Appendix 12 for Math 632: 2025 Winter Notes

Chunye Yang

March 17, 2026

In this part of the notes, we will use what we have developed to study something concrete, i.e. curves. Let's be more specific about what we mean by curves. Throughout this chapter, we will assume that all curves are **projective**, **geometrically integral**, **regular**, **purely one dimensional** schemes over a field k. Sometimes, if necessary, we will add the hypothesis that k is algebraically closed.

The strategy we will use to understand curves is to first prove a criterion to determine when a morphims is a closed embedding. Then assuming Serre duality, we will observe a few useful properties which are really useful, and you will find we actually have seen quite a lot of them before. Then using these, we will study curves of various genera and finally develop the theory of hyperepplipticc curves in a hands-on way.

1 A Criterion for a Morphism to be a Closed embedding

Recall that if $\pi : X \to Y$ is a closed embedding, then we know that it's projective and is injective on points, but only these two properties don't ensure a morphism to be a closed embedding, and the following examples shows that:

Example 1.1. Consider the field $k = \mathbb{F}_p$ and the following morphism:

$$\mathbb{A}^1_k \to \mathbb{A}^1_k \qquad x \mapsto x^p$$

I claim that this is a bijection of the underlying topological space. To see this, notice that the corresponding morphism is injective, and it is obviously finite since we know that $1, x, \cdots, x^{p-1}$ generates $k[x]$, thus it's projective. Therefore, since it's a finite extension, by the lying over theorem, we know that the corresponding morphism of schemes is surjective. To show it's injective, say (f) is a prime, then we know that it's inverse image is (f) since we know that (f) is mapped to (f^p) and (f) is already a maximal prime, therefore it's injective.

Moreover, this morphism even induced isomorphisms on closed points we already showed that this morphism will induce morphisms on the same residue field, and I will let you show that this morphism is not 0.

However, this morphism is not a closed embedding, as the morphism is induced by a surjective ring map.

We will find out soon enough that the piece of information we are missing is that we have to make sure π also induces injective morphisms on tangent spaces at closed points, for example when k is algebraically closed. The issue of the above Forbenius morphism is that it's not injective on tangent spaces at all closed points. For example, consider (x), we have to show that it's not surjective on the cotangent space, i.e.:

$$(x)/(x^2) \to (x)/(x^2)$$

is not surjective where the morphism is given by $x \mapsto x^p$ for $p \geqslant 2$, therefore this morphism on the cotangent space is 0, not surjective.

We are now ready to state the criterion:

Theorem 1.2. Suppose that $k = \overline{k}$ and $\pi : X \to Y$ is a projective morphism of finite type k-scheme that is injective on closed points and injective on tangent vectors at closed points, then π is a closed embedding.

We have already saw that if $\pi : X \to Y$ is a closed embedding, then the corresponding morphism on the cotangent space is $m/m^2 \to m/m^2 + I$ which is surjective, thus the corresponding morphism on the tangent space is injective and a closed embedding is of course injective on closed points since it's even injective on all points.

Remark 1.3. Consider the example $Spec\mathbb{C} \to Spec\mathbb{R}$, this is injective on closed points, and the corresponding tangent space is 0 thus the map on tangent spaces is injective, but this is not a closed embedding, therefore, the hypothesis that k is algebraically closed is important and can't be removed.

The hypothesis that the morphism is projective can also not be removed. An example is the normalization of the nodal cubic, we know that this is not a closed embedding since it's firstly not injective on points, but if we erase one point in the preimage of the node point, it's injective on closed points, and injective on tangent vectors, but it's still not a closed embedding. The reason is that it's not projective. To see why, notice that the morphism is of finite fiber, therefore, if it's projective, then it's finite, but notice that the morphism is induced by:

$$k[x, y]/(y^2 - x^2(x + 1)) \hookrightarrow k[t] \hookrightarrow k[t, (t - 1)^{-1}]$$

But this is not finite since using $(t - 1)^{-1}$, we have elements of arbitrarily low degree. And this is definitely not a closed embedding as the morphism is not surjective, for example $(t - 1)^{-1}$ is not in the image.

Now we can prove the above theorem, which seems to be a statement that is fundamentally about finite type k-schemes since we are using something like the tangent space. However, it's actually a consequence of the following result:

Theorem 1.4. Suppose that $\pi : X \to Y$ is a morphism of Noetherian schemes whose degree at each closed point of Y is 0 or 1, then π is a closed embedding.

We now make some general remarks about finite morphisms whose degree is 1 or 0 at all points of the target, which also helps review a lot of algebra facts.

Remark 1.5. Notice that if the degree is 0 or 1, then it's necessarily injective on points. This actually holds for all finite morphisms between Noetherian schemes, since we know that the degree at a point is the dimension of the space of function on the fiber of p, considered as a vector space over $k(p)$, or in other words, it's $Spec(B \otimes k(p))$. To proceed further, we need to recall some algebra fact we proved before.

Recall that if M is a finite length module over A, then it has a finite composition series, and then it's annihilated by the product of maximal ideals appearing in the composition series, in other words, M is a $A/m_1 \cdots m_n$ module if $m_1, \cdots, m_n$ are the maximal ideals appearing in the decomposition. We can apply this to A itself, and recall that if A is finite length over itself, we call A an Artinian ring. Then this implies that $A/m_1 \cdots m_n$ is just A (moreover, these m_i's are all the maximal ideals of A, even better they are all the primes, can you see why? therefore, we have showed that Artinian rings only has finitely many maximal ideals), and if we write it as $A/n_1^{l_1} \cdots n_s^{l_s}$ to avoid repeated maximal ideals, Chinese Remainder theorem tells us that we can decompose A to $A/n_1^{l_1} \times \cdots \times A/n_s^{l_s}$. Then consider the elements in A that is mapped to $(1, 0, \cdots, 0), \cdots, (0, \cdots, 0, 1)$ in the product, we call them e_i, we know that $e_i = 1 \bmod n_i$ and is 0 mod any n_j for $j \neq i$. Then we know that we can also decompose A into the following form:

$$A \simeq \prod_i e_i A$$

the morphism is easy to built, just $a \mapsto (ae_i)$.

Similar stories also hold for finite length A module M, we pick out all the maximal ideals in the composition series and conclude that M is actually $A/m_1 \cdots m_n$-module, then we decompose A similarly and decompose M similarly.

Then we can apply this ti $B \otimes k(p)$, notice that the prime ideals of $B \otimes k(p)$ can be thought as $B \otimes A_p/pA_p \simeq B_p \otimes_{A_p} k(p)$, therefore we know that the prime are exactly the primes of B such that the inverse image is p. Notice that this is a finite dimensional vector space over $k(p)$ (since B_p is a finite module over A_p), thus Artinian (you have to argue a little bit more than just $B_p \otimes k(p)$ is a finite dimensional $k(p)$ vector space, we need to say it is a finite dimensional $k(p)$-algebra). Therefore all the primes are maximal, therefore we can apply the previous decomposition and notice that if there is more than one point, then the dimension is at least 2, a contradiction to degree 1 or 0.

Remark 1.6. More than that we can show that π induced isomorphisms on the residue fields. Let's again work affine locally and assume that $SpecB \to SpecA$ is a finite morphism between specs of Noetherian rings. We know that if q is mapped to p, we want to show that:

$$A_p/pA_p \to B_q/qB_q$$

is an isomorphism. It's injective, thus we only have to show it's surjective. What we know right now is $B \otimes_A k(q)$ is one dimensional over $k(p)$, or in other words, $B_p \otimes_{A_p} k(p)$ is one dimensional, but I claim that this implies that $B_q \otimes_{A_p} k(p) = B_q/pB_q$ is also one dimensional over $k(p)$, thus using the canonical surjection $B_q/pB_q \to B_q/qB_q$, we conclude that B_q/qB_q is also one dimensional over $k(p)$.

To see why $B_p \otimes_{A_p} k(p)$ being one dimensional implies that $B_q \otimes_{A_p} k(p)$ is one dimensional. We need a general algebra fact. Suppose that S is a multiplicative set in B, then $S^{-1}B \otimes_A C \simeq S'^{-1}(B \otimes_A C)$ where S' is the image of S in $B \otimes C$. Then we know that $B_q \otimes_{A_p} k(p)$ is the localization of $(B_p \otimes_{A_p} k(p))$, but notice that $B_p \otimes_{A_p} k(p)$ is a field! Thus any localization is itself, we are done.

Remark 1.7. The above remark makes it possible to discuss the corresponding morphism on tangent spaces, and we will show that it's also injective.

Recall that we need this isomorphism of residue field since it we consider the corresponding morphism on the cotangent space:

$$m_y/m_y^2 \to m_x/m_x^2$$

We want to define the corresponding morphism to be the dual. However, recall that the definition of the dual depends on the field, since it's $\mathrm{Hom}(-, k)$ and this k matters here. Therefore, we don't know which field we need to use if the residue field is not the same, thus the morphism of tangent spaces is not always well defined.

Now we go back to question we are interested, $SpecB \to SpecA$ is a finite morphism of specs of Noetherian spaces and the degree at each point of $SpecA$ is either 0 or 1. Now we only have to prove the morphism on the cotangent space is surjective. We already know that m_y is mapped into m_x, but if you look at the isomorphism:

$$A_y/m_y \to B_x/m_x$$

then since the inverse image of m_x is m_y, thus all the elements in A_y that is mapped to m_x comes from m_y, but notice that $A_y \to B_x$ is surjective, thus $m_y \to m_x$ is also surjctive.

From the above three remarks, we know that the key hypothesis: injective on points and injective on tangent vectors is implictly embedded in the assumption of Thm 1.4, and now we show that we can reduce the proof of Thm 1.2 to the proof of the more general version Thm 1.4:

Proof. The property of being a closed embedding is local on the target so we may assume Y is affine say $SpecB$. I claim that π actually has finite fiber over any point, not just closed points. Recall that the fiber dimension of a projective morphism is upper semicontinuous, therefore we know that the locus where the fiber has dimension at least 1 is a closed subset of Y, thus since Y is Noetherian, if it's not empty, it must contain a closed point of Y, a contradiction, thus it's empty. Therefore we have prove that π is a projective morphism with finite fibers, thus it's finite.

Now I claim that the degree of π at any point of Y is at most 1. Let's first prove it for closed points of Y, or in other word, we want to prove that if $SpecA \to SpecB$ is a finite morphism of finite type k-schemes whose induced morphism on tangent spaces at closed points is injective, then the degree at closed points is at most 1. We need to show that $A \otimes_B k$ is one dimensional over k, but if you consider the fiber Cartesian diagram:

$$\begin{array}{ccc} SpecA \otimes_B k & \longrightarrow & Speck \\ \downarrow & & \downarrow \\ SpecA & \longrightarrow & SpecB \end{array}$$

we find that $A \otimes_B k$ is actually a finite k-algebra for k algebraically closed. Notice that $A \otimes_B k = A \otimes_B B/m_B = A/m_B A$ where m is the corresponding maximal ideal of B, and since we assumed that the corresponding

tangent map is injective, the cotangent map is surjective, thus the maximal ideal m_B of B maps surjectively to that m_A of A, thus $A/m_BA = A/m_A$ which a a field! Therefore we know that:

$$k \hookrightarrow A \otimes_B k$$

is actually a finite field extension, but notice that k is algebraically closed, thus the only possible such extension is that $A \otimes_B k$ is one dimensional over k, we are done.

Then notice that the degree of a morphism is the rank of a finite type quasicoherent sheaf, thus is upper semicontinuous, then exactly the same argument: the locus whose degree is at least 2 is closed and if not empty, includes a closed point, a contradiction, shows that for all points in Y, the degree is 0 or 1. □

Therefore, now we have reduced Thm 1.2 to Thm 1.4, we only have to prove the later:

Proof. Again, closed embedding is local on Y, the let's assume Y is affine, say $SpecB$, thus X is also affine, say $SpecA$, and π correspond to the ring map $B \to A$, and we want to show this is surjective. Let K be the cokernel of $B \to A$ and we only have to show $K = 0$(recall that this ring map can be though as a B-module morphism).

TO show it's 0, recall that we only have to check the localization at each maximal ideal n of B, thus we obtain an exact sequence for each n:

$$B_n \to A_n \to K_n \to 0$$

Now apply the the right exact functor $\otimes_{B_n} B_n/nB_n$, we get an exact sequence:

$$B_n/nB_n \to A_n/nA_n \to K_n/nK_n$$

we know from the hypothesis that A_n/nA_n is either one dimensional over B_n/nB_n or it's 0. If it's 0, then $K_n/nK_n = 0$. If it's one dimensional, we know that $B_n/nB_n \to A_n/nA_n$ is a B_n/nB_n vector space morphism which is between two finite dimensional vector spaces of the same dimension, and it's injective, thus it's surjective. Therefore, either way $K_n/nK_n = 0$. Recall that A_n is a finite module over B_n, thus K_n is finitely generated over B_n, then Nakayama's lemma tells you that $K_n = 0$, we are done. □

Remark 1.8. Recall we proved that if $\pi : X \to Y$ is an affine morphism over k and l/k is a field extension, then π is a closed embedding iff $\pi \times_k l$ is. This is a great result, and the affine hypothesis is not necessary, it's only there so that the proof is easier and we will use it to prove some result over schemes not over an algebraically closed field. Details in the next example:

Example 1.9. We already know that the Veronese embedding is a closed embedding, but let's pretend we don't know it and we want to prove it using the criterion we just established.

First, we need to pass to the algebraic closure to apply our criterion and to do so we need to make sure it's an affine morphism. But if you think about how we define the morphism, you will see that:

$$v_d : \mathbb{P}^n_k \to \mathbb{P}^N_k$$

using the complete linear series $|\mathcal{O}(d)|$, we see that the inverse image of each $D_+(x_i)$ in $\mathbb{P}^N_k$ correspond to $D_+(f)$ where f is a homogeneous polynomial of degree d, thus this is indeed an affine morphism.

Then consider the corresponding morphism after we base change to the algebraic closure, i.e. the following diagram:

$$\begin{array}{ccccc} \mathbb{P}^n_{\overline{k}} & \longrightarrow & \mathbb{P}^N_{\overline{k}} & \longrightarrow & Spec\overline{k} \\ \downarrow & & \downarrow & & \downarrow \\ \mathbb{P}^n_k & \longrightarrow & \mathbb{P}^N_k & \longrightarrow & Speck \end{array}$$

A good way to see the pullback is still the d-th Veronese embedding is to see what is the pullback of $\mathcal{O}(1)$ on $\mathbb{P}^N_{\overline{k}}$ to $\mathbb{P}^n_{\overline{k}}$. We know that the two vertical morphisms are determined by $\mathcal{O}(1)$, thus we know that the pullback of $\mathcal{O}(d)$ on $\mathcal{P}^n_k$ to $\mathbb{P}^n_{\overline{k}}$ is $\mathcal{O}(d)$ and f is pullback to f. Then the following details are left to you. Therefore we can pretend that we initially work with an algebraically closed field.

Then we need to prove that it's injective on closed points and injective in tangent vectors. Recall that when you work with an algebraically closed field, the closed points of $\mathbb{P}^n_k$ is represented by $(k_0 : \cdots : k_n)$ and we know that this morphism act on closed points by:

$$x = (k_0 : \cdots : k_n) \mapsto (f_0(x) : \cdots : f_N(x))$$

Then suppose that $(f_0(x) : \cdots : f_N(x)) = (f_0(y) : \cdots : f_N(y))$, then we know that there is a k such that $(f_0(x), \cdots, f_N(x)) = k(f_0(y), \cdots, f_N(y))$, since this is an algebraically closed field, there is a $t \in k$ such that $t^d = k$, therefore since f_i's are homogeneous of degree d, we know that we can conclude that $f_i(x) = f_i(ty)$ in particular, $x_i^d = y_i^d t^d$ for some $x_i \neq 0, y_i \neq 0$, this implies that $x_i = y_i t \times \eta$ for some d-th root of unity η, since we can scale x, y, let's assume that $t = 1$, then we know that $x_i = y_i \eta$, we apply to $x_i^{d-1} x_j = y_i^{d-1} y_j$, we conclude that $x_j \eta^{d-1} = y_j$, but notice that $\eta^{d-1} \cdot \eta = 1$, thus we know $x_j = y_j \eta$, we are done. Therefore we know that this implies that $x = y$.

We can also prove it's injective on tangent spaces, or equivalently, surjective on cotangent spaces. To see this, we can work with the standard affine $D_+(x_i^d) \to D_+(x_j)$, where the ring morphism is given by:

$$(k[x_0, \cdots, x_N]_{x_j})_0 \to (k[x_0, \cdots, x_n]_{x_i^d})_0$$

which is surjective, then of course the corresponding maximal ideal map is going to be surjective.

You can also do this for Segre embedding, but it's not too enlightening to do so, so we omit it.

2 A Series of Crucial Tools

In this section, we mainly reviewed a lot of the results we have established before, as they are going to show up really often when we study curves, so it's best if they are at the tip of your tongue.

In what follows, all curves C are assumed to be projective, gemetrically regular, geometrically integral, variety over a field k and $\mathcal{L}$ is an invertible sheaf on C.

1. The first thing we will use is **Serre duality**, on a geometrically irreducible projective k variety of dimension n, there will be a dualizing sheaf, and in our case, on C, we call it ω_C, we have already see that if the genus of C is g, there will be g linearly independent sections and the degree is $2g - 2$. Moreover, for any finite rank locally free sheaf $\mathcal{F}$, we have:

$$h^i(C, \mathcal{F}) = h^{1-i}(C, \omega_C \otimes \mathcal{F}^\vee)$$

2. Then we know that negative degree line bundles have no nonzero global sections. The reason is that geometrically regular implies regular, then we know that degree of a line bundle can be computed using any nonzero rational section, and the result will be the number of zeros minus the number of poles, suitably counted, but if there is a regular section, then it has no poles, thus the degree of $\mathcal{L}$ is necessarily nonnegative.

3. Next, we would like to understand when degree 0 line bundles are trivial since we already know that trivial line bundle has degree 0 just by definition.

   Now, if $\deg\mathcal{L} = 0$, then I claim that the dimension of the global section is 0 or 1 and if the dimension is 1, then it's isomorphic to the structure sheaf, i.e. trivial. This is because if we have any two nonzero global sections s, t, we can compute the degree using the zeros and poles. Since they have no poles, thus no zeros, therefore both are nonwhere vanishing sections, and I want to claim that s is a scalar multiple of t. To see this, we first notice that s gives a trivialization of $\mathcal{L} \simeq \mathcal{O}_C$ or you can think of this as the line bundle and divisor correspondence on a normal locally Noetherian scheme, but either way, we know that s, t are actually regular functions on C, but we know that C is geometrically integral and projective, thus we can base change to $\overline{k}$, and we already know that an integral projective variety over k has 1 dimensional global sections, and cohomology is stable under field extension. (This is where we need geometrically integral, but again if you want to work with algebraically closed field, then this is not a problem.)

4. Next, we can compute the dimension of the global section using the degree **if the degree is high enough**. We can do this because of Serre duality which can convert the computation on degree 0 to degree at least of $2g-2$.

   I claim that if $\deg\mathcal{L} > 2g-2$, then $h^0(C,\mathcal{L}) = \deg\mathcal{L} - g + 1$. To see why, we first notice that again, $h^0(C,\mathcal{O}_C) = 1$, then we know that $h^1(C,\mathcal{O}_C) = g$, therefore, Riemann-Roch, which is $\deg\mathcal{L} + \chi(C,\mathcal{O}_C) = \chi(C,\mathcal{L})$ becomes:

$$h^0(C,\mathcal{L}) - h^1(C,\mathcal{L}) = \deg\mathcal{L} + 1 - g$$

   Then if $h^1(C,\mathcal{L})$ vanishes, we obtain the formula.

   To see that it vanishes, we use Serre duality:

$$h^1(C,\mathcal{L}) = h^0(C,\mathcal{L}^\vee \otimes \omega_C)$$

   Notice that on a projective curve, degree is additive upon tensors, therefore $\deg\mathcal{L}^\vee\otimes\omega_C$ is $2g-2-\deg\mathcal{L}$, then if $\deg\mathcal{L} > 2g-2$, the degree is negative, thus no nonzero global sections.

   Remark 2.1. With somewhat similar ideas, we can show that if a line bundle $\mathcal{L}$ is of degree $2g-2$, then it's of $g-1$ or g sections, and if it admits g sections, then it's isomorphic to the dual sheaf.

   You can imagine that this is still a consequence of Serre duality, to prove that $\mathcal{L} \simeq \omega_C$, it's equivalent to prove that $\mathcal{L}^\vee \otimes \omega_C \simeq \mathcal{O}_C$ and notably, the degree of $\mathcal{L}^\vee \otimes \omega_C$ is 0, thus we know that it's global section is either of dimension 1 or dimension 0, if it's of dimension 1, then $\mathcal{L}$ is isomorphic to ω_C. Moreover, we have:

$$h^1(C,\mathcal{L}) = h^0(C,\mathcal{L}^\vee \otimes \omega_C)$$

   which is 0 or 1, but we know from Riemann Roch that $h^0(C,\mathcal{L}) - h^1(C,\mathcal{L}) = 2g-2-g+1 = g-1$, therefore depending on whether $h^1(C,\mathcal{L})$ is 0 or 1, $h^0(C,\mathcal{L})$ is either g or $g-1$.

   Remark 2.2. Suppose that C is now of genus $g > 1$, then I claim that there is a closed point of degree at most $2g-2$ over the base field, i.e. the degree of the field extension is at most $2g-2$. To see why, consider the canonical bundle ω_C, it's of degree $2g-2$, but since $g > 1$, the degree is positive, and we know that since the dimension of the global section is g, there is a nonzero global section, and we use this section to compute the degree, or in other words, we need to compute the degree of the divisor $div(s)$, but notice that it's a regular section, thus no poles, only zeros, therefore even if the divisor only has one zero (it at least has a zero since the degree of ω_C is positive), then we know that it's degree is at most $2g-2$, not even to mention if there are multiple zeros.

