch equivalent to $\mathbb{P}^{n-1}$ is defined as the patch where $x_0 = 0$.) Again because of the decomposition $\mathbb{P}^n = \mathbb{A}^n \sqcup \mathbb{P}^{n-1}$, $X \backslash Z = \mathbb{A}^n$. Now the sequence from above becomes

$$\mathbb{Z} \to Pic(\mathbb{P}^n) \to Pic(\mathbb{A}^n)$$

Since $Pic(\mathbb{A}^n) = 0$, the kernel of the second map must be all of $Pic(\mathbb{P}^n)$, so since the map is exact $Pic(\mathbb{P}^n) \cong \ker(f_1) \cong \mathbb{Z}$.

Example: As a final example, when considering the Picard group of an elliptic curve over an algebraically closed field, we can recover the standard group law for elliptic curves. Let E be an elliptic curve over some algebraically closed field k. Though typically elliptic curves are considered over projective space, here it is more convenient to consider E as an affine variety. If we were to take E as a projective variety, we would have to account for poles of polynomials. In affine space polynomials (and in particular lines) do not have poles, so we can circumvent that trouble. Beginning the calculation, the prime divisors of this elliptic curve are all of the individual points on the curve. Thus, the divisor group is all the finite formal sums of these points. To compute the Picard group, we have to find which of these sums are principal divisors. If a set of points of the elliptic curve all lie on one polynomial, then the sum of those points (considering multiplicity) must is the principal divisor generated by that polynomial. In particular, the sum of all the points on a single line is a principal divisor. If P is a point on the curve and $\bar{P}$ is the reflection of that point over the x-axis, then the line passing through P and $\bar{P}$ does not pass through any other points. (The third point of intersection guaranteed by Bézout's Theorem would be the point at infinity, which is not on our affine curve.) Hence, in the Picard group, $P + \bar{P} = 0$, or $-P = \bar{P}$. Using that relation, we can rewrite any sum of points as a sum of points with positive coefficients. As a corollary, a principal divisor generated by any rational function can be rewritten as a principal divisor with positive coefficients, i.e. as a principal divisor generated by a polynomial. Using that property, we can prove that no point on the affine curve behaves as the identity. As the elliptic curve is defined over an algebraically closed field, Bézout's theorem tells us that any polynomial of degree n that intersects the curve must do so exactly $3n$ times (considering multiplicity). However, some of those intersections might be points at infinity, which are not part of the affine curve that we are considering. Fortunately, an elliptic curve can only have one point at infinity, so a polynomial of degree n must intersect the curve at least $3n - 1$ times. Importantly, any polynomial must intersect the curve at least twice, so no single point is a principal divisor and hence no single point behaves as the identity in the Picard group. Finally, the addition formula of two points follows from considering the principal divisors generated by a line. If the line intersects the curve only twice, then we recover the aforementioned formula for $-P$. So here we assume the line intersects the curve thrice. Say those points of intersection are P_1, P_2, and P_3. Then $P_1 + P_2 + P_3 = 0$, or $P_1 + P_2 = -P_3 = \bar{P}_3$. That is exactly the definition of the sum of two points in the usual elliptic curve group law. Furthermore, using that formula we can reduce any formal sum of points to either a single point or 0. Thus every element of the Picard group (except for 0) is actually a single point on the elliptic curve. (Note that in deriving this formula we see another advantage of considering an affine curve over the projective curve: on a projective elliptic curve, we would get $P_1 + P_2 + P_3 - 3P_\infty = 0$, which is only helpful if one proves that $P_\infty = 0$. For an affine elliptic curve, we don't need to prove that $P_\infty = 0$; we can simply define P_∞ to be an extension of the curve that corresponds to the element 0 of the Picard group.)

4 Resources

`https://www.math.ucdavis.edu/~osserman/classes/248A-F09/divisors.pdf` https://homepages.warwick.ac.uk/~maseap/arith/notes/picard.pdf

http://math.stanford.edu/~vakil/0708-216/216class2829.pdf