5. Let's go back to our tool package. Now we show that if you twist a line bundle by a degree 1 closed point, the dimension of the global section is twisted by at most 1, i.e. if p is a closed point of degree 1, then $h^0(C,\mathcal{L}) - h^0(C,\mathcal{L}(-p)) = 0$ or 1. The reason is again simple, since we assume regularity, then we have a closed embedding diagram of effective Cartier divisor:

$$0 \to \mathcal{O}(-p) \to \mathcal{O}_C \to \mathcal{O}|_p \to 0$$

   tensor it with $\mathcal{L}$ and look at the LES:

$$0 \to H^0(C,\mathcal{L}(-p)) \to H^0(C,\mathcal{L}) \to H^0(C,\mathcal{L}|_p)$$

   Notice that being a degree one point, then $\mathcal{O}|_p$ is the skyscraper sheaf at p with stalk the base field, i.e. $\mathcal{L}|_p$ is also the skyscraper sheaf at p with the stalk the residue field since $\mathcal{L}$ is locally free, therefore the dimension of $H^0(C,\mathcal{L}|_p)$ is at most 1, then this gives you the desired result.

6. Here is a criterion for a line bundle to be base point free. Suppose that we now assume k is algebraically closed, so all closed points have degree 1. Then I claim that if $h^0(C,\mathcal{L}) - h^0(C,\mathcal{L}(-p)) = 1$ for all closed points p, then $\mathcal{L}$ is base point free. The reason is that if this equation holds, then we know that the morphism $H^0(C,\mathcal{L}) \to H^0(C,\mathcal{L}|_p)$ is surjective (can you see why?), then this fact plus $H^0(C,\mathcal{L}|_p) = 1$

implies that there is a global section of $\mathcal{L}$ such that when you evaluate it's value at the fiber at p, it doesn't vanish.

This bu since we work with a Noetherian scheme (a variety), for each closed point, if we have a neighborhood, then the union is the whole space, this implies that it's base point free(can you see why?).

7. Next, we assume further more that there are p, q, distinct closed points of degree 1 each. What we can say for sure is:
$$h^0(C, \mathcal{L}) - h^0(C, \mathcal{L}(-p-q)) = 0, 1, 2$$
However if this difference is exactly 2, we observe that this 2 is obtained in essential one way, i.e. $h^0(C, \mathcal{L}) - h^0(C, \mathcal{L}(-p)) = 1$ and $h^0(C, \mathcal{L}(-p)) - h^0(C, \mathcal{L}(-p-q)) = 1$, then by what we just discussed, there is a section of $\mathcal{L}$ that doesn't vanish at p, and there is a section of $\mathcal{L}$ that vanishes at p but it doesn't vanish at q (the global sections of $\mathcal{L}(-p)$ is a subspace of the global sections of $\mathcal{L}$ and they all vanish at p). Then consider the morphism f to the projective space that is given by $\mathcal{L}$, I claim that $f(p) \neq f(q)$, or in other words, people often call this this linear series **separates the points** p and q.

The reason is that if you think about how this morphism is defined, you find that since the coordinate hyperplanes of the projective space is pulled back to global sections of $\mathcal{L}$, then the locus where the section vanishes is the inverse image of the hyperplane, then consider all the coordinate hyperplanes, we find that there is one of them whose inverse image contain p but it doesn't contains q. This is because if not, then all sections of $\mathcal{L}$ that vanish at p also vanish at q, which is contradiction.

Remark 2.3. We didn't really explicitly proved that the vanishing locus of pullback of sections of a line bundle, thus we discuss it here. Say $f : X \to Y$ is any morphism of schemes and $\mathcal{L}$ is a line bundle on Y with $x \in \Gamma(Y, \mathcal{L})$, then if we consider f^*x in $\Gamma(X, f^*\mathcal{L})$, then I claim that $V(f^*x) = f^{-1}V(x)$. To see why, assume that p is the vanishing locus of f^*x, we want to show that x vanishes at $q = f(p)$, and we also want to prove that if q is a vanishing locus of x there is a $p \in X$ where f^*x vanishes such that $f(p) = q$. These are all local properties, thus we can choose an affine open of $q = f(p)$ where $\mathcal{L}$ is trivial, then we know that the pullback of $\mathcal{L}$ on the inverse image is also trivial, then we know that here the pullback morphism is equal to the scheme pullback morphism, therefore we can just assume that if $f : X \to Y$ is a scheme morphism and x is a regular function on Y, we consider it's pullback as a regular function of X and we want to figure out the desired property. To do this, we may assume that X, Y are affine, and I will let you do the reduction, thus the question just becomes if $f : A \to B$ is a ring morphism and $x \in A$, then if p is a prime in B such that fx vanishes, then x vanishes at $f^{-1}p$. And if p is a prime of B such that x vanishes at $f^{-1}p$, then we want to show that $f(x) \in p$, which is again trivial. We are done.

Well, you might also wonder why the pullback morphism on the structure sheaf of Y is the same as that of the pullback morphism given by the scheme morphism. There are a lot of ways to see this, one common way to do this is to first look at what happens on $SpecB \to SpecA$, where we have a clear description of the pullback morphism. Then for the global description, we use the sheaf axiom (identity axiom), details are left to you.

8. By exactly the same method, consider the following quantity:
$$h^0(C, \mathcal{L}) - h^0(C, \mathcal{L}(-2p))$$
we know that it's $0, 1, 2$, and we are still interested in the case when this quantity is 2. I claim that in this case the morphism to the projective space which correspond to $\mathcal{L}$ (using the section doesn't vanish at p, or just the complete linear series $|\mathcal{L}|$) separates tangent vectors at p, or in other words, it's injective as tangent maps, or equivalently, it's surjective on cotangent spaces.

Let's see what is the corresponding cotangent morphism:
$$m_q/m_q^2 \to m_p/m_p^2$$
since we assumed regularity, the dimension of this vector space m_p/m_p^2 is the same as the dimension of the local ring, or the codimension of the closed point, i.e. 1 since in variety, dimension and codimension

add up to the total dimension. Then this morphism on tangent spaces is a vector space morphism to a one dimensional space, thus, it's surjective iff it's not 0. Therefore, it suffice to find a local function on the projective space that vanishes at q, whose pullback vanishes at p only at order 1 but not order 2.

To find this element, let's first interpret the equation $h^0(C, \mathcal{L}) - h^0(C, \mathcal{L}(-2p)) = 2$, this means that there is a global section of $\mathcal{L}$ that vanishes at p, but it doesn't vanish at order 2. To see why, consider the following SES:

$$0 \to \mathcal{L}(-2p) \to \mathcal{L}(-p) \to \mathcal{L}(-p)|_p \to 0$$

The key is how to interpret $\mathcal{L}(-p)|_p$, I will let you figure out why the global section of $\mathcal{L}(-2p)$ exactly correspond to global sections of $\mathcal{L}$ that vanish at p and also vanishes at degree 2 at p, or in other words is in $m_p^2\mathcal{L}_p$, then this global section x is what we are looking for.

This is because that there is a hyperplane that is pulled back to x, and we know that this implies that $f(p)$ is in the hyperplane, thus we know that we can choose any affine open of $f(p)$ where $\mathcal{O}(1)$ is trivial, and restrict the section determining the hyperplane to that open, we know that the function we obtain vanishes at $f(p)$ since it vanishes on all points on the hyperplane and $f(p)$ is in the hyperplane. And we consider the pullback of this function, which is the restriction of x, and we know that x vanishes at p but not with order 2 at p, we are done.

9. Combining our previous arguments, we found a criterion for a line bundle to be very ample if we work over an algebraically closed field. Then I claim that $\mathcal{L}$ is very ample if for all closed points p, q of C, not necessarily distinct, the following equation holds:

$$h^0(C, \mathcal{L}) - h^0(C, \mathcal{L}(-p-q)) = 2$$

The key here is to show the morphism to the projective space is a closed embedding, then we can use our criterion.

Remark 2.4. Suppose that we work with a algebraically closed field k, so the previous criterion applies. Let p be a closed point on C, then I claim that $C - \{p\}$ is affine. To show this, consider the line bundle $\mathcal{O}(jp)$, then I claim that for $j \gg 0$, this is base point free. To see why, we use a previous remark and show that $h^0(C, \mathcal{O}(jp)) - h^0(C, \mathcal{O}(jp-q)) = 1$ for any closed point q in C. The first thing we need to notice is that the degree of $\mathcal{O}(p)$ is 1 since we can compute the degree using the divisor and the result is just a degree 1 closed point, thus the degree of the line bundle is 1, this implies that for high enough j, the degree of $\mathcal{O}(jp)$ and $\mathcal{O}(jp-q)$ are necessarily larger than $2g-2$, therefore we can compute h^0 using degree and g, then I will let you see why this implies that the assertion. Moreover, the same method shows that for $j \gg 0$, there are at least two linearly independent sections of $\mathcal{O}(jp)$, we can take one of them to be the one that vanishes only at p and we need another one to be a section that doesn't vanish at p, but this holds since we can know that $h^0(C, \mathcal{O}(jp)) - h^0(C, \mathcal{O}(jp-p)) = 1$.

Now these two sections determined a morphism to $\mathbb{P}^1$ and we know that we can choose the morphism such that the preimage of $[0:1]$ is going to be p. I claim that this morphism is finite. You probably want to conclude that this is a closed embedding since we know that for $j \gg 0$ the line bundle $\mathcal{O}(jp)$ satisfies the desired property, but this only means that $\mathcal{L}$ is very ample, not meaning that any morphism determined by the sections of $\mathcal{L}$ is a closed embedding. To show it's finite, we already know that it's projective, thus the only thing we need is to show that it has finite fibers. We already know that it's not a constant map since there will be some points whose image is $[1:0]$. Then we know that for each closed point of $\mathbb{P}^1$, it's preimage is a proper closed subset of C, and we know that closed subsets of C, since it's a curve, are just finite collections of closed points, and we know that the preimage of the generic point of $\mathbb{P}^1$ is going to be the generic point of C. Then since $C - \{p\}$ is the preimage of $\mathbb{A}^1$, then it's affine.

A similar argument shows that C with finitely many closed points removed is going to be affine. Since if you want to remove, say $p_1, \cdots, p_n$, you can consider the line bundle $\mathcal{O}(n(\sum p_i)))$ and notice that the preimage of $[0:1]$ is going to be the union of all the closed points, we are done.

But you can also argue that projective implies separate, and separated implies intersection of affines is affine, we are also done.

10. We now combine all the discuss above and give a numerical criterion for a line bundle to be base point free and very ample.

    I claim that if $\deg\mathcal{L} \geqslant 2g$, then it's base point free and if $\deg\mathcal{L} \geqslant 2g+1$, it's very ample. The reason is that when the degree of $\mathcal{L}$ is at least $2g$, then the degree of $\mathcal{L}(-p)$ is at least $2g-1$, which enables us to compute the dimension of sections using degree and genus. Similarly, if $\deg\mathcal{L} \geqslant 2g+1$, then $\deg\mathcal{L}(-p-q) \geqslant 2g-1$ and we can still compute the dimension using degree and genus. Moreover, in this case, any basis $s_0, \cdots, s_{\deg\mathcal{L}-g}$ of the global sections of $\mathcal{L}$ gives a closed embedding to the projective space.

    Corollary 2.5. An invertible sheaf on a projective, regular, integral curve over $k = \overline{k}$ is ample iff $\deg\mathcal{L} > 0$.

    Proof. First, if it's ample, then we know that it has global sections, thus if a line bundle has negative degree, it has no global sections, therefore we know that an ample line bundle must have nonnagative degree, but if it's degree is 0, I claim that it is not ample. This is because that if it's isomorphic to the structure sheaf, we know that it's not ample. Or else it has no nonzero global sections, thus not ample.

    Then we prove that for a line bundle with degree > 0, it's ample, we only have to show that high powers of that is very ample, but notice that degree is additive upon tensor and we know that for all line bundles with degree at least $2g+1$, it's very ample, we are done. □

    Remark 2.6. We didn't mention why the structure sheaf is not ample on a projective curve, at least if we assume that we work over an algebrically closed field and with an integral projective curve. Recall that ample means that the locus where sections $s \in \Gamma(C, \mathcal{L}^{\otimes n})$ don't vanish form a basis of C, but if $\mathcal{L}$ is $\mathcal{O}_X$, the only possible nonzero global sections are the constants, thus any of the nonvanishing locus is going to be all of C, a contradiction except when C is a point, we are done.

11. Finally, we want to drop the assumption that k is algebraically closed. And it turns out that if we assume geometrically regular and geometrically integral, then for a large part of our discussion, we can indeed drop the assumption that k is algebraically closed and still obtain the same result. For example, we can prove that degree at least $2g$ implies base point free and degree at least $2g+1$ implies very ample.

    Not surprisingly, we still use the base change to the algebraic closure. Since the dimension of cohomology groups are stable under base change, then the degree of the pullback line bundles remains the same as those on the base. For example, if we first deal with base point free line bundles, we know that if $\mathcal{L}$ has degree at least $2g$, then it's degree is also at least $2g$ on the base change, which implies that it's base point free there. But we have proved that base point free is independent of base changing to the algebraic closure, thus we are done. Now if we consider very ampleness, we can consider the following diagram:

$$\begin{array}{ccc} C_{\overline{k}} & \hookrightarrow & \mathbb{P}^n_{\overline{k}} \\ \downarrow & & \downarrow \\ C & \longrightarrow & \mathbb{P}^n_k \end{array}$$

    if we can show that the morphism downstairs is affine, we are done since an affine morphism is a closed embedding iff it's base change is. But the morphisms downstairs is actually finite as it's projective and has finite fiber (not constant since we know that the locus where x_i vanishes are all hit by the image as the degree of $\mathcal{L}$ is at least 1, thus it can't be the structure sheaf, thus it wonlt happen that the pullback of x_i doesn't vanish anywhere.)

    Corollary 2.7. Suppose that $\mathcal{L}$ is a geometrically integral, geometrically regular projective curve over an arbitrary field k, then it's ample iff $\deg\mathcal{L} > 0$.

    Proof. Suppose that $\mathcal{L}$ is ample, which means that there is a power of $\mathcal{L}$ such that the morphism it induces is a closed embedding to a projective space, then we again consider the pullback morphism,

which is still a closed embedding and this implies that the pullback of $\mathcal{L}$ is ample, therefore it's degree is positive, then we use the fact that degree is preserved under base change.

Conversely, say the degree is positive, then the degree of the pullback is positive, which means that for each high enough tensor power of $\mathcal{L}$, the morphism defined by any basis of the global section will be a closed embedding, then recall that a basis of the tensor product downstairs, after you pull back them, gives a basis of the global sections on the base change (to prove this you need something more than just knowing the dimension, you have to prove that the pullbacks are still linearly independent, or you have to prove that $f^*x = 0$ iff $x = 0$, but this is tensor with a field, which is implies that if it's 0 after tensor with 1, then it's originally zero.) Then we use the fact that an affine morphism is a closed embedding iff it's a closed embedding after pullback (the morphism downstairs is a finite morphism). □

Finally, we can reproduce the result that $C - \{p\}$ is affine even without algebraically closed assumption.

Corollary 2.8. Let C be a projective, geometrically regular, geometrically integral curve over a field k, then for any closed point p in C, $C - \{p\}$ is affine.

Proof. Recall that Serre duality doesn't require any algebraic closed assumption, thus the conclusion that we can compute dimension of global sections using degree and genus when the degree is $> 2g - 2$ still applies, then consider the the line bundle $\mathcal{O}(p)$, we know that it's degree is positive, thus for a high enough power, we know that any basis of the global section gives a morphism to the projective space, we can pick one section which only vanishes at p and expand it to a basis by arbitrary sections. Then we know that we can choose this morphism such that the preimage of $[0 : \cdots : 0 : 1]$ is p, then we know that the preimage of $D_+(x_0)$ is $C - \{p\}$, which implies that $C - \{p\}$ is affine. □

These are all the crucial tools we will use in the next section, before we end, we briefly discuss a result we mentioned but didn't prove before: all proper curves are projective. For the purpose of this study we don't assume that curves are smooth, regular or even reduced so this is a result that has much more generality. We will use Serre's cohomological criterion for ampleness:

The first result we want to prove is that for a reduced proper curve (a finite type k-scheme that is purely dimensional) C, ampleness can be checked on it's normalization:

Proposition 2.9. Let C be a **reduced** proper curve over k and $\mathcal{L}$ is a line bundle on C such that the pullback to the normalization $v : \widetilde{C} \to C$, $v^*\mathcal{L}$ is ample, then $\mathcal{L}$ is ample.

Proof. We will use the fact that normalization maps are finite. There is a wired fact that for every finite morphism between schemes, say $\pi : X \to Y$ there is a right adjoint for the pushforward functor π_*, which we will call $\pi^{!?}$ which takes quasicoherent sheaves on Y to quasicoherent sheaves on X, and we know that for each quasicoherent sheaf $\mathcal{F}$ on Y we have a canonical morphism:

$$\pi_*\pi^{!?}\mathcal{F} \to \mathcal{F}$$

We don't want to go into the details construction of this weird adjoint, and we will do it later when we need it later, here we will only state the properties we need.

Apply this to our question we take the kernel and cokernel of the canonical morphism and obtain the following SES:

$$0 \to \mathcal{E} \to v_*v^{!?}\mathcal{F} \to \mathcal{F} \to \mathcal{G} \to 0$$

Recall that for finite type k-schemes, normalization is going to be an isomorphism on a dense open subset of C, therefore we want to conclude that (like what we have for the adjoint between pushforward and pullback) $v_*v^{!?}\mathcal{F} \to \mathcal{F}$ is an isomorphism on that dense open, therefore both $\mathcal{E}$ and $\mathcal{G}$ can only be supported on a proper closed subset that doesn't contain any generic points of the components, thus a finite collection of closed points. But to do this, we need to do some work, since even for the adjoint pair of pushforward and pullback, we have to do some work to show this and in general this adjoint map commutes with restriction property doesn't hold for each adjoint pair. Recall that it's really confusing when we proved this kind of

results for pullback and pushforward, but things are simpler here since we are dealing with finite morphisms which is affine and extremely simplifies stuff. (for more discussion see the remark down below.)

Now, we will use the exact sequence above to show that $H^i(C, \mathcal{F} \otimes \mathcal{L}^{\otimes n}) = 0$ for $i > 0$ if $\mathcal{F}$ is a coherent sheaf. Now I claim that $v^{!?}$ takes coherent sheaves to coherent sheaves and notice that since v is finite the pushforward of a coherent sheaf is also going to be coherent, then we twist the above exact sequence by $\mathcal{L}^{\otimes n}$ and break it into two SES. We first can prove that:

$$H^i(C, v_* v^{!?} \mathcal{F} \otimes \mathcal{L}^{\otimes n}) = 0$$

for $n \gg 0$ and $i > 0$ since we can apply the projection formula, cohomology is invariant under pushforward of affine morphisms and conclude using Serre's cohomological criterion for ampleness. Notice that since the support of $\mathcal{E}$ is just a finite collection of closed points, easy computation using a suitable cover shows that the higher cohomology of $\mathcal{E}$ vanishes, therefore, we know that the higher cohomology of the cokernel of $\mathcal{E} \otimes \mathcal{L}^{\otimes n} \to v_* v^{!?} \mathcal{F} \otimes \mathcal{L}^{\otimes n}$ also vanishes. This fact plus the second SES tells you that the higher cohomology of $\mathcal{F} \otimes \mathcal{L}^{\otimes n}$ also vanishes for $n \gg 0$, which shows that $\mathcal{L}$ is ample. □

Remark 2.10. The way we prove that the adjoint map between pushforward and pullback commutes with restriction is by the following sequence of isomorphisms:

$$\begin{array}{ccccccc}
 & & \mathrm{Hom}_X((\pi^*\mathcal{G}), \mathcal{F}) & \xrightarrow{\simeq} & \mathrm{Hom}_Y(\mathcal{G}, \pi_*\mathcal{F}) & & \\
 & & \downarrow & & \downarrow & & \\
\mathrm{Hom}_U(i^*(\pi^*\mathcal{G}), \mathcal{F}') & \xrightarrow{\simeq} & \mathrm{Hom}_X((\pi^*\mathcal{G}), i_*\mathcal{F}') & \xrightarrow{\simeq} & \mathrm{Hom}_Y(\mathcal{G}, \pi_* i_* \mathcal{F}') & \xrightarrow{=} & \mathrm{Hom}_Y(\mathcal{G}, j_*(\pi|_U)_*\mathcal{F}') \\
= \uparrow & & & & & & \downarrow \\
\mathrm{Hom}_U((\pi^*\mathcal{G})|_U, \mathcal{F}') & \xleftarrow{\simeq} & & & \mathrm{Hom}_V(\mathcal{G}|_V, (\pi|_U)_*\mathcal{F}') & \xleftarrow{=} & \mathrm{Hom}_V(j^*\mathcal{G}, (\pi|_U)_*\mathcal{F}')
\end{array}$$

where the ='s stands for exactly the same object and $\mathcal{F}'$ is actually $i^*\mathcal{F}$, then I will let you figure out the rest of the details.

But the reason the proof is so complicated is becasue we are dealing with any morphism f, it it so general that you can imagine that the proof is also some general abstract nonsense. But this doesn't happen for this $\pi^{!?}$ for a finite morphism π, since it's affine and proof is going to be a lot easier.

Use the above result we have the following proposition:

Proposition 2.11. Reduced proper curves are projective.

Proof. We will produce an ample line bundle on C, which means that a high enough power of that gives a closed embedding to the projective space which proves that C is projective.

To do this, recall that on a reduced curve, the regular points are dense, there is a regular point on each component of C, let's consider the corresponding effective Cartier divisor and the corresponding line bundle. We want to prove that this line bundle is ample. We know from the previous proposition that we can check it by pulling back to the normalization, where you will have a regular curve. Now we can choose these regular points to be in the dense open where v happens to be an isomorphism, then we know that the pullback of this line bundle is

Recall that the normalization is a proper regular curve over k, therefore it's projective as we already proved this before. As a quick recap, we know that every irreducible regular proper curve admits an open embedding into a projective curve, but notice that this open embedding is also proper, therefore it's a closed embedding, thus finite, thus the composition is projective. Now if the curve is not irreducible, but still proper and regular, I claim that it's just a disjoint union of irreducible regular proper curves. This is because that since C is regular, then every point only has one irreducible component passing through it, then we know that different components don't have a point in common, therefore they are also the connected components, therefore we know that each open embedding of the components is also a closed embedding, then we only have to show that this finite disjoint union of projective varieties is projective, we only have to produce a ample line bundle, and notice that we proved that for proper schemes, Serre's cohomology criterion shows that we can check ampleness on each component, and we can pick an ample line bundle on each component,

and since they are disjoint, we can define a line bundle on the whole space by considering on each component finitely any we know that on each component it's ample, we are done.

In conclusion, the normalization is a projective regular curve over k and we have a line bundle on C and we wish to check that this line bundle is ample. Then recall that to check a line bundle is ample on a proper scheme, we can check it on each irreducible component of of the normalization. Notice that the pullback of the line bundle $\mathcal{L}$ to the normalization correspond to the line bundle associated to the effective Cartier divisor which is the inverse image of the regular closed points in C. To be more precise, if you consider the injective morphism:

$$\mathcal{L} = \mathcal{I} \hookrightarrow \mathcal{O}_C$$

Then you pull it back, obtain:

$$v^*\mathcal{L} \to v^*\mathcal{O}_C$$

The problem is that this may not be injective since the pullback morphism is only right exact. However, in our case this is indeed exact. To see this, notice that to check it's injective, we can restrict to opens and check there. First, we restrict to the open that excludes the inverse images of the finite closed points. We know that pullback commutes with restriction, then since we know that $\mathcal{I} \hookrightarrow \mathcal{O}_C$ is the identity downstairs, then the pullback is also the identity upstairs.

Then we can restrict to a open on each of the closed subset downstairs, where the normalization is an isomorphism, then the assertion is trivial. Therefore, we know that the pullback has a natural injection to the structure sheaf upstairs thus is an ideal sheaf, and it coincides with the line bundle associated to the effective Cartier divisor upstairs defined by these finite closed points. Then we further restrict this line bundle to each of the irreducible components, which is also open, thus this restriction is trivial, and it's just the line bundle corresponding the effective Cartier divisor on that component which is those points that lie in that component. We only need to prove that it's ample on this component. Notice that this line bundle is the tensor product of the line bundle determined by just one closed point, if there are multiple closed points in this component. Since tensor product of ample line bundles will be ample, we now assume that we work with a regular projective integral curve and a line bundle that is associated to a single closed point, we wish to prove that this is ample.

To do it, we only have to prove that a higher enough power of this line bundle is very ample. We first notice that if we want to prove that $\mathcal{L}$ is ample on C, by Serre's cohomology criterion, we need to show that $H^i(C, \mathcal{F} \otimes \mathcal{L}^i) = 0$ for all coherent sheaves $\mathcal{F}$ on C, but notice that we have the following result:

$$H^i(C, \mathcal{F} \otimes \mathcal{L}^{\otimes n}) \otimes K \simeq H^i(C_K, (\mathcal{F} \otimes K) \otimes (\mathcal{L} \otimes K)^{\otimes n})$$

Then what we are left is **** to be completed, don't know how to do it, it's true if we assume k is algebraically closed, but if not, I am not sure* □

Proposition 2.12. Every proper curve over k (not necessarily reduced) is projective.

Proof. To be completed. □

Proposition 2.13. A line bundle on a projective curve is ample if and only if it's of positive degree.

Proof. To be completed. □

3 Curves of Genus 0

We now use what we have learned before to answer the question, what are curves of genus 0. Recall that the curve $x^2 + y^2 + z^2 = 0$ in $\mathbb{P}^2_{\mathbb{R}}$ is of genus 0 (the genus is computed by $(d-1)(d-2)/2$), but I claim it is not isomorphic to $\mathbb{P}^1_k$ even if we know that $\mathbb{P}^1_k$ also has genus 0. The reason is that it doesn't have any $\mathbb{R}$-valued point. The reason is that $x^2 + y^2 + z^2 = 0$ doesn't have any real solution except for $x = y = z = 0$, but this is not a point in $\mathbb{P}^2_{\mathbb{R}}$. To make it more precise, we know that since any k-algebra morphism:

$$k[x_0, \cdots, x_n]/f \to k$$

is determined by where x_i goes such that f is mapped to 0, we know that if f doesn't have a solution, then we know that there is not k-valued point.

It turns out that this is not a coincidence, as we will show below: a genus zero curve with a k-valued point is isomorphic to 0. Again, we will assume that all curves is projective, geometrically integral and geometrically regular

Proposition 3.1. Let C be a genus 0 curve, such that $p \in C$ is a k-valued point, then $\mathbb{C} \simeq \mathbb{P}^1_k$.

Proof. Let p be such a point and consider $\mathcal{L} = \mathcal{O}(p)$, which is of degree 1, then we know we can compute the dimension of the global section using degree and genus since $- > -2$. Then we know that $h^0(C, \mathcal{O}(p)) = 2$ and we know that it's very ample since $1 \geqslant 2 \cdot 0 + 1$, therefore, the complete linear series $|\mathcal{O}(p)|$ gives a closed embedding to $\mathbb{P}^1_k$. However, recall that the only closed embedding to $\mathbb{P}^1$ of something that is also integral of dimension 1 is an isomorphism. □

Corollary 3.2. There are no degree 1 line bundles on $x^2 + y^2 + z^2 = 0$ in $\mathbb{P}^2_{\mathbb{R}}$.

Proof. If there is, then apply the above argument, we know that it's isomorphic to $\mathbb{P}^1$, which is a contradiction. □

This example shows that over a non-algebraically closed field (even if the curve is regular), there might be a curve who has genus 0, but not isomorphic to $\mathbb{P}^1$.

Proposition 3.3. All genus 0 curves can be described as conics in $\mathbb{P}^2_k$.

Proof. Any genus 0 curve has a degree 2 line bundle, i.e. the dual of the dualizing sheaf $\omega_C^\vee$, which has genus $-2g + 2 = 2$.

Now since $2 \geqslant 1$, we know that this sheaf is very ample, then since the dimension of global sections is $2 + 1 = 3$ it gives a closed embedding into $\mathbb{P}^2_k$.

Now we have to show that this is a conic in $\mathbb{P}^2_k$, i.e. it can be cut out by a homogeneous polynomial of degree 2. First, we notice that the since this regular curve is embedded using a line bundle of degree 2, we know that the degree of this closed embedding is 2. Consider the map:

$$\mathrm{Sym}^2 H^0(C, \mathcal{L}) \to H^0(C, \mathcal{L}^{\otimes 2})$$

which is defined using the product of $H^0(C, \mathcal{L})$ to $H^0(C, \mathcal{L}^{\otimes 2})$. Notice that the first space is of degree 6 but the second space, as the global section of a line bundle of degree 4, is of dimension 5, therefore is has nontrivial kernel.

Now, if you consider the following diagram:

$$\begin{array}{ccc} \mathrm{Sym}^2 H^0(\mathbb{P}^2_k, \mathcal{O}(1)) & \xrightarrow{\simeq} & H^0(\mathbb{P}^2_k, \mathcal{O}(2)) \\ \downarrow \simeq & & \downarrow \\ \mathrm{Sym}^2 H^0(C, \mathcal{L}) & \longrightarrow & H^0(C, \mathcal{L}^{\otimes 2}) \end{array}$$

we know it's commutative and we also know that the top horizontal map is an isomorphism. Therefore, the fact that the morphism below has a nontrivial kernel implies that the vertical morphism on the right has a nontrivial kernel, say f is one conic in the kernel.

I claim that f is the conic we desire. The reason is simple, our goal is to find a conic f such that $V(f)$ is the image of $i : C \hookleftarrow \mathbb{P}^2$. Recall that how this closed embedding i is defined, it's defined locally by on $D_+(x_i)$ $\frac{x_j}{x_i}$ goes to trivializations of the basis of global sections of $\mathcal{L}$. Then I will let you think about why $\frac{f}{x_i^2}$ is mapped to 0, thus the image is contained in $V(f)$, or in other words, we have the following diagram:

$$C \hookrightarrow V(f) \hookrightarrow \mathbb{P}^2_k$$

We now only have to show that the closed embedding $C \hookleftarrow V(f)$ is an isomorphism. Recall that both of them has degree 2 in $\mathbb{P}^2$ and degree is the leading coefficient of the linear term of the Hilbert polynomial of $C, V(f)$. Notice that the Hilbert polynomial of $V(f)$ is $2m + 1$ and the Hilbert polynomial of C is also $2m + 1$, then we know that they have the same Hilbert polynomial, thus by a previous exercise, they are the same closed embedding. □

Proposition 3.4. Suppose that C is a genus 0 curve, still projective, geometrically integral and regular. Then C has a point of degree at most 2.

Proof. Suppose that the closed embedding of degree 2, $i : C \to \mathbb{P}^2$ is given by the line bundle $\mathcal{L}$ of degree 2. Then since we work with a regular curve, there is a divisor D such that $\mathcal{O}(D) \simeq \mathcal{L}$ and since we know that $\mathcal{O}(D)$ is just the tensor product of a few $\mathcal{O}(p)$ for closed points p, then using the fact that degree is additive upon tensor, we know that degree of each $\mathcal{O}(p)$ is at most 2. □

4 Classical Geometry Arising from Curves of Positive Degree

Now we begin to investigate curves of positive genus, and before that we will introduce a useful proposition when we study curves of positive degree and use it as an excuse to say something about classical geometry using modern point of view.

Proposition 4.1. Let C be a projective, gr, gi curve over a field k and suppose that C is not isomorphic to $\mathbb{P}^1_k$, with no assumption on the genus of C, and $\mathcal{L}$ is a line bundle of degree 1, then $h^0(C, \mathcal{L}) < 2$.

Proof. If $\mathcal{L}$ is a degree 1 line bundle whose global sections has dimension at least 2, the pick any two linearly independent sections. Since the degree of $\mathcal{L}$ is one, then the divisor determined by these two sections s_1, s_2 are a single closed point with degree 1, then if they vanish at the same point, then consider the regular function $\frac{s_1}{s_2}$ in $\mathcal{O}_C$, this is going to be a regular function on C, but you know that since the regular functions on C are all constants(after base change to C_K where K is the algebraic closure), then s_1, s_2 are dependent, contradiction. (You may want to make this precise by think about $\mathcal{L} \otimes \mathcal{L}^\vee$). Then these two sections determines a morphism to $\mathbb{P}^1_k$ and I claim that this is a closed embedding thus an isomorphism. This is first a finite morphism since it's projective and finite fiber and we already proved it's degree 1 using a previous proposition.

Then we know that the induced extension of function field is a degree 1 extension, this is because that the pushforward of the structure sheaf is locally constant of rank 1, therefore, we know that the fiber at the generic point is 1 dimensional over the function field, and the fiber at the generic point is just the function field, thus as a degree one extension, it's an isomorphism, thus we are done since we know that integral regular curves whose function fields are isomorphic will be isomorphic as curves. □

The following corollary is also very helpful:

Corollary 4.2. If C is a projective, gr, gi curve over k, not isomorphic to $\mathbb{P}^1_k$, then $\mathcal{O}_C(p) \simeq \mathcal{O}_C(q)$ iff $p = q$ for degree 1 points p, q.

Proof. Say $\mathcal{O}_C(p) \simeq \mathcal{O}_C(q)$ but $p \neq q$, then recall that $\mathcal{O}_C(p)$ has a global section whose divisor is q and it also has a global section whose divisor is q, again, these two sections are linearly independent, but this contradicts the fact that the dimension of the global sections will be less then 2. □

Proposition 4.3. Suppose that C is a projective, gr, gi curve over an algebraically closed field, then it's of genus 0 iff all degree 0 line bundles are trivial.

Proof. Say it's of genus 0, then we know that a degree 0 line bundle has degree larger than -2, thus the dimension of the global sections is 1, thus it's trivial.

Then conversely, say that all degree 0 line bundles have dimension 1 global sections. Let's assume that C has positive genus, then it's not isomorphic to $\mathbb{P}^1$ as the genus of $\mathcal{P}^1$ is 0. However, choose two distinct closed points, p, q, we know that $\mathcal{O}(p - q)$ is a degree 0 line bundle which is not trivial from the above corollary, but on the other hand, by assumption, the dimension of global sections is 1, thus the line bundle is trivial, a contradiction. □

Now we prove something that help us to understand the classical geometry we are going to talk about later:

Proposition 4.4. Suppose that C is a gr, gi projective plane curve of degree $e > 2$, and D_1, D_2 are two plane curves of degree d that doesn't contain C. By Bezout's Theorem, we know that since D_1, D_2 doens't contain the generic point of C, the degree of the intersection $D_i \cap C$ is de(we know that the intersection is just a finite collection of closed points).

Now suppose that $D_1 \cap C$ and $D_2 \cap C$ have $de - 1$ "same points" in common, then the last point is also the same. To be precise, suppose that there is an effective Cartier divisor E in C such that $D_i \cap C = E + p_i$ for some degree 1 point p_i and $i = 1, 2$, then $p_1 = p_2$.

Proof. Notice that since p_1 and p_2 are all of degree 1, we want to use the above proposition, i.e. we will show that $\mathcal{O}(p_1) \simeq \mathcal{O}(p_2)$ since we know that the degree of C is larger than 2, thus it can not be isomorphic to $\mathbb{P}^1$ since for we know that the genus of a degree e hypersurface in $\mathbb{P}^2$ is computed by $(e-1)(e-2)/2$, which is not 0, thus it's not isomorphic to $\mathbb{P}^1$, thus the corollary above can be applied.

Then we show that $D_i \cap C$ is an effective Cartier divisor in C, recall that this is a complete intersection in $\mathbb{P}^2$, thus $D_i \cap C$ is indeed an effective Cartier divisor in C. We are now assuming that this effective Cartier divisor can be written as the sum of two effective Cartier divisors $E + p_i$, and recall that this means that the corresponding invertible sheaf of $D_i \cap C$ is the tensor product of that of E and p_i. Therefore we have an isomorphism:

$$\mathcal{O}(E) \otimes \mathcal{O}(p_1) \simeq \mathcal{O}(E) \otimes \mathcal{O}(p_2) \Rightarrow \mathcal{O}(p_1) \simeq \mathcal{O}(p_2)$$

we are done. □

As two interesting applications if the above result, we prove two classical result:

Theorem 4.5. Suppose that l, m are distinct lines in the projective plane and α, β, γ are distinct points on l and α', β', γ' are distinct points on m with all six points different from $l \cap m$, then the points $x = \overline{\alpha\beta'} \cap \overline{\alpha'\beta}, y = \overline{\alpha'\gamma} \cap \overline{\alpha\gamma'}$ and $z = \overline{\beta\gamma'} \cap \overline{\beta'\gamma}$ are colinear.

The above theorem is called **Pappus's Theorem** and it will be the degenerate case of the following theorem:

Theorem 4.6. If a hexagon $\alpha\gamma'\beta\alpha'\gamma\beta'$ is inscribed in a smooth conic K and the opposite pairs of sides are extended until they meet, then the three intersection points x, y, z are colinear.

Remark 4.7. This theorem is always called **Pascal's theorem** and the above Pappus's Theorem can be viewed as a degeneration case. The reason is also simple, recall that the scheme-theoretic union of two lines in $\mathbb{P}^2$ is also a conic as if we assume that $ax + by + cz = 0$ cuts the first line and $dx + ey + fz = 0$ cuts out the second line, then the scheme-theoretic union is cut cut out by $(ax + by + cz)(dx + ey + fz) = 0$, which is also a conic.

And you can see from this that the condition that the six distinct points are inscribed in this conic just means that the conic contains these six points.

Before we prove Pascal's Theorem, we can use it to prove the following:

Proposition 4.8. Suppose that $\alpha, \beta, \gamma, \alpha', \beta'$ are five points in $\mathbb{P}^2_{\mathbb{R}}$ no three on a line, then there is a unique conic K passing through the five points and is regular.

Proof. *** to be completed □

Now let's prove Pascal's theorem, and for convenience we will assume that k is algebraically closed, even though this can be removed:

Proof. Let's first do some preparations. First, notice that for distinct two lines in $\mathbb{P}^2$, they meet at exactly one k-valued point, i.e. degree 1 point. Then if you unpack what we need to prove, we need to make sure that the line $\overline{xy}$ meets $\overline{\beta\gamma'}$ and $\beta'\gamma$ at the same point *** to be completed □

5 Hyperelliptic Curves

Let's assume in this section that the field k is algebraically closed and k is not of characteristic 2.

A projective regular integral curve C of genus g is called **hyperelliptic** if it admits a double cover, i.e. degree 2 finite morphism to $\mathbb{P}^1_k$. When we say that C is hyperelliptic, we implictly mean that we have in mind a choice of this double cover map $\pi : C \to \mathbb{P}^1$. We will later see that if $g \geqslant 2$, then there always at least one such morphism and this morphism π is called the **hyperelliptic map**. Recall that as this finite morphism is of degree 2, and we can compute the degree using preimages of closed points. Recall that this morphism is always surjective, this is because that this morphism is always dominant, and this is again because that it's not a constant map (recall that finite ring maps are integral, and for integral ring maps $A \to B$ we know that if $p \subset q$ and $p \neq q$ in B, then the inverse image is different.). Now finite plus dominant between integral schemes implies surjective, this again follows the properties of integral extension.

Now we know the preimage of a closed point $p \in \mathbb{P}^1_k$ can only possibly be 1 or 2 points, if $\pi^{-1}p$ consists of only one point, we say that p is a **branch point** and $\pi^{-1}p$ is a **ramification point** of π.

All these stuff will be discussed in detail later, but right now, we can prove the following special case of **Riemann-Hurwitz formula**:

Theorem 5.1. Suppose that $k = \overline{k}$ and char$k \neq 2$, then if $\pi : C \to \mathbb{P}^1$ is a double cover by a projective regular integral genus g curve over k, then there are $2g + 2$ branch points for π.

In complex geometry, this is a generalization of the statement that a genus one complex curve covers $\mathbb{P}^1$ branching at four points.

To prove this theorem, we need the following result:

Proposition 5.2. Assume that char$k \neq 2$ and $k = \overline{k}$, given r distinct points $p_1, \cdots, p_r \in \mathbb{P}^1$, there is precisely one double cover branched at precisely these points if r is even and none if r is odd, all modding out automorphisms of C over $\mathbb{P}^1_k$.

Proof. First, we know that by an appropriate automorphism of $\mathbb{P}^1$, I can assume that none of these r points are either $0 = [1 : 0]$ or $\infty = [0 : 1]$. This is becasue that since k is algebraically closed, we can assume that besides the r points, there are still two other points, and we already know that the automorphic on $\mathbb{P}^1$ acts strictly three transitively on $\mathbb{P}^1$, therefore we can assume that there is an automorphism such that after we apply it, $[1 : 0]$ and $[0 : 1]$ are not the branch points.

Now we can assume that all branch points are in $\mathbb{P}^1 - \{\infty\} = \mathbb{A}^1 = Speck[x]$. To study this, we first study a double cover of $\mathbb{A}^1$, $C' \to \mathbb{A}$ with x the coordinate on $\mathbb{A}^1$. We know that we have a quadratic (i.e. degree 2) field extension K over $k(x)$, since char$k \neq 2$, this will be a Galois extension. This is because the minimal polynomial is $T^2 - f(x)$ where $f(x) \in k(x)$ is square free for a degree 2 extension and we know that when char$k \neq 2$, this polynomial is separable since the derivative is not 0. This is also normal since the extension is $k(x, y)/(y^2 - f(x))$ and this polynomial $T^2 - f(x)$ has roots $y, -y$ that is in $k(x, y)/(y^2 - f(x))$ and we know that this is a finite, separable, normal extension thus is Galois and the order of the Galois group is 2, then we consider the nontrivial element σ in the group(the Galois involution):

$$\sigma : K \to K$$

we let y be the element such that $\sigma(y) = -y$ and $y, 1$ will be the basis of K over $k(x)$, and are eigenvectors of σ, we know that $\sigma(y^2) = y^2$, so $y^2 \in k(x)$ and say $y^2 = \frac{f}{g}$. Now since k is algebraically closed, we can replace y by an appropriate multiple of $k(x)$ such that y^2 is in $k[x]$ and is monic (for example we can first replace y by gy, then looking at fg, we read off the leading coefficient c, and since k is algebraically closed, there is a b such that $b^2 = c$).

Now assume that $y^2 = x^N + a_{N-1}x^{N-1} + \cdots + a_0$ where the polynomial on the right call it $f(x)$ has no repeated roots (if it has, we can again muldify y to eliminate it). Now consider the curve C'_0 in $\mathbb{A}^2_k$ cut out by $y^2 = x^N + a_{N-1}x^{N-1} + \cdots + a_0$ or in other words, by $y^2 - x^N + a_{N-1}x^{N-1} + \cdots + a_0 = 0$, we know that since this has no repeated roots, after we compute the derivative with respect to x, there is no place where it vanishes, thus there are no singular closed points, thus C'_0 is a regular curve, thus normal. Then we know that C' and C_0 are both normalizations of $\mathbb{A}^1_k$ in the finite extension of function field generated by y (both of them have the same function field). Therefore, we know that C'_0 and C' are isomorphic, therefore,

we have obtained a explicit construction of C' over $\mathbb{A}^1_k$. Now consider the branch points, of $C'_0 \to \mathbb{A}^1_k$, which are points whose inverse image is only one point. Consider the diagram below of fibers:

$$\begin{array}{ccc} k[y]/(y^2 - f(a)) & \longleftarrow & k \\ \uparrow & & \uparrow{\scriptstyle x\mapsto a} \\ k[x,y]/y^2 - x^N + a_{N-1}x^{N-1} + \cdots + a_0 & \longleftarrow & k[x] \end{array}$$

we know that the fiber has 1 point, since k is algebraically closed, iff when $f(a) = 0$ where $f(x) = x^N + a_{N-1}x^{N-1} + \cdots + a_0$. Therefore, we know that the branch points of $\mathbb{A}^1$ are exactly the roots of f.

Now we consider the case over $\mathbb{P}^1_k$. Notice that there are two affine covers of $\mathbb{P}^1_k$, the first one is $Speck[x]$ and the other one is $Speck[u]$ and the two are glued using $u = \frac{1}{x}$. Now suppose that:

$$C \to \mathbb{P}^1_k$$

is a double cover, then we know that if you consider the corresponding morphism from the inverse image to $Speck[x]$ and to $Speck[u]$, they are also finite and the degree is also 2 since the degree can be computed using inverse image of closed points and valuations. Then we know how $C \to \mathbb{P}^1_k$ looks like over each of the two affine covers $\mathbb{A}^1$ by the discussion we had before and the only problem is how to glue them together.

Recall that since the function field of C is the same as those of the inverse image over the two $\mathbb{A}^1_k$, thus we can apply the same argument to $Speck[u]$ and obtain that $C'' \to Speck[u]$ is just:

$$Spec[Z,u]/(Z^2 - (u - 1/p_1)\cdots(u - 1/p_r))$$

Here we have to use the reciprocal of p_i since if we are think that the function field extension in the following diagram:

$$\begin{array}{ccc} k(x) & \longrightarrow & K \\ {\scriptstyle x\mapsto \frac{1}{u}}\downarrow & \nearrow & \\ k(u) & & \end{array}$$

thus we know that u is mapped to the inverse of x thus we know that $y^2 = f(\frac{1}{u})$, then we use Z instead of y and get the above description. Notice that we can modify this ideal: $(Z^2 - (u - \frac{1}{p_1})\cdots(u - \frac{1}{p_r}))$ and it's $(((-1)^r \prod p_i)Z^2 - u^r f(1/u))$. Therefore, to glue them, we have the following picture:

$$\begin{array}{ccccccc} k[Z,u]/((-1)^r\prod p_i)Z^2 - u^r f(1/u) & \to & k[Z,u,\frac{1}{u}]/((-1)^r\prod p_i)Z^2 - u^r f(1/u) & \leftarrow & k[y,x,\frac{1}{x}]/y^2 - f(x) & \leftarrow & k[y,x]/y^2 - f(x) \\ \uparrow & & \uparrow & & \uparrow & & \uparrow \\ k[u] & \longrightarrow & k[u,\frac{1}{u}] & \underset{x\mapsto\frac{1}{u}}{\longleftarrow} & k[x,\frac{1}{x}] & \longleftarrow & k[x] \end{array}$$

and we need a k-algebra isomorphism in the middle on the top row such that the square in the middle commutes.

I now claim that this translates to the following situation: we need that in $K(C)$, i.e. the function field of C, the following equation holds:

$$z^2 = u^r f(1/u) = f(x)/x^r = y^2/x^r$$

where z is obtained by multiplying Z by a square roof of $(-1)^r \prod p_i$. This is because if there is such a ring isomorphism (k-algebra isomorphism), then we know that x is already determined to go to $\frac{1}{u}$, thus we don't have a choice for $\frac{1}{x}$ as well, therefore we can only determine y such that $y^2 - f(x)$ goes to 0. Then in the function field, $y^2/x^r = f(x)/x^r$ is mapped to $u^r f(\frac{1}{u}) = z^2$, thus we know that in the ring morphism y^2 should be mapped to $z^2 x^r$. In other words, where y^2 should go is already determined, then if this equation $y^2 = z^2 x^r$ has a solution, for example when r is even, we can take $y = \pm z x^{r/2}$ and these two gluing result in the same C (differ by an automorphism of C over $\mathbb{P}^1$, notice that this minus sign gives an isomorphism on the gluing it's y, z that are affected by the minus sign, thus you can project u, x down to $\mathbb{P}^1$ without being

affected), thus we are done if we can prove this is an isomorphism. Notice that it's easy to see that this is a surjective morphism, and by computing the transcendence degree of the function field, we know the two rings are of the same dimension and they are integral domains, thus we know that this is an isomorphism since surjective morphism between integral domains of the same dimension is an isomorphism.

However, this r is odd, I claim that there is no solution of $y^2 = x^r z^2$, i.e. there is no such gluing and this the content of the following proposition: □

Proposition 5.3. Suppose that char$k \neq 2$, then x doesn't have a square root in the field $k(x)[y]/(y^2 - f(x))$ where f is a polynomial with nonzero roots $p_1, \cdots, p_r$

Proof. Let's first consider the following question: I claim that $\sqrt{3}$ is not in the field $\mathbb{Q}(\sqrt{2})$. Recall that this is a degree 2 extension of $\mathbb{Q}$, therefore a basis is $1, \sqrt{2}$, then we know that every element is uniquely of the form $a + b\sqrt{2}$, then if $\sqrt{3}$ is in this field, we know that $a^2 + 2b^2 + 2ab\sqrt{2} = 3$, therefore we know that $ab = 0$ by comparing the coefficients, then $a^2 + 2b^2 = 3$ and $a = 0$ or $b = 0$, therefore we are just asking if there is a rational number x such that $x^2 = 3$ or $x^2 = \frac{3}{2}$, and the question is transferred back to $\mathbb{Q}$, and the answer is no.

Back to our question, we know that every element in the field can be written as $a + b\sqrt{f(x)}$, and if x has a square, we know that:

$$a^2 + b^2 f(x) + 2ab\sqrt{f(x)} = x$$

then we are just asking is there is an element n in $k(x)$ such that $n^2 = x$ or $n^2 = \frac{x}{f(x)}$ and there is no such element and we can use the fact that $k[x]$ is a DVR and we know that for every $n \in k(x)$, the valuation of n^2 in $k(x)$ should be even, but we know that x has valuation 1 at $x = 0$, contradiction. Then when f has non zero roots, we know that $\frac{x}{f(x)}$ has valuation 1 at $x = 0$.

Then we explain why this helps us to answer the question: whether $x^r z^2$ or equivalently y^2/x^r is a square or not in $K(C)$. Recall that $K(C)$ can be viewed as the field $k(x)[y]/(y^2 - f(x))$, and when r is odd, we know that if y^2/x^r is a square, then $(a + b\sqrt{f(x)})^2 = y^2/x^r$, or in other words, we know that:

$$a^2 + f(x)b^2 = f(x)/x^r$$

and $a = 0$ or $b = 0$, then if $b = 0$, we are asking if $a^2 = f(x)/x^r$. I claim that in our case, $x = 0$ is not a root of $f(x)$, and if this holds, we know that the valuation of $f(x)/x^r$ at $x = 0$ is odd, thus not a square. To see this, recall that in our preparation, we already used a automorphism of $\mathbb{P}^1$ and avoided $x = 0$ and $u = 0$ being a branch point, therefore we are done. □

Remark 5.4. For future reference, we write down here the explicit description (two affine) of the hyperelliptic cover $C \to \mathbb{P}^1$:

$$\begin{array}{ccc} k[x,y]/(y^2 - f(x)) & \xleftrightarrow{z \mapsto \frac{y}{x^{r/2}}} & k[u,z]/(z^2 - u^r f(\frac{1}{u})) \\ \uparrow & & \uparrow \\ k[x] & \xleftrightarrow[x \mapsto \frac{1}{u}]{} & k[u] \end{array}$$

Now we go back to the proof of the Riemann-Hurwitz formula:

Proof. Our explicit description of the double cover of $\mathbb{P}^1$ indicates that first, the brach points can only be even and larger than 2 on $\mathbb{P}^1$ for algebraically closed field. This will correspond to $2g + 2$ for $g \geqslant 0$.

Now, our strategy is to watch every such double cover $C \to \mathbb{P}^1_k$ with $2g + 2$ branch points, and prove that the genus of C is g. Recall that this explicit description of C using two affine covers helps us to compute everything using Cech complex, thus $g = h^1$. Therefore, let's consider the Cech complex:

$$0 \longrightarrow k \longrightarrow k[x,y]/(y^2 - f(x)) \times k[u,z]/(z^2 - u^r f(\tfrac{1}{u})) \xrightarrow{d}$$

$$(k[x,y]/(y^2 - f(x)))_x \longrightarrow 0$$

and we need to compute the cokernel of d to figure out the dimension of h^1.

First, I will let you think about why there is a basis consisting of $x^n y^m$ with $n \in \mathbb{Z}$ and $m = 0, 1$ for $(k[x,y]/(y^2 - f(x)))_x$. Then notice that the morphism $k[x,y]/(y^2 - f(x)) \to (k[x,y]/(y^2 - f(x)))_x$ can gives you all the basis $x^n y^m$ for n being a nonnegative integer and $y = 0, 1$. Then if you think about the map $k[u,z]/(z^2 - u^r f(\frac{1}{u})) \to (k[x,y]/(y^2 - f(x)))_x$ since z is mapped to $\frac{y}{x^{r/2}}$, you get all the basis $x^{-n}(\frac{y}{x^{r/2}})^m$. Thus you can see that all the basis that the linear combinations are missing are $x^{-1}y, x^{-2}y, \cdots, x^{-\frac{r}{2}+1}y$, thus the dimension is $\frac{r}{2} - 1 = g + 1 - 1 = g$, we are done. □

Remark 5.5. As a consequence of the hyperelliptic Reimann-Hurwitz formula, we can obtain curves of each genus if we work with an algebraically closed field of characteristic not 2. To be precise, we have already proved that there are double cover $C \to \mathbb{P}^1$ that branch at $2g + 2$ points for each $g \geqslant 0$ and the genus of the curve C is g, thus we have obtained curves for genus $g \geqslant 0$.

We will later show that every genus $g \leqslant 2$ curve over an algebraically closed field of characteristic not 2 can be obtained using this description. However, for $g > 2$, we will later give you a vague evidence that most of the curves don't arise as a hyperelliptic curve.

Proposition 5.6. A regular, projective, integral curve C of degree at least 1 over an algebraically closed field has a double cover of $\mathbb{P}^1$ iff it admits a degree two invertible sheaf $\mathcal{L}$ with $h^0(C, \mathcal{L}) = 2$.

Proof. Let's first assume that C admits a double cover of $\mathbb{P}^1$, then we want to show that it has a degree 2 line bundle with exactly 2 linearly independent global sections. We know that it has at least 2 linearly independent sections, that is the pullback of x_0 and x_1. This is because this morphism, being a degree 2 cover, is surjective, thus the pullback of x_0 and x_1 will not vanish at exactly the same locus, thus they are not independent. Now I claim that it only has these two linearly independent sections. To see this, first notice that $\mathcal{L}$ is base point free and then notice that $h^0(C, \mathcal{L}(p)) - h^0(C, \mathcal{L}) = 1$ since $h^0(C, \mathcal{L}(p))$ is base point free, then we can keep going by tensoring with $\mathcal{O}(p)$ as tensor of base point free is base point free, then we know that $h^0(C, \mathcal{L}(np)) - h^0(C, \mathcal{L}) = n$ and we know that when n is large enough, the degree of $\mathcal{L}(np)$ is large enough, then we can compute the global dimension using:

$$h^0(C, \mathcal{L}(np)) = \deg \mathcal{L} + n - g + 1$$

and we know that its at most $2 + n$, then we know that $h^0(C, \mathcal{L})$ is at most $\deg \mathcal{L}$. Then if we can prove that $\deg \mathcal{L}$ is 2, we are done. Recall that since C is regular, we can compute the degree of the line bundle using global section. Then we can pullback global sections of $\mathcal{O}(1)$ and use it to compute the degree. Recall that this is a degree 2 cover and the branch points are only finite, we choose one of the non branch points and conclude that the inverse image are two points, and we know that the valuation of that global section at that point are both going to be 1. Or you can also use branch points to do this, but this time, the inverse image is only of point, but the valuation there is going to be 2, thus no matter how you compute the degree, it's going to be 2.

Conversely, suppose that it has a degree 2 line bundle with global section of dimension 2. Let's first prove that it's base point free, thus giving a morphism to $\mathcal{P}^1$, and it's automatically finite, similarly, you can compute the degree using inverse images and valuation to show that this morphism is of degree 2. To prove it's base point free, let's assume that for the sake of contradiction, there is a base point of $\mathcal{L}$, then we know that the dimension of $\mathcal{L}(-p)$ is still 2 whose degree is 1, but we already saw that if C is not isomorphic to $\mathbb{P}^1$, and degree 1 line bundle can not have dimension 2 global sections, a contradiction since the genus of C is 1, not isomorphic to $\mathbb{P}^1$. We are done. □

Remark 5.7. In the process of proving this above proposition, we actually proved that if C is of genus at least 1, then any degree 2 line bundle that has at least 2 linearly independent sections at most have 2 and it's base point free, and it gives a hyperelliptic map.

Proposition 5.8. Assume $g \geqslant 2$, if $\mathcal{L}$ correspond to a hyperelliptic cover $C \to \mathbb{P}^1$, then $\mathcal{L}^{\otimes g-1} \simeq \omega_C$.

Proof. Recall that if $\mathcal{L}$ is a degree $2g - 2$ invertible sheaf with g independent sections (or at least g since it's either g or $g - 1$), is isomorphic to the dualizing sheaf. Therefore this is our goal.

Now to prove this, we compose the hyperelliptic map with the $g - 1$ Veronese embedding:

$$C \xrightarrow{\pi} \mathbb{P}^1_k \xrightarrow{|\mathcal{O}(g-1)|} \mathbb{P}^{g-1}_k$$

then we know that this morphism correspond to the linear series of $\mathcal{L}^{\otimes g-1}$. Now notice that the degree of $\mathcal{L}$ is 2, which can be still computed using the pullback of global sections, therefore we know that the degree of $\mathcal{L}^{\otimes g-1}$ is $2g-2$. Then if we can show that it has g independent sections, we are done.

We only have to show that it at least have g independent sections since we know that it at most has g independent sections. I claim that the pullback map $H^0(\mathbb{P}^{g-1}, \mathcal{O}(1)) \to H^0(C, \mathcal{L}^{\otimes g-1})$ is injective, then since the dimension of $H^0(\mathbb{P}^{g-1}, \mathcal{O}(1))$ is g, we are done. Suppose that x is in $H^0(\mathbb{P}^{g-1}, \mathcal{O}(1))$ such that f^*x is 0. If you examine what this means, if it vanishes, we know that this morphism is degenerate and conversely, if it doesn't vanish, it's not degenerate. Therefore, we only have to show that this is not degenerate. The reason is simple, we know that Veronese embedding is a complete linear series, thus not degenerate and π is surjective, thus the composition is not degenerate. □

Remark 5.9. The fact that $H^0(\mathbb{P}^{g-1}, \mathcal{O}(1)) \to H^0(C, \mathcal{L}^{\otimes g-1})$ is injective immediately implies that it's an isomorphism, thus this composition morphism is a complete linear series and you can also use this to show that it's not degenerate.

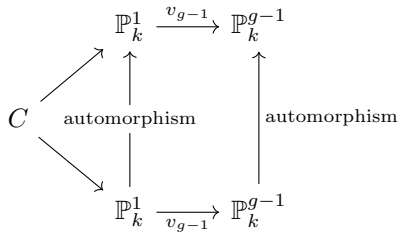
Now we can classify hyperelliptic curves over an algebraically closed field not of characteristic 2:

Proposition 5.10. Any curve C of genus at least 2 admits at most 1 double cover of $\mathbb{P}^1$. More precisely, if $\mathcal{L}$ and $\mathcal{M}$ are both line bundles that gives a degree 2 morphism to $\mathbb{P}^1_k$ (then automatically the degree of $\mathcal{L}$ and $\mathcal{M}$ is 2 and they have exactly 2 linearly independent sections), then $\mathcal{L} \simeq \mathcal{M}$.

Proof. Before we proceed, we need to make a remark, the morphisms $C \to \mathbb{P}^1$ defined by $\mathcal{L}$ and $\mathcal{M}$ could differ by an automorphism of $\mathbb{P}^1$, and you will see this feature in the proof.

Recall that if we consider some complete linear series $|\mathcal{L}|$, which gives you a morphism $X \to \mathbb{P}^n$, this is actually not a one hundred percent clear statement, since and I will let you think why this actually represent morphisms to $\mathbb{P}^n$ modding out automorphisms of $\mathbb{P}^n$ (they are in bijection with PGL_n), or in other words, two such morphism can differ by an action of something in PGL_n.

Then we know that if you have two line bundles $\mathcal{L}, \mathcal{M}$, then you can compose it with this $g-1$-th Veronese embedding and the result will be a morphism to $\mathbb{P}^n$ induced by ω_C, then they differ by an automorphism of $\mathbb{P}^n$, then the following diagram is commutative:



where we can choose the automorphism of $\mathcal{P}^1_k$ to make the square commute. This is because the automorphism of $\mathbb{P}^{g-1}_k$ preserves the image of $\mathbb{P}^1_k$. Notice that the automorphism can be written as a matrix in PGL_2, say it's:

$$B = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Recall that this matrix acts three transitively on $\mathbb{P}^1$, therefore, we only need to make sure where $p_1 = [1 : 0], p_2 = [0 : 1], p_3 = [1 : 1]$ are mapped to uniquely determine B, but we know that the automorphism preserves v_{g-1}, then say we call if α, we only need to find where $\alpha(v_{g-1}(p_i))$ goes, we are done.

This also proves that $\mathcal{L} \simeq \mathcal{M}$ and details are left for you. □

Remark 5.11. This morphism determined by the dualizing sheaf ω_C, or sometimes called the canonical bundle, is called the **canonical morphism**(modding out the automorphism of the target). We will use this a lot when we discuss curves of other genus, and especially elliptic curves.

Recall that when we constructed the hyperelliptic cover $\pi : C \to \mathbb{P}^1$, we saw that for each even number of branch point on $\mathbb{P}^1$, there is exactly one nontrivial, automorphism of C over $\mathbb{P}^1$(i.e. the one where we choose the negative sign instead of the positive sign and obtain another gluing), and this is called the **hyperelliptic involution**, denoted by ι:

Proposition 5.12. Suppose that C is a hyperelliptic curve of genus at least 2, then the hyperelliptic involution commutes with any other automorphisms of C.

Proof. Suppose that g is an automorphism of C, we just want to show that:

$$g \circ \iota \circ g^{-1} = \iota$$

If we can prove that this is still an automorphism of C over $\mathbb{P}^1$, we are done, since we know that this is of order 2 (conjugation preserves order), we are done since there is only one nontrivial order two automorphism of C over $\mathbb{P}^1$, i.e. ι.

To show this is indeed an isomorphism over $\mathbb{P}^1$, notice that $\pi \circ g$ is a degree 2 finite morphism to $\mathbb{P}^2$, then since we know that there is a unique automorphism ϕ of $\mathbb{P}^1$ such that we know that:

$$\pi \circ g = \phi \circ \pi$$

Therefore we know that if we compute:

$$\pi \circ g \circ \iota \circ g^{-1} = \phi \circ \pi \circ \iota \circ g^{-1} = \phi \circ \pi \circ g^{-1} = \pi \circ g \circ g^{-1} = \pi$$

we are done. □

Remark 5.13. By what we have discussed in this section (the following will only be a vague discussion since we didn't laern any thing about moduli spaces at all), we find that given any $2g+2$ points on $\mathbb{P}^n$, we can modulo the symmetric group S_{2g+2} (as the order of this points is not important), then mod out the automorphisms of $\mathbb{P}^1$, and we get all the degree $g \geqslant 2$ hyperelliptic curves. Therefore, in some sense, you find that the dimension of the space of hyperelliptic curves is $2g + 2 - \text{dimAut}\mathbb{P}^1_k = 2g - 1$.

After you learn moduli spaces, you can make this discuss precise.

6 Curves of Genus 2

Remark 6.1. In this section, we will start officially study positive genus and investigate curves of genus 2. The reason we skip curves of genus 1 is because that the theory of genus 1 curves are very rich so we will later discuss them in great details and since curves of higher genus is not related to genus 1 in any essentialy way, we can fist end our discussion on higher genus and come back to genus 1.

Genus 2 curves don't have quite enough interesting properties we can say now, thus we first start with a general comment:

In general, curves can have quite different behaviors due to different genus. For example, we know that a genus 0 curves (projective, gr,gi) can have infinitely many rational points (k-valued points), and so is genus 1 curves, which you will see later when we study elliptic curves. But by Flating's theorem, people know that curves of genus at least 2 only have finitely many rational points. Therefore, before the proof of Fermat's last theorem, we know that in $\mathbb{P}^2$, since the curve $x^n + y^n = z^n$ for $n \geqslant 4$ has genus $(d-1)(d-2)/2 > 1$, we know that the rational solutions is only finitely many.

In the language of complex geometry, this result is know as that Riemann surfaces of genus 0 are positively curves, Riemann surfaces of genus 1 are flat, while if the genus is at least 2, it's negatively curved. In terms of automorphism groups, you will see that for genus at least 2 curves, the automorphism group is finite, for genus 1, it's dimension 1 and for genus 0 curves over algebraically closed field (which is $\mathbb{P}^1$), it's automorphism group is PGL_2 which is of dimension 3.

Now we go back to genus 2 curves: Fix a curve C of genus 2, then it's canonical bundle has degree $2g - 2 = 2$, and I claim that it's base point free. This is because it has $g = 2$ sections, and we know that for a curve of genus at least 1, any degree 2 line bundle on C with at least two sections only have these two sections, and is base point free and gives a hyperelliptic map.

Now we assume we work over an algebraically closed field $k = \overline{k}$. Then we have classified all double covers of $\mathbb{P}^1$ and given such a cover $\pi : C \to \mathbb{P}^1$, we know that it comes from a degree 2 line bundle on C with at least 2, thus only two sections. And since genus is 2, we know that this sheaf is the dualizing sheaf. Then consider the following map:

$$\{\text{genus 2 curves over } k = \overline{k}\} \to \{\text{genus 2 double curves of } \mathbb{P}^1\}/\mathrm{PGL}_2$$

where C is mapped to the morphism induced by ω_C. And our discussion shows that this is a bijection, as the inverse is given by $\pi : C \to \mathbb{P}^1$ is mapped to C. Checking that going from right to left and then to right is the identity is the hard part, I will let you do it, but the key here is to recall that on C, since it's genus is at least 2, double cover to $\mathbb{P}^1$ defined by the same line bundle only differs by an isomorphism on $\mathbb{P}^1$. These above discussion doesn't use the Riemann Hurwitz formula, bu if we assume further that the field is not of characteristic 2 as well, we can apply the Riemann-Hurwitz formula and conclude that each genus 2 curve branch over $\mathcal{P}^1$ at $2 \times 2 + 2 = 6$ points. And we have a informal discussion last section that there will be a $2g - 1 = 3$ dimensional space of genus 2 curves. This is not precise, but the following proposition is precise:

Proposition 6.2. Fix an algebraic closed field k of characteristic not 2, there are infinitely many pairwise nonisomorphic genus 2 curves over k.

Proof. We still need to assume characteristic not 2 in order to use Riemann Hurwitz formula. Recall that given any 6 points on $\mathbb{P}^1$, there is exactly one such genus 2 curve C, and we know that for any automorphism of $\mathbb{P}^1$, you will also obtain isomorphic C. Therefore, our task is to make precise the following statement: Even if we quotient out the automorphisms of $\mathbb{P}^1$, there are still infinitely choices of 6 distinct points on $\mathbb{P}^1$. This is easy actually, since we know that automorphism on $\mathbb{P}^1$ is strictly transitive. Then if we fix 5 points and let one vary, it has infinitely many choices and strict three transitive guarantees that there is no automorphism on $\mathbb{P}^1$ such that we can get one configuration from another.

This is enough, as we know that if two genus two curves are isomorphism over $\mathbb{P}^1$, modding out automorphisms of $\mathbb{P}^1$, we have the following diagram:

$$\begin{array}{ccc} C_1 & \xrightarrow[\simeq]{} & C_2 \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi_2} \\ \mathbb{P}^1 & \xrightarrow{\simeq} & \mathbb{P}^1 \end{array}$$

then the branch points of π_2 is taken to branch points of π_1 by an automorphism of $\mathbb{P}^1$. □

Proposition 6.3. any genus 2 curve over a field not of characteristic 2 has a finite automorphism group.

Proof. Let's first prove this over the algebraic closure of k, then recall that the following fibered product:

$$\begin{array}{ccccc} C_{\overline{k}} & \xrightarrow[\simeq]{} & C_{\overline{k}} & \longrightarrow & Spec\overline{k} \\ \downarrow & & \downarrow & & \downarrow \\ C & \xrightarrow[\simeq]{} & C & \longrightarrow & Speck \end{array}$$

it gives you a map from $\mathrm{Aut}(C) \to \mathrm{Aut}(C_{\overline{k}})$. I claim that this morphism is injective, this is because tensoring with K is faithfully flat.

Therefore we know that if $\mathrm{Aut}(C_{\overline{k}})$ is finite, then $\mathrm{Aut}(C)$ is finite.

Now assume k is algebraically closed, we need to prove the automorphism group is finite. Now suppose that α is an automorphism of C, then the following diagram is commutative:

$$\begin{array}{ccc} C & \xleftarrow[\alpha]{} & C \\ {\scriptstyle \pi}\downarrow & & {\scriptstyle \pi}\downarrow \\ \mathbb{P}^1 & \xleftarrow{\sigma} & \mathbb{P} \end{array}$$

where σ is the unique automorphism of $\mathbb{P}^1$ such that this diagram is commutative. This gives you a group homomoprhism:

$$\mathrm{Aut}(C) \hookrightarrow \mathrm{Aut}(\mathbb{P}^1)$$

Now, given such an α, say the branch locus is B, consisting of six points, we know by the above diagram that $\sigma(B) = B$, therefore, we have a homomorphism to permutation group of order 6:

$$\psi : \mathrm{Aut}(C) \to S_6$$

Then consider the following SES:

$$1 \to \ker\psi \to \mathrm{Aut}C \xrightarrow{\psi} \mathrm{Im}\psi \to 1$$

Let's compute the kernel. Suppose that α_1, α_2 is mapped to the same σ (we can assume this again because automorphisms of $\mathbb{P}^1$ are strictly 3-transitive.) Then we have the following diagram:

$$\begin{array}{ccc} C & \xleftarrow{\alpha_1} & C \\ & \xleftarrow{\alpha_2} & \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathbb{P}^1 & \xleftarrow{\sigma} & \mathbb{P} \end{array}$$

If you examine what happens, you find that the following commutes:

$$\begin{array}{ccc} C & \xleftarrow{\alpha_1 \circ \alpha_2^{-1}} & C \\ \downarrow{\scriptstyle \pi} & \swarrow{\scriptstyle \pi} & \\ \mathbb{P}^1 & & \end{array}$$

thus it's either the hyperelliptic involution or the identity, thus the kernel is of rank 2, thus we know that the number of elements in the automorphism is at most $2 \times 6!$, we are done. □

7 Curves of Genus 3

We will begin with a general discussion of curves of genus $g > 1$ and then specialize to $g = 3$.

Proposition 7.1. Assume $k = \overline{k}$ (which can be removed and you will see why in the proof), suppose that C is a curve of genus $g > 1$, then if C is not hyperelliptic, the dualizing sheaf gives a closed embedding $C \hookrightarrow \mathbb{P}^{g-1}$.

Proof. Recall that the line bundle $\mathcal{O}(p+q)$ if of degree 2, then we know that if $\mathcal{O}(p+q)$ has at least 2 linearly independent sections, C is hyperelliptic, thus by our assumption, it can only have 1 or 0 independent sections. Then recall that for a line bundle $\mathcal{L}$, if we can prove that:

$$h^0(C, \mathcal{L}) - h^0(C, \mathcal{L}(-p-q)) = 2$$

for any closed points p, q not necessarily distinct, then it induces a closed embedding. Thus we need to show the above quantity holds, or we can split it into two equations:

$$h^0(C, \mathcal{L}) - h^0(C, \mathcal{L}(-p)) = 1 \qquad h^0(C, \mathcal{L}(-p)) - h^0(C, \mathcal{L}(-p-q)) = 1$$

Now if $\mathcal{L}$ is the dualizing sheaf, we need to show that $h^0(C, \omega_C(-p-q)) = g - 2$. Or we need to show that $h^1(C, \omega_C(-p))$ and $h^1(C, \omega_C(-p-q)) = 0$. Using Serre duality, we know that this converts to show that $h^0(C, \mathcal{O}(p)) = 1$ and $h^0(C, \mathcal{O}(p+q)) = 1$. But this suffice to show only the second, since we know that a degree one line bundle on a curve not isomorphic to $\mathbb{P}^1$ at most have 1 dimensional sections, and if $h^0(C, \mathcal{O}(p+q)) = 1$, we know that $h^0(C, \mathcal{O}(p)) \neq 0$ and we are done. □

Remark 7.2. The corresponding statement on non algebraically closed field need the assumption of gr,gi and we can base change to do the above argument.

Definition 7.3. Such a curve embedded in $\mathbb{P}^{g-1}$ via the dualizing sheaf, also known as the canonical line bundle, is called a **canonical curve** and the closed embedding is called a **canonical embedding**.

Now we go back to our study of genus 3 curves. First, a genus 3 curve could be hyperelliptic, and suppose that we work with algebraically closed fields of characteristic not 2, we have a pretty good understanding of these hyperelliptic genus 3 curves already. Therefore, let's think about those non-hyperelliptic genus 3 curves. Now ω_C is a line bundle of degree 4, with 3 linearly independent sections, therefore, we know from the first proposition in this section that: if C is not hyperelliptic, then the canonical bundle expresses C as a closed embedding in $\mathbb{P}^2$, whose degree is 4. Now I prove that all this is a quartic curve in $\mathbb{P}^2$. To do this we will use a similar method that proved all genus 0 curves are conics in $\mathbb{P}^2$. Consider $\omega_C^{\otimes 4}$, it has degree $16 > 4$, therefore the dimension of global sections is $h^0(C, \omega_C^{\otimes 4}) = \deg - g + 1 = 16 - 3 + 1 = 14$. Now consider $\mathrm{Sym}^4 H^0(C, \omega_C)$, which has dimension 15, then the canonical map:

$$\mathrm{Sym}^4 H^0(C, \omega_C) \to H^0(C, \omega_C^{\otimes 4})$$

has a nontrivial kernel, therefore, we conclude that it's contained in a quartic, then to show they are the same, we only need to show that their Hilbert polynomial agrees for large m. Notice that the Hilbert polynomial is linear, since the support is both 1 dimensional, then we know that we only have to show the constant term agrees. Now, notice that the curve is regular and integral, thus you know that topologically C is an irreducible component of $V(f)$, and scheme theoretically, it's the unique reduced closed subscheme whose underlying topological space is that component. We know that topologically, if we write the irreducible component of f, C is one of them, but this will contradict with the degree of C, therefore C can only be $V(f)$, we are done.

Conversely, we know that any integral quartics in $\mathbb{P}^2$, as a closed embedding has degree 4, thus the line bundle that embeds it into $\mathbb{P}^2$ has degree 4, and it has genus 3, and I claim that this line bundle has 3 sections. To see why, this line bundle is actually the pullback of $\mathcal{O}(1)$, i.e. $i^*\mathcal{O}(1)$, now consider the following SES of the effective Cartier divisor (any quartic H is an effective Cartier divisor)

$$0 \to \mathcal{O}(-4) \to \mathcal{O} \to \mathcal{O}|_H \to 0$$

Now twist it by $\mathcal{O}(1)$, we get:

$$0 \to \mathcal{O}(-3) \to \mathcal{O}(1) \to i_*\mathcal{O}_H \otimes \mathcal{O}(1) \to 0$$

Using the projection formula, we know that the last term is:

$$i_*(\mathcal{O}_H \otimes i^*\mathcal{O}(1))$$

Then we take the associated LES using some vanishing and cohomology is invariant under pushforwards by closed embeddings, we are done. Therefore, this closed embedding is given by a degree 4 line bundle with exactly 3 sections. If we assume that we work with algebraically closed field, then this integral quartic has an invertible sheaf, which is the only degree 4 line bundle with 3 sections, thus this integral quartic is canonically embedded.

Remark 7.4. The above argument shows that any nonhyperelliptic curve, modding out automorphisms of $\mathbb{P}^2$, can be expressed as a regular integral quartic in $\mathbb{P}^2$ in essentially one 1 way.

And in particular, since there are regular integral quartics, there are nonhyperelliptic genus 3 curves.

Informally, just like what we did for hyperelliptic curves, we can try to get a space of nonhyperelliptic genus 3 curves. We already know that it's in correspondence with regular integral quartics in $\mathbb{P}^2$ quotient the automorphism groups of $\mathbb{P}^2$, i.e. PGL(3). The space of quartics in $\mathbb{P}^2$ is of dimension 15, but we need regular quartics, which is characterized by the Jacobian condition, which makes the dimension drops by 1, then we quotient out the automorphism group, which is of dimension 8, then in the end, we get a space that is of dimension $15 - 1 - 8 = 6$.

Now given the fact that the space of nonhypereeliptic genus 3 curves is of dimension 6, since we also know that the dimneison of hyperelliptic genus 3 curves is 5, we seem to get a simple classification of genus 3 curves. But there is actually more to it, as in some sense, hyperellptic curves is a limit of non-hyperelliptic curves, therefore the space of genus 3 curves can be viewed as a single space of dimension 6, but these discussion in details go far beyond what we want to say here.

There is another question of genus 3 curves that is interestingl i.e. are there any genus 3 curves with no nontrivial automorphism groups. We already know that that for hyperelliptic genus 2 curves since the hyperelliptic involutio is nontrivial, there is always a nontrivial automorphism. But we show below that there are certain nonhyperelliptic genus 3 curves such that there are no nontrivial curves. The first thing you need to notice is that automorphisms of C, as C can be embedded to $\mathbb{P}^2$ as a quartic, can be viewed as automorphisms of $\mathbb{P}^2$ that preserves C, this is because if α is an automorphism of C we think about the following diagram:

$$\begin{array}{ccc} C & \xleftarrow{\alpha} & C \\ {\scriptstyle i}\downarrow & & {\scriptstyle i}\downarrow \\ \mathbb{P}^2 & \xleftarrow{\simeq} & \mathbb{P}^2 \end{array}$$

where the automorphism down below, say denoted by σ, is the unique such that this diagram commutes. Moreover, notice that this diagram is Cartesian and you can directly check it by hand by verifying the universal property.

Conversely, if σ is given that preserves C, then if we think about C as $V(f)$ in $\mathbb{P}^2$, then we know that there is a diagram:

$$\begin{array}{ccc} V(f) & \xrightarrow{\simeq} & V(f) \\ \downarrow & & \downarrow \\ \mathbb{P}^2 & \xrightarrow{\simeq} & \mathbb{P}^2 \end{array}$$

induced by an isomorphism of the graded ring(here this automorphism between $V(f)$ exists because as the automorphism preserves $V(f)$, it preserves it as a set, then since we know that the image of $V(f)$ is the image of $\mathbb{P}^2 - D(f)$, which is $\mathbb{P}^2 - D(\varphi(f)) = V(\varphi(f)) = V(f)$ where φ is the isomorphism of graded rings. Recall that (f) is a prime ideal since $V(f)$ is C which is irreducible closed, therefore $V(f) = V(\varphi(f))$ implies that $(\varphi(f)) = (f)$, then since they are not zerodivisors, we know that $\varphi(f) = kf$ for some constants k, we are done.). Then this diagram gives a unique automorphism between C by $C \simeq V(f)$. I claim the above two constructions are inverses, and I will let you check why this is true.

Then by the above argument, we know that if we want to find such a genus 3 curve that only has trivial automorphism group, we need to find automorphisms of $\mathbb{P}^2$, which has the property that if it preserves C then it's the identity. Our guess is that there has to be some quadric that satisfies this property, but in order to find one of such regular integral quartic needs work and Poonen gives such an example in characteristic 0:

$$y^3z - 3yz^3 = 3x^4 - 4x^3z + z^4$$

I will not let you verify this, but the following statement is interesting:

Proposition 7.5. Suppose that C is an irreducible smooth projective curve with no nontrivial automorphisms, then no two distinct open subsets of C are isomorphic.

Proof. Suppose for the sake of contradiction that there are two of such nonempty opens that are isomorphic, say we have an isomorphism $f : U \simeq V$, then consider $f : U \to C$, we know that by repeated applying the Curve to Projective theorem (smooth implies regular), we get an extension $f : C \to C$. Then we consider the inverse $g : V \simeq U$, which extends to $g : C \to C$. Now if you compose $f \circ g$ and $g \circ f$, you find that they are identity on a dense open, i.e. the intersection $U \cap V$, then since we know that C is proper, thus separated, therefore we know that morphism that agrees on dense opens agrees everywhere, thus f, g are nontrivial automorphisms, a contradiction. □

There are also genus 3 curves that has nontrivial automorphisms, for example, hyperelliptic curves. And people have also found nonhyperelliptic such curves, for example, there is the so called Klein quartic:

$$x^3y + y^3z + z^3x = 0$$

in $\mathbb{P}^2_{\mathbb{C}}$, which has 168 automorphisms, which is the unique finite simple group of order 168 and later, if we assume that automorphism groups of genus at least 2 curves are finite, we can prove that no genus 3 curves can have more automorphisms.

8 Curves of Genus 4 and 5

Again, we consider nonhyperelliptic curves of genus 4, then we know that the dualizing sheaf is of degree 6 and has 4 sections, thus the canonical embedding $i : C \to \mathbb{P}^3$ describes i as a degree 6 curves in $\mathbb{P}^3$, and we shall see that all such curves are complete intersections of quadric surfaces and cubic surfaces and conversely all complete intersections of quadric surfaces and cubic surfaces will be genus 4 nonhyperelliptic curves, canonically embedded.

To begin with, notice that the pullback of $\mathcal{O}(1)$ is of degree 6 and since the pullback morphism is injective, we know that it has at least 4 sections, thus it's the canonical line bundle, then using Riemann-Roch and Serre duality:

$$h^0(C, i^*\mathcal{O}(2)) = h^0(C, \omega_C^{\otimes 2}) = 12 - 4 + 1 = 9$$

On the other hand, we know that $h^0(\mathbb{P}^3, \mathcal{O}(2)) = \binom{3+2}{2} = 10$, therefore we know that the pullback map:

$$H^0(\mathbb{P}^3, \mathcal{O}(2)) \to H^0(C, i^*\mathcal{O}(2))$$

has a nontrivial kernel, and say a quadric f is in that kernel, we know that the embedding is scheme-theoretically contained in $V(f)$. Recall that a quadric can only be either a double plane, or the union of two planes or a cone or a regular quadric. Since this embedding is not degenerate, we know that this quadric can not be a union of planes or a double plane, therefore we can assume that it's either a cone or a regular quadric, and in particular, we know that Q is irreducible.

It's not possible that C is contained in the intersection of two such quadrics since we know that if Q', Q are distinct such quadrics, then $Q' \cap Q$ is a curve since they are both irreducible, thus not containing the generic point of the other and they don't have embedded points, therefore we know that by Bezout's theorem, the closed embedding $Q' \cap Q$ has degree $4 = 2 \times 2$, then since the degree of C is $6 > 4$, it will not be contained in $Q \cap Q'$.

Next, we consider cubic surfaces, again, we know that $h^0(C, \omega_C^{\otimes 3}) = 18 - 4 + 1 = 15$ and $\mathrm{Sym} H^0(C, \omega_C)$ has dimension $\binom{3+3}{3} = 20$, therefore consider:

$$\begin{array}{ccc} \mathrm{Sym}^3 H^0(\mathbb{P}^3, \mathcal{O}(1)) & \xrightarrow{\simeq} & H^0(\mathbb{P}^3, \mathcal{O}(3)) \\ \downarrow & & \downarrow \\ \mathrm{Sym}^3 H^0(C, \omega_C) & \longrightarrow & H^0(C, \omega_C^{\otimes 3}) \end{array}$$

since the bottom has a kernel of at least dimension 5, the vertical map on the right has a kernel of at least dimension 5, thus we know that the canonical embedding is contained in cubic of dimension 5. Now, since this embedding is contained in Q, then we can multiply this by linear terms $ax + by + cz + dw$ and conclude that in these 5 dimensions, 4 of them comes from Q, and there is another cubic that is not divisible by Q, thus we take that cubic and denote it by K, we know that $K \cap Q$ is a complete intersection since Q and K shares no components and hypersurfaces have no embedding points, therefore, we know that the degree of $K \cap Q$ is just $2 \times 3 = 6$ and so is C and C is contained in $K \cap Q$. Moreover, we know that the genus of $K \cap Q$, as what we have computed before, is 4, therefore the degree and the genus completely determines the Hilbert polynomial since the polynomial is nothing but a linear one. Therefore C and $K \cap Q$ has the same Hilbert polynomial, therefore, they are the same.

We now show the converse, i.e. all irreducible regular complete intersections of C of a quadratic surface with a cubic surface is canonically embedded. Notice that it's of genus 4 since it's a complete intersection. Then we will show:

Proposition 8.1. $\mathcal{O}_C(1)$ has at least 4 sections, thus since it's of degree 6, it's the canonical curve.

Proof. We only need to show that the pullback map is injective, or equivalently, C is not degenerate. Suppose that for the sake of contradiction, we assume that it's contained in a hyperplane, then we know that Q and K, the quadric and cubic, can't be divisible by the hyperplane say H, otherwise, we know that this will not be a complete intersection. Let's assume that K is not divisible by H, then the intersection $H \cap K$ is complete, thus has degree 3. And we know that $k \cap H$ contains $K \cap (K \cap Q)$. But this is a contradiction,

since they both had dimension 1 and the degree $K \cap Q$ is 6 while something larger only has degree 3, a contradiction, this also holds if we assume that Q is not divisible by H. Therefore a contradiction always happens if we assume $K \cap Q$ is contained in a hyperplane, we are done. □

In particular, the above theorem shows that the line bundle $\mathcal{O}_C(1)$ is the unique line bundle that has degree 6 and 4 sections, thus the canonical line bundle.

Now we go to the discussion of genus 5 curves and then end the discussion by briefly looking at what happens for larger genus in general. We still try to understand nonhyperelliptic curves in terms of complete intersections. But unfortunately, things already start to get a little bit messy at genus 5:

Proposition 8.2. Let C be a nonhyperelliptic curve of genus 5, then the canonical embedding is of degree 8 and it's going to lie in the intersection of three quadric surfaces (not necessarily equal and this intersection is not necessarily complete) in $\mathbb{P}^4$. Conversely, any irreducible regular complete intersection of three quadrics will be canonically embedded as a degree 8 genus 5 curve.

Proof. Recall let's first consider the following map:

$$\mathrm{Sym}^2 H^0(C, \omega_C) \to H^0(C, \omega_C^{\otimes 2})$$

The stuff on the left has dimension is $5 + 4 + 3 + 2 + 1 = 15$ and the stuff on the right has dimension $\deg - g + 1 = 16 - 5 + 1 = 12$, therefore we know that the kernel is at least of dimension 3. Therefore this canonical embedding lies in at least a three dimensional space of quadrics and we pick three independent sections. Notice that we know that any of these quadrics can not be a union of two lines or double lines since the embedding is nondegenerate, therefore we can assume that Q_1, Q_2, Q_3 doesn't contain the component of each other. But we don't know whether the intersection is complete or not, since we don't know if Q_3 contains components of $Q_1 \cap Q_2$ or not.

But if there is an irreducible regular intersection of three quadrics, I claim that it's going to be be canonically embedded as a genus 5 curve. Again, we only need to show that the line bundle $\mathcal{O}_C(1)$ has 5 sections, or in other words, this complete intersection is not degenerate, we use a similar argument as above to show this, the genus is 5 can also be computed using an earlier result. □

Sadly, when $g \geqslant 6$, our luck of describing nonhyperelliptic curves using complete intersections has run out:

Proposition 8.3. Say $C \subset \mathbb{P}^{g-1}$ is a canonical curve, then it's not a complete intersection for $g \geqslant 6$. Notice that the degree of this embedding is $2(g-1)$ and if it's a complete intersection, since it's not contained in any hyperplane, those in the intersection should be quadrics or higher degree, but even if we assume that they are all quadrics, the degree is 2^{g-2}, when $g = 5$, this is the last g such that $2(g-1)$ and 2^{g-2} could be equal, and for $g \geqslant 6$, 2^{g-2} is always larger than $2(g-1)$, we are done.

These are basically all we can say for curves of higher degrees for now without the knowledge of stacks or moduli spaces. There are some particular cases where we can indeed say something, for example a **del Pezzo** surface, but we will discuss these stuff later after we know what is differentials and blow-ups. For now, let's just be satisfied with what we have done and move to the discussion of genus 1 curves, on which we spend the rest of the notes:

9 Curves of Genus 1

The plan is we will present the theory by discussing line bundles of gradually increasing degree. Recall that degree d line bundles on C are denoted by $\mathrm{Pic}^d C$.

Suppose that C is of genus 1 and $\mathcal{L}$ is a line bundle of degree 0, which is of degree $2 \times 1 - 2$, then we know that the canonical bundle is of degree 0 and it has 1 sections, thus $\omega_C \simeq \mathcal{O}_C$. This is not saying that there are not degree 0 line bundle without nontrivial global sections, this is just saying that one important property of genus 1 curves is that the structure sheaf is the dualizing sheaf.

Now we move to line bundles of higher degree. Notice that if $\deg \mathcal{L} > 0$, then we can compute the global sections using degree, then we know that:

$$h^0(C, \mathcal{L}) = \deg \mathcal{L}$$

9.1 Line Bundles of Degree 1

Recall that a degree 1 point p defines a degree 1 line bundle by taking the associated line bundle of this effective Cartier divisor $\mathcal{O}(p)$, and we know that for different p, q, $\mathcal{O}(p)$ is not isomorphism to $\mathcal{O}(q)$. This is because that if they are isomorphic, then the section that vanishes at p also vanishes at q as $\mathcal{L}$ only has one independent section of any degree 1 line bundle. Then conversely, given such a line bundle $\mathcal{L}$, we can compute the degree using any global section, that we know that the only independent section vanishes at a degree 1 point at order 1, and we already know that in this case, $\mathcal{O}(p) \simeq \mathcal{L}$.

Therefore we know that we have a canonical bijection between degree 1 line bundles (mod the isomorphism, thus actually the bijection is from $\mathrm{Pic}^1 C$) and degree 1 closed points.

Definition 9.1. An elliptic curve is a genus 1 curve E with a choice of k-valued point p. This choice of point p is also part of the definition of an elliptic curve and elliptic curve is not just a synonym for genus 1 curves.

An elliptic curve is always denoted by E instead of C.

Remark 9.2. If we don't work with algebraically closed field, there could be no k-valued points at all for a genus 1 curve. For example, consider the curve:

$$y^2 = -x^4 - 1$$

in $\mathbb{A}^2_{\mathbb{Q}}$. It's obvious that it doesn't even have any $\mathbb{R}$-valued point, therefore not $\mathbb{Q}$-valued point. It's genus 1 since it's part of a hyperelliptic genus 1 curve over $\mathbb{P}^1_{\mathbb{Q}}$ that branches over 4 points. Therefore, this is another warning that elliptic curves are not just a genus 1 curve.

If (E, p) is an elliptic curve, there is a canonical bijection between the set of degree 0 invertible sheaves (up to isomorphism, thus still from $\mathrm{Pic}^0 E$) to the set of degree 1 points of E:

$$\mathcal{L} \to \mathrm{div}(\mathcal{L}(p)) \qquad q \mapsto \mathcal{O}(p - q)$$

Recall that degree 0 line bundles form a group under tensor product, so we have proved the following result:

Proposition 9.3. The above bijection determines a abelian group structure on the set of degree 1 points on E, with the identity p.

So from now on, we will identity closed points of E with degree 0 line bundles without comment. For the time being, this bijection is just a bijection of groups, but we know that E has much richer structure, i.e. E itself is a variety, thus we should be motivated to think that there is some scheme structure on $\mathrm{Pic}^0 E$ and this is indeed true after we develop enough backgrounds and this bijection of sets can be upgraded to an isomorphism of schemes.

9.2 Line Bundles of Degree 2

Notice that $\mathcal{O}(2p)$ has two sections for degree 1 point p, therefore since the genus is 1, we have proved that it admits a double cover of $\mathbb{P}^1$ and we know that one of the ramification point will be p as there is a section of $\mathcal{O}(2p)$ that vanishes only at p with order 2, and say that via the pullback map, some linear form is pulled back to that section, then the vanishing locus of that linear form is going to be a brach point. If we assume further that $k = \overline{k}$ and $\mathrm{char} k \neq 2$, we can apply the Riemann-HUrwitz formula and conclude that E has four ramification points p and three others. Conversely, given any 4 distinct points of $\mathbb{P}^1$, there is a unique double cover with genus 1.

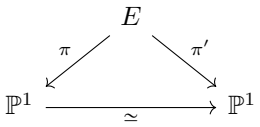
Therefore, given an elliptic curve (E, p), you can obtain an hyperelliptic map with one ramification point being p and given a hyperelliptic map and a choice of one of the four branch points, we obtain an elliptic curve. Up to automorphisms of $\mathbb{P}^1$, we know that elliptic curves (E, p) correspond to the choice of 4 points in $\mathbb{P}^1$, one marked by P, mod automorphism of $\mathbb{P}^1$ (can you figure out why we need to quotient automorphisms?).

Proposition 9.4. The other three ramification points correspond to the 2-torsion points on E, i.e. those q such that $\mathcal{O}(q)$ is not isomorphic to $\mathcal{O}(p)$, but $\mathcal{O}(2p) \simeq \mathcal{O}(2p)$.

Proof. Suppose that q is another ramification point, thus $p \neq q$, then we know that $\mathcal{O}(p)$ is not isomorphic to $\mathcal{O}(q)$. Now we consider the pullback of $\mathcal{O}(1)$ via the double cover, and I claim this pullback is isomorphic to $\mathcal{O}(2p)$ and $\mathcal{O}(2q)$, thus concluding that $\mathcal{O}(2p) \simeq \mathcal{O}(2q)$.

To see this, notice that we pullback is isomorphic to the line bundle that is determined by the divisor computed using any global section(since everything is regular here, thus normal), then we know that there are sections of the pullback that vanishes at $2p$ and $2q$, therefore, we are done.

Also, if we assume that q is a 2-torsion point, i.e. $\mathcal{O}(2p) \simeq \mathcal{O}(2q)$, then we know that the double covers $\pi, \pi' : E \to \mathbb{P}^1$ defined using $\mathcal{O}(2p)$ and $\mathcal{O}(2q)$ differs by an automorphism of $\mathbb{P}^1$, and q is going to be a ramification point of π', then using the following diagram:



we know that q is also a ramification point of π. □

Therefore, (again assume $k = \overline{k}$ and char$k \neq 2$), every elliptic curve has exactly four 2-torsion points, one being the identity and three others. All ramification points of the double cover to $\mathbb{P}^1$.

Remark 9.5. An elliptic curve with full level n-structure is an elliptic curve with an isomorphism of it's n-torsion points with $(\mathbb{Z}/n)^2$. In particular, we know that a an elliptic curve with full level 2-structure has 2-torsion points isomorphic to $(\mathbb{Z}/2)^2$. The algebraic structure of $(\mathbb{Z}/2)^2$ and the fact that there are always 4 distinct 2-torsion points implies that once we give an order to these four points, it's naturally isomorphic to $(\mathbb{Z}/2)^2$.

Now we insist the assumption that k is algebraically closed and not of characteristic 2. Say (E, p) is an elliptic curve and we consider the double cover $E \to \mathbb{P}^1$ given by $\mathcal{O}(2p)$. Let's label the other three branch points by Q_1, Q_2, Q_3, and we know that there is a unique automorphism of $\mathbb{P}^1$ that takes P, Q_1, Q_2 to $\infty, 0, 1$ respectively, then say Q_3 is taken to some number λ where we know necessarily $\lambda \neq 0, 1, \infty$.

This value λ is called the **cross-ratio** of the four points (P, Q_1, Q_2, Q_3) in $\mathbb{P}^1$. This number λ is useful since we have the following result:

Proposition 9.6. Isomorphism classes of of four ordered distinct closed point on $\mathbb{P}^1$ over an algebraically closed field, up to automorphisms of $\mathbb{P}^1$ is classified by cross-ratio.

Proof. Let's first be specific about what is an isomorphism class of four ordered distinct four points up to automorphisms of $\mathbb{P}^1$. Two sets of four ordered distinct points on $\mathbb{P}^1$, (P_1, P_2, P_3, P_4) and (Q_1, Q_2, Q_3, Q_4) are isomorphic if there is an automorphism of $\mathbb{P}^1$ such that under this automorphism P_i is mapped to Q_i. Then we know that if they are isomorphic, then they have the same cross-ratio.

Conversely, suppose that they have the same cross-ratio, we know that this implies that the last point in the two sets is mapped to the same point in $\mathbb{P}^1$ if we insist the first three are mapped to $\infty, 0, 1$, then we can use this to give an automorphism such that the image of this first set is the second. □

Proposition 9.7. The cross-ratio of (a, b, c, d) is the same as that of (b, a, d, c) and further more, if we consider the action of S_4 acting on the cross ratio, then when we restrict to $V_4 \subset S_4$, the Klein 4 group, it's trivial.

Proof. To prove this, we view the cross-ratio in a different way. Say $P \in \mathrm{PGL}_2(k)$ is:

$$P = \begin{bmatrix} x & y \\ z & w \end{bmatrix}$$

Then we know that if the homogeneous coordinate of a point is $[a : b]$, then it's taken to $[xa + yb : za + wb]$. Then since we are only interested in the ratio:

$$\frac{xa + yb}{za + wb}$$

in the end, let's use the coordinate $t = \frac{a}{b}$ where $t \in k \cup \{\infty\}$, and we can write this as a Mobius transformation:

$$t \mapsto \frac{xt + b}{zt + w}$$

when $t = \infty$, we define it to be $\frac{x}{z}$, and when the numerator is 0, we define it to be ∞. Then I will let you check that this is consistent with any possibilities and we can now assume that a, b, c, d are numbers in $k \cup \{\infty\}$. (You should also be aware that since P is invertible therefore z, w are not 0 simultaneously and since we know that $zt + w$ could be 0, then z is not 0.) The condition we are imposing says that $\frac{xa+y}{za+w} = \infty$, $\frac{xb+y}{zb+w} = 0$ and $\frac{xc+y}{zc+w} = 1$, and we are interested in what is $\frac{xd+y}{zd+w}$. Notice that $za + w = 0$ $xb + y = 0$ implies that this Mobius transformation can be written as:

$$t \mapsto \frac{x(t - b)}{z(t - a)}$$

then when $t = c$, it's mapped to 1 implies that $\frac{x}{z} = \frac{c-a}{c-b}$, therefore we know that d is mapped to:

$$\frac{c - a}{c - b}\frac{d - b}{d - a}$$

When $d = \infty$, we see the result is $\frac{c-a}{c-b}$, which is consistent.

Then with this description, we see that there are certain permutations of a, b, c, d that doesn't change the cross-ratio, i.e. those in S_4 that are two distinct two cycles. We are done. □

Remark 9.8. Notice that if we fix our elliptic curve (E, p) and the double cover $E \to \mathbb{P}^1$. If we now map P, Q_2, Q_1 to $(\infty, 0, 1)$, then you can check that Q_3 is mapped to $1 - \lambda$, this is because, we are in this case, considering the cross-ratio of (P, Q_2, Q_1, Q_3), thus by the formula we just established, it's:

$$\frac{P - Q_1}{Q_2 - Q_1} \cdot \frac{Q_2 - Q_3}{P - Q_3}$$

And the cross-ratio of (P, Q_1, Q_2, Q_3) is:

$$\frac{P - Q_2}{Q_1 - Q_2} \cdot \frac{Q_1 - Q_3}{P - Q_3}$$

You can check that the sum is:

$$\frac{-(P - Q_3 + Q_3 - Q_1)(Q_2 - Q_3) + (P - Q_3 + Q_3 - Q_2)(Q_1 - Q_3)}{(Q_1 - Q_2)(P - Q_3)} = 1$$

And you can also try to map (P, Q_1, Q_3), (P, Q_3, Q_1), (P, Q_2, Q_3) and (P, Q_3, Q_2) to $(\infty, 0, 1)$, you will get the cross-rations $\frac{1}{\lambda}$, $1 - \frac{1}{\lambda}$, $\frac{1}{(1-\lambda)}$ and $\frac{\lambda}{\lambda-1}$. But these are all the same elliptic curve, it's just we are choosing different orders of Q_1, Q_2, Q_3, therefore, there will be $|S_3| = 6$ possible cross-ratios, all related to each other.

This result is already very satisfactory since if you want to check if two elliptic curves are isomorphic or not, you can consider their double cover to $\mathbb{P}^1$, and if since we know that to determine if they are isomorphic or not, automorphisms of $\mathbb{P}^1$ doesn't matter, therefore, we know that we only have to think about if it's possible to bring the branch points of (E, p) to branch points of (E', p'), and we know that they can be checked using cross-ratio, and since there is the question of how to choose the order, we know that you only need to check all the six possible cross-ratios.

Well, we can actually be more greedy and ask instead of 6 cross-ratios, can we actually find a single valued criterion to determine whether two elliptic curves are isomorphic or not. This is possible and it will be called the j-invariant, or we want to have such a j that $j(\lambda) = j(\lambda')$ iff:

$$\lambda' = \lambda, \frac{1}{\lambda}, 1 - \lambda, \cdots$$

i.e. iff two elliptic curves are isomorphic. You can try to figure out what is this function and there are indeed some work you need to do if you are the first one who tries to do this and there are some philosophy that can help you find this j, but it's not super important, and we just hand you such a function:

$$j = \frac{2^8(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}$$

9.3 Line Bundles of Degree 3

Consider the degree 3 invertible sheaf $\mathcal{O}(3p)$, by Riemann-Roch, we know that it has three sections and it thus gives a morphism to $\mathbb{P}^2_k$, also, since this is a line bundle that has degree larger than 2, thus it's very ample and every morphism it gives using all the linearly independent sections will be a closed embedding. Therefore, we have described C as a degree 3 curves in $\mathbb{P}^2$, then we can use similar method to prove that it's contained in a cubic curve and since the genus of this cubic curve is $(3-2)(3-1)/2 = 1$, and degree is 3, therefore we know that this degree 3 embedding is a cubic curve. Now, recall that the pullback map is injective since this closed embedding is not degenerate, therefore for dimension reasons, it's an isomorphism. Then since we know that the inverse image of the place where a section of $\mathcal{O}(1)$ vanishes will be the locus where the pullback vanishes, we take the section that is pullback to the section where it vanishes at p of order 3, say it's a linear homogeneous polynomial f, then consider the line $V(f)$, we know that $V(f)$ only meet E at p, therefore we know from Bezout's theorem that the scheme theoretic intersection is of degree $3 = 3 \times 1$.

Remark 9.9. This remark is not essential.

Recall that when we discuss the smooth variety in $\mathbb{A}^n$ cut out by f, we defined the tangent line of $V(f)$ at a k-valued point(where $V(f)$ is not contained in the tangent line), from the point of view of what we know right now we can think of this as the intersection of $V(f)$ and a hyperplane in the projective space and the we restrict to the standard affine open $D_+(x_i)$. Then we know that this intersection is at least of degree 2. We now extend this definition, and say that as long as the intersection of a smooth curve with a line is of degree at least 2 at a point, the line is called a tangent line, and if the intersection is one point and the degree is at least of degree 3, the line is said to be a **flex** line.

Now, we can choose an automorphism of $\mathbb{P}^2$ such that p is now $[0:1:0]$, and we know that the line $V(f)$ should vanish at $[0:1:0]$, therefore, it has no y term, and we know that we can further choose this automorphism such that $[0:1:0]$ is preserved by the line is not $z = 0$. Then we consider what is the cubic of (E, p) in $\mathbb{P}^2$. First, we know that when $x = z = 0$, the cubic vanishes at $y = 1$, therefore we know that this cubic has no y^3 term. Furthermore, I claim that it has no $x - y$ cross term since we know that $z = 0$ only intersect this cubic at one point $[0:1:0]$ and if there is any cross term, since the field is algebraically closed, there will be another intersection point. Then, we also know that the coefficient of x^3 is not 0, otherwise it's contained in $V(z)$. Now I claim that the coefficient of y^2z is not 0 since otherwise, the curve is singular at $x = z = 0$, then by scale z, we know that we can assume that the coefficient of y^2z is -1. Now if the characteristic is not 2, by further apply an automorphism of $\mathbb{P}^2$, we can replace y by $y+?x+?z$ and so that the coefficient of xyz, yz^2 are 0. If the characteristic is not 3, we can apply another automorphism that maps x to $x+?z$ and fixes y, z, so that x^z has coefficient 0, therefore in the end, we can represent this elliptic curve by:

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

with the flex line $z = 0$. This is called the **Weierstrass normal form** of the elliptic curve.

Remark 9.10. We can recover the hyperelliptic form from the Weierstrass normal form by the following procedure.

Recall that there is a rational map $\mathbb{P}^2 \dashrightarrow \mathbb{P}^1$ defined from $D_+(x) \cup D_+(z) \to \mathbb{P}^1$. You should think of this map as defined by map of graded rings:

$$k[x, z] \to k[x, y, z] \qquad x \mapsto x, z \mapsto z$$

We know that this ring morphism gives you a morphism:

$$\mathbb{P}^1 - V(x, z) = D_+(x) \cup D_+(z) \to \mathbb{P}^1$$

You can also try to think of it using sections of line bundles, i.e. we know that x, z on $\mathbb{P}^2$ gives a rational map from $D_+(x) \cap D_+(z)$ to $\mathbb{P}^1$.

Then via the closed embedding $E \hookrightarrow \mathbb{P}^2$, notice that the the locus where E lie in $V(x) \cup V(z)$ is the closed point $[0:1:0]$, therefore, we get a morphism:

$$E - \{p\} \to \mathbb{P}^1$$

then recall that $\mathbb{P}^1$ is projective with no embedded point, therefore the curve to projective theorem tells you that this extends to a honest morphism $E \to \mathbb{P}^1$. I claim that this is the hyperelliptic cover, i.e. it's induced by the line bundle $\mathcal{O}(2p)$. To see why, notice that in the composition:

$$E - \{p\} \to D_+(x) \cup D_+(y)$$

is just the restriction of the map $E \hookrightarrow \mathbb{P}^2$ to $D_+(x) \cup D_+(z)$, then we compose with the morphism to $\mathbb{P}^1$, you can think of this as still defined by $\mathcal{O}(3p)$, but only the two sections, i.e. the pullback of x, z on $\mathcal{O}(3p)$. The reason why this doesn't give a morphism from E to $\mathbb{P}^1$ is because the pullback of z vanishes at p with order 3 and the pullback of x vanishes at p with order 1. We already know that pullback of z vanishes at p with order 3, the reason the pullback vanishes at p with order 1 is becasue the we know that $V(x)$ intersect with E for at least 3 closed point, then we know that if we compute the degree of the morphism using the pullback of x, we need to compute for at least 3 points, thus each of those 3 points contribute at most 1 vanishing order.

Knowing this, recall that we can view the global sections of $\mathcal{O}(3p - p)$ as a space of $\mathcal{O}(3p)$,consisting of those that vanish at p, thus the pullback of x, z are in the global sections of $\mathcal{O}(2p)$, and this time, x, thought as a section in $\mathcal{O}(2p)$ doesn't vanish at p, otherwise it's vanishing order is 2, thus $\mathcal{O}(2p)$ gives you a honest morphism to $\mathbb{P}^1$ and we know that away from p, $\mathcal{O}(2p) \simeq \mathcal{O}(3p)$, thus we know that the morphism defined agrees on $E - \{p\}$, we are done, thus the hyperelliptic map is the extension of $E - \{p\} \to \mathbb{P}^1$ we obtained before.

To see more explicitly how this works, say the Weierstrass normal form is:

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

I claim one of the two affine description of the hyperelliptic double cover is obtain by setting $z = 1$, i.e. the hyperelliptic map restricted to two affines can be viewed as:

$$Speck[x, y]/(y^2 = x^3 + ax + b)$$

The reason is very simple: we already saw that the morphism $\mathbb{E} \to \mathbb{P}^1$ defined by $\mathcal{O}(2p)$ restricted to $D_+(z)$, if the same as the morphism $E - \{p\} \to \mathbb{P}^1$ defined by x, z restricted to $D_+(z)$.

But we will not be able to obtain the other affine description by a similar method since we know that the hyperelliptic map $E \to \mathbb{P}^1$ only agrees with the morphism $E - \{p\} \to \mathcal{P}^1$ on a set not including p. This doesn't matter since we know that for hyperelliptic maps, we only have to know it on one such affine, as the gluing is going to be either the involution or the trivial gluing.

The reason we are explaining this here is that, this tells you that the j-invariant can be expressed by a, b in the Weierstrass normal form by the above discussion, I will not let you do it and it's listed below:

$$j(a, b) = \frac{2^8 3^3 a^3}{4a^3 + 27b^2}$$

The following exercise is interesting:

Proposition 9.11. The three torsion points on E are precisely those flex points on E.

Proof. Let q be a three torsion point, by definition, this implies that $\mathcal{O}(3q - 3p)$ is trivial. I want to claim that this q is a flex point, or in other words, we need to find a line $V(f)$ in $\mathbb{P}^2$ such that $V(f) \cap E$ is only q. To see why, notice that $\mathcal{O}(3q)$ also induced a closed embedding of degree 3 into $\mathbb{P}^2$, then we know that there will be something in the global section of $\mathcal{O}(1)$ such that the pullback only vanishes at p, for degree 3, we are done.

Conversely, say q is a flex point, under the closed embedding to $\mathbb{P}^2$ induced by $\mathcal{O}(3p)$, and the line that only meets E at q for degree 3 is $V(f)$, then we know that there will be a global section of $\mathcal{O}(3p)$ whose associated divisor is $3q$, then we know by the correspondence between line bundles and divisors that $\mathcal{O}(3q) \simeq \mathcal{O}(3p)$. □

9.4 Group Law: Geometrically

Recall that we described all the closed points on E as a group abstractly using line bundles. Now using the Weierstrass form, we can do this in a geometric way(actually we don't really need this Weierstrass coordinate, as you will see in the discussion below).

Recall that in the Weierstrass coordinate, the identity in the group law, p, is the only closed point that meets the line $V(z)$. Then now if we assume that another line $V(f)$ meets E at three points p_1, p_2, p_3, since the total degree is 3, the vanishing degree at each point p_i is 1. Then we can say by the correspondence between divisors and line bundles:

$$\mathcal{O}(p_1 + p_2 + p_3) \simeq \mathcal{O}(3p)$$

Notice that this translate to $p_1 + p_2 + p_3 = 0$ in the group. Then say q a point on E that is different from p, then we can consider the line $\overline{pq}$, now what we know is that there are two possibilities: The first is the intersection only has two points, then we know that $\mathcal{O}(2p + q)$ or $\mathcal{O}(p + 2q)$ is $\mathcal{O}(3p)$, i.e. we know that either $q = 0$ or $2q = 0$, but the first case is not possible, since we assumed that q is not p, the second case implies that the inverse of q is itself. Another possibility is that the intersection has p, q, r three points, then r is going to be the inverse of q.

If we want to know what is $q + s$ for $q \neq s$, we only need to look at the line $\overline{qs}$, if we want to know what is $2q = r$. We can use the tangent line at q, then if the line intersects only at q with degree 3, then q is a three torsion point, if not since we know that the intersection degree at q with the tangent line is at least 2 (this is because that if we want to show that f vanishes to order 2 at a k-valued point $(k_1, \cdots, k_n)$, we first can assume that $(k_1, \cdots, k_n) = 0$ by a linear change of coordinates(it doesn't affect the derivative), then we know that we need to first verify $f(0, \cdots, 0) = 0$, then we want to prove that it doesn't have any linear terms, but is equivalent to the second partial derivative vanishes, we are done.)

What is worth-noting is that we can tell anyone this rule of inverses and additions and and they can understand this pretty easily if there are familiar with projective space. But then you will have to prove that this is indeed a group law, which is had to verity without the help of line bundles.

9.5 Line Bundles with Higher Degree

We can keep increasing the degree of the line bundle we can study E using $\mathcal{O}(4p)$, which is a line bundle of degree 4, and we want to study the closed embedding it gives to $\mathbb{P}^3$:

Proposition 9.12. The above closed embedding is the complete intersection of two quadrics in $\mathbb{P}^3$.

Proof. The argument is very similar to what we saw before, you first show that it's a dimension at least 2 vector space of quadrics and use the fact that this embedding is not degenerate to conclude that the two quadrics we choose are irreducible, then use Bezout's theorem to conclude that the degree is 4 and the genus is 1, then they have the same Hilbert polynomial, we are done. □

The story doesn't end here, for example, we can try to study the closed embedding given by $\mathcal{O}(5p)$, but as the degree gets higher, the situation gets quite complicated. We will choose to omit the related discussions and move on to something that is not useful and interesting.

10 Elliptic Curves are Abelian Varieties

The main goal of this section is to show that elliptic curves are group varieties. Before we head to the real content, we first discuss a little bit on group varieties and abelian varieties.

We first discuss group objects in a category $\mathcal{C}$: Say that $\mathcal{C}$ is any category with a final object Z and with products. Then a **group object** in $\mathcal{C}$ is an object X along with three morphisms:

1. Multiplication: $m : X \times X \to X$.
2. Inverse: $i : X \to X$.
3. Identity element: $e : Z \to X$, not the identity map!

These morphism are required to satisfy the following properties:

1. Associativity axiom: The following diagram commutes:

$$\begin{array}{ccc} X \times X \times X & \xrightarrow{m \times id} & X \times X \\ {\scriptstyle id \times m}\downarrow & & \downarrow{\scriptstyle m} \\ X \times X & \xrightarrow[m]{} & X \end{array}$$

   This correspond to the fact that multiplication in a group is associative.

2. Identity axiom:

$$X \simeq Z \times X \overset{e \times id}{\to} X \times X \overset{m}{\to} X$$

   is equal to:

$$X \simeq X \times Z \overset{id \times e}{\to} X \times X \overset{m}{\to} X$$

   and they are both equal to the identity object. This correspond to the fact that multiply by the identity element on the left or right is the identity.

3. Inverse axiom:

$$X \times X \overset{i \times id}{\to} X \times X \overset{m}{\to} X$$

   and

$$X \times X \overset{id \times i}{\to} X \times X \overset{m}{\to} X$$

   are both $X \to Z \overset{e}{\to} X$. This is the fact that in a group the element times it's inverse on the left or right are both the identity element.

Using this definition, you can easily see that group objects in the Category of Sets is the same as the usual groups.

Definition 10.1. A group scheme is a group object in the category of schemes, a group scheme over a ring A or a scheme S is a group object in A-schemes or S-schemes.

Now let's look at a few example to get you familiar with this notion:

Proposition 10.2. $\mathbb{A}^1_{\mathbb{Z}}$ is a group scheme.

Proof. To show it's a group scheme, we need to first determine what are the three morphisms.
For the identity morphism, we define it to be:

$$Spec\mathbb{Z} \to \mathbb{A}^1_{\mathbb{Z}}$$

induced by $\mathbb{Z}[x] \to \mathbb{Z}$ where $x \mapsto 0$. For the multiplication, we define it to be:

$$\mathbb{Z}[x] \to \mathbb{Z}[x] \otimes_{\mathbb{Z}} \mathbb{Z}[y] = \mathbb{Z}[x, y]$$

where $x \mapsto x + y$. You can also view this as map $x \mapsto x \otimes 1 + 1 \otimes x$. Finally the inverse is given by $x \mapsto -x$.
Then I will let you check the corresponding axioms. □

Proposition 10.3. If G is a group object in a category $\mathcal{C}$, then for any $X \in \mathcal{C}$, the object $\mathrm{Mor}(X, G)$ has a natural structure as a group and this group structure is preserved by pullback.

Proof. We define the multiplication map by f, g is mapped to fg where $fg(x) = f(x) \cdot g(x)$, or you could view it as defined by the following diagram:

$$X \xrightarrow{\Delta} X \times X \xrightarrow{f \times g} G \times G \xrightarrow{m} G$$

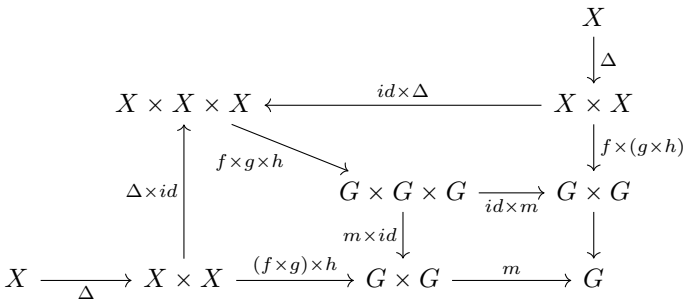
Notice that the composition of Δ with f, g can be viewed as the morphism induced by $f : X \to G$ and $g : X \to G$. The inverse is defined by:

$$X \xrightarrow{f} G \xrightarrow{i} G$$

and the identity morphism in $\mathrm{Mor}(X, G)$ is:

$$X \longrightarrow Z \xrightarrow{f} G$$

To prove this satisfies the axioms, for example, to verify the associativity axiom, I will let you figure out how to use the following diagram



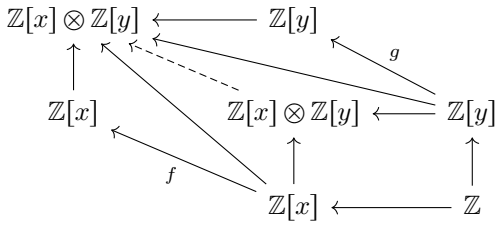
□

Proposition 10.4. The group structure on $X = \mathbb{A}^1_{\mathbb{Z}}$ and the previous proposition gives a group structure on $\Gamma(X, \mathcal{O}_X) = \mathbb{Z}[x]$ that is the same as the addition structure on $\mathbb{Z}[x]$.

Proof. Recall that $\mathrm{Mor}(X, X) = \Gamma(X, \mathcal{O}_X)$. Then via the previous proposition, we know that if $f, g \in \Gamma(X, \mathcal{O}_X)$ we want to compute the product, then what you do is looking at the following composition:

$$\mathbb{Z}[x] \to \mathbb{Z}[x] \otimes \mathbb{Z}[y] \xrightarrow{f,g} \mathbb{Z}[x] \otimes \mathbb{Z}[y] \to \mathbb{Z}[x]$$

Then $x \mapsto (x \otimes 1 + 1 \otimes y) \mapsto (f \otimes 1 + 1 \otimes g) \to f + g$ where the morphism in the middle is defined by:

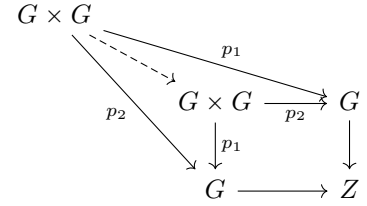


□

Remark 10.5. Similarly, we can try to define **abelian group objects** in any category or **ring objects** in any category, these are all defined using a similar idea as the definition of group objects, where you just need to generalize the usual set definition to category.

For example, if you want a definition of abelian group structure, first it's a group object, but the multiplication morphism need to satisfy one more axiom, i.e. the commutativity axiom:

$$G \times G \underset{p_2 \times p_1}{\overset{p_1 \times p_2}{\rightrightarrows}} G \times G \xrightarrow{m} G$$



where I require the first morphism factor via the coequaliser diagram (or in other words, $m \circ (p_1 \times p_2) = m \circ (p_2 \times p_1)$) and $p_2 \times p_1$ is defined in the diagram next to it.

There is a more functorial way to understand group schemes:

Proposition 10.6. Suppose that we have a contravariant functor F from the category of schemes to the category of groups, suppose further that after we compose the forgetful functor, this functor is representable and represented by an object Y, then the group operations on $F(X)$ as X varies through Sch uniquely determines group structure on Y such that induced group structure on $\mathrm{Mor}(X,Y)$ is the same as $F(X)$.

Proof. Since that F is represented by Y, we know that there is a functorial isomorphism:

$$\mathrm{Mor}(X,Y) \simeq F(X)$$

functorial in X. Let's assume that the multiplication map on $F(X)$ is(after transferring it to $\mathrm{Mor}(X,Y)$, notice that the new group law on $\mathrm{Mor}(X,Y)$ may not be the usual one):

$$m : \mathrm{Mor}(X,Y) \times \mathrm{Mor}(X,Y) \to \mathrm{Mor}(X,Y)$$

This will be functorial in X since F is a contravariant functor to the category of groups, thus $F(f) : F(X) \to F(Z)$ for a morphism $f : Z \to X$ will be morphism of groups, thus the following diagram is commutative:

$$\begin{array}{ccc} F(X) \times F(X) & \longrightarrow & F(X) \\ \downarrow & & \downarrow \\ F(Z) \times F(Z) & \longrightarrow & F(Z) \end{array}$$

and you can then translate it to a daigram of $\mathrm{Mor}(X,Y), \mathrm{Mor}(Z,Y)$.

Notice that there is a natural bijection:

$$\mathrm{Mor}(X,Y) \times \mathrm{Mor}(X,Y) \simeq \mathrm{Mor}(X, Y \times Y)$$

functorial in X, then we can consider the map:

$$\mathrm{Mor}(X, Y \times Y) \to \mathrm{Mor}(X,Y)$$

As it's a composition of maps functorial in X, it's also functorial in X, thus by Yoneda's lemma, this is induced by a morphism $Y \times Y \to Y$, this will be the candidate for the multiplication map and I claim that it is. Well too see this, you need to prove that a certain diagram of Y is commutative and what is available for us is a similar diagram, but for $\mathrm{Mor}(X,Y)$ is commutative, for all X:

$$\begin{array}{ccc} \mathrm{Mor}(X,Y) \times \mathrm{Mor}(X,Y) \times \mathrm{Mor}(X,Y) & \xrightarrow[m \times id]{} & \mathrm{Mor}(X,Y) \times \mathrm{Mor}(X,Y) \\ \downarrow{\scriptstyle id \times m} & & \downarrow{\scriptstyle m} \\ \mathrm{Mor}(X,Y) \times \mathrm{Mor}(X,Y) & \xrightarrow{\quad m \quad} & \mathrm{Mor}(X,Y) \end{array}$$

but I will let you figure out why we can convert that diagram to the commutativity of following diagram:

$$\begin{array}{ccc} \mathrm{Mor}(X, Y \times Y \times Y) & \xrightarrow{\circ(m \times id)} & \mathrm{Mor}(X, Y \times Y) \\ \downarrow{\scriptstyle \circ(id \times m)} & & \downarrow \\ \mathrm{Mor}(X, Y \times Y) & \longrightarrow & \mathrm{Mor}(X,Y) \end{array}$$

but this diagram commutes for all X implies that the original diagram commutes. You will use the similar method to obtain the inverse and identity and check the corresponding diagram is commutative.

Therefore, you obtained a group structure on Y, which is forced upon you by the group structure of $F(X)$ for each X. We still need to check that the group structure on $\mathrm{Mor}(X,Y)$ induced by the group structure on Y is the structure on $F(X)$, but this is just a tautology and I will let you check is if you like to. □

Remark 10.7. Combine what we have developed in the above two propositions, we get a clearer picture. What you should think is that we have known the fact that $\mathbb{A}^1_{\mathbb{Z}}$ is the scheme that represents the the global section functor:

$$F : X \mapsto \Gamma(X, \mathcal{O}_X)$$

from the category of schemes to the category of groups and the fact that $\mathbb{A}^1_{\mathbb{Z}}$ is a group scheme. These two facts are both easy to establish separately, but what we have shown above tells you that these two are not separated and in fact they are consequences of each other and this relation can be generalized to any category.

Given a group scheme Y, you know that it represents a functor to the category of groups, i.e. $\mathrm{Mor}(-, Y)$. Moreover, you find that this functor is actually represented by Y. Conversely, given a representable functor F from the category of schemes to groups, we find that the representing object Y is a group object and moreover, $\mathrm{Mor}(-, Y)$ has exactly the same group structure as we started with. Therefore, these two constructions are kind of inverses of each other.

Moreover, our experience tells us that the idea can work further than just groups, and you should expect, for example, F is a representable functor from schemes to some category that is set with some additional structures, then the representing object should have similar properties.

Example 10.8. Let's see a few example and try implementing our idea from the above proposition.

The first example is our old friend $\mathbb{A}^1_{\mathbb{Z}}$, we know that it represents the function of global sections and we want to use this fact to give a group structure on $\mathbb{A}^1_{\mathbb{Z}}$. First, to obtain the multiplication map, we need to consider:

$$\mathrm{Mor}(X, \mathbb{A}^2_{\mathbb{Z}}) \to \mathrm{Mor}(X, \mathbb{A}^1_{\mathbb{Z}})$$

and this morphism comes from:

$$\mathrm{Mor}(X, \mathbb{A}^1_{\mathbb{Z}}) \times \mathrm{Mor}(X, \mathbb{A}^1_{\mathbb{Z}}) \to \mathrm{Mor}(X, \mathbb{A}^1_{\mathbb{Z}})$$

where the morphism that correspond to (f, g) is mapped to the map that correspond to $f + g$. Then we know that the morphims $X \to \mathbb{A}^2$ that corresponds to $x \mapsto f$ and $y \mapsto g$ goes to the morphism $X \to \mathbb{A}^1$ where $x \mapsto f + g$. And we know that this holds for each X and is functorial, therefore, this correspond to a morphism $\mathbb{A}^2 \to \mathbb{A}^1$ where we know it must be $x \mapsto x + y$. Therefore, the multiplication map is forced by the group structure on $\mathrm{Mor}(X, \mathbb{A}^1_{\mathbb{Z}})$.

Another example is $\mathbb{G}_m = Spec A[t, t^{-1}]$ where A is a ring. I claim that this is also a group scheme. To see this, notice that $\mathrm{Mor}(X, \mathbb{G}_m)$ for any A-scheme correspond to $t \mapsto f$ where f is a invertible element in $\Gamma(X, \mathcal{O}_X)$. Or in other words, we know that $\mathrm{Mor}(X, \mathbb{G}_m) = \Gamma(X, \mathcal{O}_X)^\times$. It has a natural group structure given by multiplication, thus we will assume that $\mathbb{G}_m$ also has a well defined group structure by what we have seen. Indeed, I will let you figure the multiplication map is:

$$Spec A[t, t^{-1}, s, s^{-1}] \to Spec A[t, t^{-1}]$$

where t is mapped to ts. The inverse is $t \mapsto t^{-1}$ and the identity is the natural $Spec A \to \mathbb{G}_m$.

The last example is the $\mathbb{GL}_n(A)$ group. It's defined to be:

$$\mathbb{GL}_n(A) = Spec A[x_{ij}, \Delta^{-1}]$$

where x_{ij} are $n \times n$ variables and Δ is the formal determinant of these variables. This group scheme is called the general linear group because you can see that an A-morphism from X to $\mathbb{GL}_n(A)$ corresponds to choose $n \times n$ functions in the global sections of X such that the determinant of which doesn't vanish. Let's try to figure out the product, inverse and identity. To figure out the product, as usual we need to look at:

$$\mathrm{Mor}(X, \mathbb{GL}_n(A) \times \mathbb{GL}_n(A)) \to \mathrm{Mor}(X, \mathbb{GL}_n(A))$$

where the first morphism correspond to choose $2 \times n \times n$ global functions on X such that the determinant of the first and second $n \times n$ functions f_{ij}, g_{ij} doesn't vanish. Then it's mapped to a morphism $X \to \mathbb{GL}_n(A)$ where the $n \times n$ functions comes from the matrix that is the product of (f_{ij}) and (g_{ij}). Thus, the multiplication map:

$$\mathbb{GL}_n(A) \times \mathbb{GL}_n(A) \to \mathbb{GL}_n(A)$$

is just x_{ij} maps to $[(x_{ij})(y_{ij})]_{ij}$, i.e. the ij-th element of the matrix. The remain stuff is left to you.

Another advantage of this functorial point of view is that is allows us to prove abstract statements easier:

Proposition 10.9. Product of group objects can be interpreted as group objects.

Proof. Say X, Y are both group objects, then we know that $\mathrm{Mor}(-, X)$ and $\mathrm{Mor}(-, Y)$ are both functors from the category of schemes to the category of groups.

We only need to show that $\mathrm{Mor}(-, X \times Y)$ is also a functor to the category of groups. But notice that you have a canonical isomorphism:

$$\mathrm{Mor}(-, X \times Y) = \mathrm{Mor}(-, X) \times \mathrm{Mor}(-, Y)$$

the you give it the product group structure, we are done. □

There is also a natural notion of morphisms of group objects:

Definition 10.10. Suppose that $\mathcal{C}$ is any category and X, Y are group objects in $\mathcal{C}$. We say that a morphism $f : X \to Y$ in $\mathcal{C}$ is in fact a morphism of groups objects if it commutes with the multiplication morphism, in the sense that the following diagram commutes:

$$\begin{array}{ccc} X \times X & \xrightarrow{f \times f} & Y \times Y \\ {\scriptstyle m_X}\downarrow & & \downarrow{\scriptstyle m_Y} \\ X & \xrightarrow[f]{} & Y \end{array}$$

Remark 10.11. In fact, just as in the category of groups, if a map preserves multiplication, then it automatically preserves inverse and identity, we can prove similar stuff here.

to prove it preserves inverse, we want to show that the diagram involving inverse commutes, and we translate is to the commutativity of:

$$\begin{array}{ccc} \mathrm{Mor}(-, X) & \xrightarrow{\circ f} & \mathrm{Mor}(-, Y) \\ {\scriptstyle \circ i_X}\downarrow & & \downarrow{\scriptstyle \circ i_Y} \\ \mathrm{Mor}(-, X) & \xrightarrow[\circ f]{} & \mathrm{Mor}(-, Y) \end{array}$$

Here the $\circ i_X$ and $\circ i_Y$ will be the inverse of the group structure on $\mathrm{Mor}(X, Y)$. But recall that f preserves multiplications implies that the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Mor}(-, X \times X) & \xrightarrow{\circ(f \times f)} & \mathrm{Mor}(-, Y \times Y) \\ {\scriptstyle m_X}\downarrow & & \downarrow{\scriptstyle m_Y} \\ \mathrm{Mor}(-, X) & \xrightarrow[\circ f]{} & \mathrm{Mor}(-, Y) \end{array}$$

but this diagram can be translated to the commutativity of the diagram that express the group structure of $\mathrm{Mor}(-, X)$ and $\mathrm{Mor}(-, Y)$, then we have translated everything to the category of groups and things are much easier here. The same strategy works for the identity morphism as well.

Example 10.12. We will show that there is a morphism of group schemes called the determinant map:

$$\det : \mathbb{GL}_n \to \mathbb{G}_m$$

I will give a functor morphism between:

$$\mathrm{Mor}(-, \mathbb{GL}_n) \to \mathrm{Mor}(-, \mathbb{G}_m)$$

such that it's compatible with the group structure on the object on both sides. This morphism is going to be the determinant morphism on global section, and I will let you verify using Yoneda that this corresponds to the morphism:

$$\mathbb{GL}_n \to \mathbb{G}_m$$

defined by $t \mapsto \det(x_{ij})$. We are done.

Another example is the following morphism:

$$(\cdot^n) : \mathbb{G}_m \to \mathbb{G}_m$$

defined by $t \mapsto t^n$ is a morphism of group schemes(you could interpret this morphism as defined as an A-algebra homomorphism which is determined by $t \mapsto t^n$, if you work over a field of characteristic dividing n, then you could also think of this as some sort of Forbenius morphism). To check this, we again check that if it defines a functor morphism for a functor to the category of groups.

Therefore, we need to first check that it defined a group morphism for each X, i.e. the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Mor}(X, \mathbb{G}_m) \times \mathrm{Mor}(X, \mathbb{G}_m) & \longrightarrow & \mathrm{Mor}(X, \mathbb{G}_m) \times \mathrm{Mor}(X, \mathbb{G}_m) \\ \downarrow & & \downarrow \\ \mathrm{Mor}(X, \mathbb{G}_m) & \longrightarrow & \mathrm{Mor}(X, \mathbb{G}_m) \end{array}$$

the commutativity is just $(fg)^n = f^n g^n$ for any invertible element f, g in the global sections of X. Then you need to show that this defines a functor morphism, i.e. the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Mor}(X, \mathbb{G}_m) \times \mathrm{Mor}(X, \mathbb{G}_m) & \longrightarrow & \mathrm{Mor}(X, \mathbb{G}_m) \\ \downarrow & & \downarrow \\ \mathrm{Mor}(Y, \mathbb{G}_m) \times \mathrm{Mor}(Y, \mathbb{G}_m) & \longrightarrow & \mathrm{Mor}(Y, \mathbb{G}_m) \end{array}$$

but this is also easy to check, we are done.

Remark 10.13. Using the language of the above few propositions and examples, we can actually prove the category of group schemes is a category, with the final object being also the initial object, thus the zero object.

Proposition 10.14. Suppose that $F : G_1 \to G_2$ is a morphism of group schemes, consider the contravariant functor:

$$\ker : X \mapsto \ker(\mathrm{Mor}(X, G_1) \to \mathrm{Mor}(X, G_2))$$

Assume further that this functor is represented by a scheme K, then it's a group scheme, with a natural morphism to G_1 making it the kernel of $G_1 \to G_2$.

Proof. Recall that this functor ker has a natural morphism to $\mathrm{Mor}(-, G_1)$, which is induced by the universal property of kernel. If it's representable, say by K, then we have a sequence of maps of functors:

$$\mathrm{Mor}(-, K) \to \mathrm{Mor}(-, G_1) \to \mathrm{Mor}(-, G_2)$$

Let's prove that K is in fact a group scheme, but the kernel of a group naturally induces a group structure, thus ker can be viewed as a functor to the category of schemes that is representable, thus K has a induced group scheme structure. Moreover, the functor morphism ker $\to \mathrm{Mor}(-, G_1)$ gives a natural morphism $K \to G_1$, then we only have to show that this is a morphism of group schemes that makes K the kernel.

Now surprisingly, we translate it to the category of groups using Yoneda. But what we have proved above actually tells you that any functorial morphism in the category of groups gives you a morphism that is a morphism of group schemes. Then to show that it's the kernel, we need to show that it satisfies a certain universal property, which again translates to Mor by Yoneda, we are done. □

Example 10.15. The kernel of $(\cdot^n)$ is representable, denoted by μ_n. Over a filed of characteristic p dividing n, this group scheme is not reduced.

To show this, notice that the kernel of the map of groups:

$$\mathrm{Mor}(X, \mathcal{G}_m) \to \mathrm{Mor}(X, \mathcal{G}_m)$$

where f is mapped to f^n, therefore, we know that the kernel is those functions f such that $f^n = 1$, i.e. all n-th root of unity in the global sections of X. Then I claim that it's represented by the following scheme:

$$\mu_n = SpecA[t]/t^n - 1$$

To see why we consider the morphism of schemes $\mathbb{G}_m \to \mu_n$ defined by $t \mapsto t$, then you get a induced morphism of the functor:

$$\mathrm{Mor}(-, \mu_n) \to \mathrm{Mor}(-, \mathbb{G}_m)$$

where f is mapped to f and $f^n = 1$, this is precisely the kernel functor of $\mathrm{Mor}(-, \mathbb{G}_m) \to \mathrm{Mor}(-, \mathcal{G}_m)$.

By a similar argument, you can show that the kernel of the determinant morphism $\det : \mathbb{GL}_n \to \mathbb{G}_m$ is also representable, which is called $\mathbb{SL}_n$, which is $SpecA[x_{ij}, \Delta - 1]$.

There are more notions you can define, for example the action of a group scheme:

Definition 10.16. Suppose that G is a group scheme and X is an arbitrary scheme, a left action of G on X is defined to be a morphism:

$$\alpha : G \times X \to X$$

such that the following two properties hold:

1. Identity axiom: The following composition:

$$X \xrightarrow{\simeq} Z \times X \xrightarrow{e \times id} G \times X \longrightarrow X$$

   is the identity morphism $X \to X$.

2. Associativity axiom: The following diagram commutes:

$$\begin{array}{ccc} G \times G \times X & \xrightarrow{id \times \alpha} & G \times X \\ \downarrow{\scriptstyle m \times id} & & \downarrow{\scriptstyle \alpha} \\ G \times X & \xrightarrow[\alpha]{} & X \end{array}$$

Remark 10.17. Similar to the notion of group schemes we can try to interpret this action using Yoneda since everything here is just dependent on morphisms of schemes and almost everything about morphisms can be described using Yodeda.

You will find that this is just a morphism of functors:

$$\mathrm{Mor}(-, G \times X) \to \mathrm{Mor}(-, X)$$

which can be written as:

$$\mathrm{Mor}(-, G) \times \mathrm{Mor}(-, X) \to \mathrm{Mor}(-, X)$$

and in the end you just obtain an action of $\mathrm{Mor}(-, G)$ on $\mathrm{Mor}(-, X)$ that is functorial. By functorial I just means that the corresponding morphism $\mathrm{Mor}(-, G \times X) \to \mathrm{Mor}(-, X)$ is a morphism of functors.

Conversely, given such a functorial group action, you can recover this group action $\alpha : G \times X \to X$.

Example 10.18. To given an example of actions by group schemes, I claim that a integer valued grading on a ring A is the same as a $\mathbb{G}_m$ action.

To see why, say you have a $\mathbb{G}_m$ action on A, i.e. a ring morphism:

$$\alpha : A \to A[t, t^{-1}]$$

that satisfies a two properties, i.e. the following diagram commutes:

$$\begin{array}{ccc} A[t, t^{-1}, s, s^{-1}] & \xleftarrow{\alpha, t \mapsto t} & A[t, t^{-1}] \\ {\scriptstyle id, t \mapsto ts}\uparrow & & \uparrow{\scriptstyle \alpha} \\ A[t, t^{-1}] & \xleftarrow[\alpha]{} & A \end{array}$$

and the following composition is the identity:

$$A \to A[t, t^{-1}] \to A$$

where $t \mapsto 1$ in A. We know that this α give the image of each $a \in A$ a unique finite decomposition:

$$\alpha(a) = \sum_{n \in \mathbb{Z}} a_n t^n$$

but we also need this to be a after we apply the morphism $A[t, t^{-1}] \to A$, therefore we know that $\sum_n a_n = a$. One thing that is interesting is that you can see that the commutativity of the diagram is automatically satisfied. Then we can define a grading on A by setting $A_d = \{a \in A : \alpha(a) = at^d\}$.

Now you need to show this is indeed a grading, i.e. A decomposed as a direct sum and $A_i A_j \subset A_{ij}$, the second condition is easy to check, thus we only have to worry about the direct sum part. First, we already see that every element in A has a decomposition, therefore, we only have to show that this is unique. Or equivalently, we need to show that $A_i \cap A_j = 0$ for $i \neq j$. Say a is in A_i and A_j, then we know that the image is both at^i and at^j for $i \neq j$, but this only holds when $a = 0$.

Now suppose that we have a grading, we want a $\mathbb{G}_m$-action, we define the morphism $A \to A[t, t^{-1}]$ to be:

$$a = \sum_d a_d \mapsto \sum a_d t^d$$

This is a well defined morphism of rings and I will let you see why. I claim that this is a action of $\mathbb{G}_m$, i.e. you need to show the commutativity, i.e. if you have $\sum a_d t^d$, then you need to show:

$$\sum a_d s^d t^d = \sum a_d s^d t^d$$

which is obvious. For the composition to be the identity, this is just the definition of the grading, and thus we get a $\mathbb{G}_m$-action.

Finally, it's easy to see that these two constructions are inverses of each other.

This is almost everything we want to say now about group schemes in general. There is definitely more to this notion and when you learn stuff like etale cohomology, you will have a lot of chances to practice with these kind of notions. But for now, let's move to something that is more relevant for us. For now, we want to work with varieties over a field k. One thing that we want to prove in the following discussion is that proper group varieties are abelian, due to the simple rigidity lemma, here the group varieties are just group objects in the category of varieties over a field k and in particular, it will be a group scheme.

Definition 10.19. An **algebraic group** over k is a smooth group variety over k.

Remark 10.20. This is a remark about some facts we won't either use or prove, it's here just for your general knowledge on group varieties:

1. A group variety over a field of characteristic 0 is automatically smooth, but this is false for fields of positive characteristics.
2. Algebraic groups are automatically quasi-projective.
3. An algebraic group is affine iff it admits a closed immersion into $\mathbb{GL}_n$ for some $n \geqslant 0$.

Definition 10.21. An **abelian variety** over a field k is an algebraic group that is **geometrically integral** and projective over k.

As the name suggests, abelian varieties are abelian, i.e. abelian varieties are commutative algebraic groups.

This is less tautological than you think since the two adjectives "abelian" is used in different senses, one is more in terms of geometric properties, i.e. geometrically integral and projective, but another one is a completely algebraic notion. It's somehow surprising that commutativity is forced by "compactness", i.e. properness. The key result is the following called the **rigidity lemma**:

Theorem 10.22. Let X, Y, Z be varieties, where X is proper and geometrically integral, with a k-valued point p and Y is irreducible. Let $pr : X \times Y \to Y$ be the projection and let $\alpha : X \times Y \to Z$ be any morphism suppose that $q \in Y$ is such that α is constant on $X \times \{q\}$, say $\alpha(X \times \{q\}) = r \in Z$, then:

1. There is a morphism $\psi : Y \to Z$ such that $\alpha = \psi \circ pr$, in particular, for every $q' \in Y$, α is constant on $X \times \{q'\}$.
2. If α is also constant on $\{p\} \times Y$, then α is constant on all of $X \times Y$.

The following diagram is helpful to understand what this diagram is saying:

$$\begin{array}{ccccc} X \times \{q\} & \longrightarrow & X \times Y & \xrightarrow{\alpha} & Z \\ \downarrow & & \downarrow{\scriptstyle pr} & \nearrow{\scriptstyle \psi} & \\ q & \longrightarrow & Y & & \end{array}$$

This diagram is saying that if there is such q, such that $X \times \{q\} \to X \times Y \to Z$ is constant, then there is a ψ such that the triangle on the right is commutative. Moreover, if α is also constant on the fiber over $\{p\}$, α is constant.

Remark 10.23. The hypothesis of this theorem can be relaxed somewhat, but this version suffices for our purpose, and when you read the proof below, you should first ignore the geometrically integral first and assume that you are working with algebraically closed fields and integral schemes to focus on the main idea.

Example 10.24. Let's use one example to show that the assumption that X is proper can not be removed.

Consider $X = Y = Z = \mathbb{A}^1_k$ and we define the morphism:

$$X \times Y \to Z$$

by $x \mapsto xy$. Notice that if you pick $q = (x)$, then we have the following diagram:

$$\begin{array}{ccccc} Speck[x] & \longrightarrow & Speck[x,y] & \longrightarrow & Speck[x] \\ \downarrow & & \downarrow & & \\ Speck & \longrightarrow & Speck[y] & & \end{array}$$

Then the top composition is defined by $x \mapsto 0$, then you find that it's indeed constant. But there is no ring morphism $k[x] \to k[y]$ such that it's composition with the canonical inclusion $k[y] \to k[x, y]$ is equal to the morphism that is defined by $x \mapsto xy$.

Now, let's prove this theorem and you can try to interpret from the proof that where properness is invoked:

Proof. Let's first consider this projection map $X \times Y \to Y$, we will first construct a section, denoted by σ_p which is pulled back from the $p \to X$. More precisely, we consider the following diagram:

$$\begin{array}{ccccc} Y & \longrightarrow & X \times Y & \longrightarrow & Y \\ \downarrow & & \downarrow & & \downarrow \\ p = Speck & \longrightarrow & X & \longrightarrow & Speck \end{array}$$

where we know that we can pick $p = Speck \to X$ such that the composition is the identity, which implies that the above composition is an automorphism of Y, then pre-compose with $Y \to X \times Y$ gives us a section. This is σ_p fits into the original diagram:

$$\begin{array}{ccccc} X \times \{q\} & \longrightarrow & X \times Y & \xrightarrow{\alpha} & Z \\ \downarrow & & {\scriptstyle pr}\downarrow \uparrow{\scriptstyle \sigma_p} & & \\ q & \longrightarrow & Y & & \end{array}$$

Now we define $\beta : X \times Y \to Z$ by $\beta = \alpha \circ \sigma_p \circ pr$. Now, if you can show that $\alpha = \beta$, we are done since we can take $\psi = \alpha \circ \sigma_p$.

To do this, we first know that $X \times Y$ is still integral. This is because that geometrically integral times integral is integral (varieties are themselves reduced). Recall that by reduced to separatedness theorem, we only have to show that α and β agrees on a nonempty open of $X \times Y$. Let U be an affine open neighborhood of r, we know that $\alpha^{-1}(Z - U)$ is a closed subset of $X \times Y$. Then as the projection pr to Y is proper (since X is proper and proper is preserved by base change), we know that $pr(\alpha^{-1}(Z - U))$ is closed in Z, it's complement is open and contains q, then we can assume that we have an open neighborhood of q disjoint from $pr(\alpha^{-1}(Z - U))$.

Now, let $\gamma : SpecK \to V$ be a geometric point of V, then we consider the following diagram:

$$\begin{array}{ccccccc} & & & & & & Z \\ & & & & & \overset{\alpha}{\nearrow} & \\ X_K & \longrightarrow & X \times V & \longrightarrow & X \times Y & \longrightarrow & X \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ SpecK & \longrightarrow & V & \longrightarrow & Y & \longrightarrow & Speck \end{array}$$

I claim that α_K which is the restriction of α to X_K is constant. The reason is that by definition of V, $X_K \to Z$ can be viewed as a morphism to U, which is affine, and morphisms to affine is determined by maps of global sections. Now, since X_K is integral proper over K, we know that it's global section is K, thus we know that a morphism $X_K \to U$ correspond to a k-algebra homomorphism:

$$A \to K$$

then we know that the kernel of this morphism is a k-algebra homomorphism, thus it factors as $A \to k \to K$ where $k \to K$ is the structure morphism. Then we know that this is just choosing a maximal ideal in A, thus we are done.

Similarly, we can prove that β_K is also constant. Then if we can prove that they have one point whose image is common, we can prove that α_K and β_K are equal as a map of sets. Recall that by definition $\beta = \alpha \circ \sigma_p \circ pr$, thus we know that $\alpha \circ \sigma_p \circ pr \circ i$ where $i : X_K \to X \times Y$, then $\beta_K(x) = \alpha \circ \sigma_p \circ pr \circ i(x)$, then if we can show that there is such a x such that $\sigma_p \circ pr \circ i(x) = i(x)$, we are done. Recall that by our definition of σ_p, if we can show that $i(x)$ is some $\sigma_p(y)$, then we are done and this is the content of the following diagram:

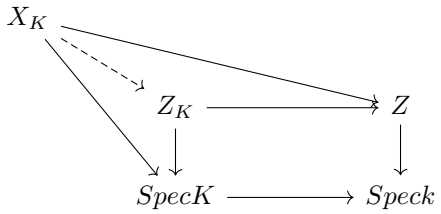
$$\begin{array}{ccccccc} \cdots & \longrightarrow & V & \longrightarrow & Y & \longrightarrow & p \\ \downarrow & & \downarrow & & \downarrow{\scriptstyle \sigma_p} & & \downarrow \\ X_K & \longrightarrow & X \times V & \longrightarrow & X \times Y & \longrightarrow & X \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ SpecK & \longrightarrow & V & \longrightarrow & Y & \longrightarrow & Speck \end{array}$$

Now, I claim that the fact that α_K, β_k agree as a map of sets implies that they actually agree as maps of varieties. To see why, recall that if you have a morphism $X \to Y$ of varieties that is over an algebraically closed field, then if they agree as a map of sets on closed points, they agree as morphisms of schemes. Now the question here is that X_K is over an algebraically closed field K, but Z is only over k, which is an arbitrary field. So to apply this, we need more work. Notice that the k-scheme morphisms:

$$X_K \to Z$$

is equivalent to a K-scheme morphism $X_K \to Z_K$ since wecan use the universal property of fibered product

and the following diagram:



Notice that the morphism as a map of sets from Z_K to Z is surjective, thus if two maps of sets X_K to Z_K agree after apply $Z_K \to Z$, then they agree before the composition, then we can use K is algebraically closed and conclude that being equal as a set theoretic map implies that they are equal as a vairiety morphism. Therefore, after the composition with $Z_K \to Z$, we still get the same morphism.

Finally, I claim that this implies that α and β implies on $pr^{-1}V$, which finishes the proof. To see this, let E be the equaliser of α and β, which is closed (since we are working with varieties so everything is separated). Then we consider the following diagram:

$$\begin{array}{ccccccc} E_K & \longrightarrow & E_V & \longrightarrow & E & & \\ \downarrow & & \downarrow & & \downarrow & & \\ X_K & \longrightarrow & X \times V & \longrightarrow & X \times Y & \overset{\beta}{\underset{\alpha}{\rightrightarrows}} & Z \\ \downarrow & & \downarrow & & \downarrow & & \\ SpecK & \longrightarrow & V & \longrightarrow & Y & & \end{array}$$

This implies that every geometric point of V lies in $pr(E_V)$, notice that $X \times V \to V$ is also proper, thus we know that the complement of the image of E_V in V is open, but there is not a single geometric point in that, using the fact that geometric points are dense, we know that the image of E_V is all of V. Notice that as we vary all the geometric point of V, we notice that the image of X_K covers every closed point of $X \times V$, therefore we know that the image of E_V covers every closed point of $X \times V$, then since closed points are closed and the image of E_V is closed in $X \times V$, we know that E_V to $X \times V$ is an isomorphism. Therefore we know that the image of $E \to X \times Y$ covers $X \times V$, we are done. □

Corollary 10.25. Let A be an abelian variety (algebraic group that is geometrically integral and projective), and G is any group variety. Let $\phi : A \to G$ is any morphism of varieties, then ϕ is a composition of a translation on A with a homomorphism of algebraic groups.

Let's first be specific about what is a translation. For a group variety over k, we define a translation to be the composition of the following morphisms:

$$G \xrightarrow{\simeq} Speck \times G \longrightarrow G \times G \xrightarrow{m} G$$

where $Speck \to G$ is a k-valued point. Then for this morphism $\phi : A \to G$, let e_A, e_G be the identity element (implicitly with morphisms $Speck \to A, Speck \to G$), suppose that $\phi(e_A) = x$, which is necessarily a k-valued point, then I claim that there is a translation T on G such that $T(x) = e_G$. To see this, consider the following composition:

$$Speck \longrightarrow G \xrightarrow{i} G$$

where i is the inversion morphism and $Speck \to G$ gives you the k-valued point x, we will call this translation $T_{x^{-1}}$. I claim that the translation by this morphism gives you the desired property. To see why, let's prove something more general. First, fix a k-valued point x, and we denote the map $Speck \to G$ by g_x, if we have a k-scheme T, then we can consider $T \to Speck \to G$, we call this morphism T_x then we consider the following morphism:

$$\mathrm{Mor}(T, G) \to \mathrm{Mor}(T, G)$$

where f is mapped to:

$$T \xrightarrow{f \times T_x} G \times G \xrightarrow{m} G$$

I claim that this is a natural transformation, since we know that if we have a k-scheme morphism $S \to T$:

$$\begin{array}{ccccc} T & \xrightarrow{f\times T_x} & G\times G & \xrightarrow{m} & G \\ {\scriptstyle\phi}\uparrow & & & & \\ S & \xrightarrow[(f\times T_x)\circ f]{} & G\times G & \xrightarrow[m]{} & G \end{array}$$

and we know that $(f\times T_x)\circ$ is $(f\circ\phi)\times(T_x\circ\phi) = (f\circ\phi)\times(S_x)$, then we compose with m to get $m\circ(f\circ\phi)\times(S_x)$ but this exactly $m\circ((f\circ\phi)\times S_x)$.

Therefore by Yoneda's lemma, this is given by the composition of a unique morphism and I claim that this morphism is the translation. Once we prove this, I claim the fact that $g_{x^{-1}}\circ g_x = id$ is easy to prove since all you need to do is to check that:

$$m\circ((m\circ(f\times T_x))\times T_{x^{-1}}) = id$$

The key to prove this property is the associativity of the multiplication map, i.e.

$$m\circ(id\times m) = m\circ(m\circ id)$$

as morphisms $G\times G\times G\to G$. In particular, if you have some T-valued points T_x $T\to G$ that comes from $T\to Speck\to G$, We have:

$$m(T_x, m(T_y,T_z)) = m(m(T_x,T_y),T_z)$$

this is because the first is:

$$m,\circ(id\times m)\circ(T_x,T_y,T_z)$$

while the second one is:

$$m\circ(m\circ id)\circ(T_x,T_y,T_z)$$

We are done.

Similarly, a homomorphism between group varieties is a morphism $\phi: G\to G$ such that $\phi(a_1,a_2) = \phi(a_1)\phi(a_2)$. Or if you want to make this precise, it's the following diagram commutes:

$$\begin{array}{ccccc} G\times G & \xrightarrow{\phi\times\phi} & G\times G & \xrightarrow{m} & G \\ {\scriptstyle m}\downarrow & & & \nearrow_{\phi} & \\ G & & & & \end{array}$$

Now, let go back to the proof:

Proof. Then we can assume that by composing ϕ with a translation on G, we assume that $\phi(e_A) = e_G$. Let's consider the morphism:

$$\alpha: A\times A\to G$$

given by $\alpha(a_1,a_2)\to\phi(a_1,a_2)\cdot\phi(a_1)^{-1}\phi(a_2)^{-1}$. Again, if you want to make this morphism precise, it's just:

$$A\times A\longrightarrow G^4\xrightarrow{m\times i\times i} G^3\xrightarrow{m} G$$

where we map the first A to the first and third of G using ϕ and the second A to the second and forth G using ϕ. Now if you look at what is $\alpha(\{e_A\}\times A)$ or $\alpha(A\times\{e_A\})$, you get $\{e_A\}$, therefore you can apply the rigidity lemma and conclude that α is constant, therefore:

$$\phi(a_1a_2) = \phi(a_1)\phi(a_2)$$

we are done. □

Corollary 10.26. Any abelian variety is an abelian group variety.

Proof. Apply the above corollary to $i : A \to A$, since $i(e) = e$, we know that i is a homomorphism, thus A is abelian. □

These are all the abstract properties we want to say about abelian varieties, now we turn to elliptic curves again to show that they are abelian varieties. Let's first prove that it's indeed a group object in the category of k-varieties. We have already seen that the degree 1 points on E forms a group and we have described this both in terms of geometric property and in terms of abstract group law using line bundles. But if E is a group object, we need to specify the multiplication, inverse and identity map, this is what we will do now.

Let's do a warm-up below:

Proposition 10.27. If char$k \neq 2, 3$, there is a morphism of k-varieties $E \to E$ that sends all degree 1 points to it's inverse and this construction behaves well under field extensions of k.

Proof. When k is not of characteristic $2, 3$, we can use the Weierstrass normal form and then let's consider the automorphism on $\mathbb{P}^2$ defined by the matrix:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Notice since the Weierstrass normal form of E is $y^2z = x^3 + axz^2 = bz^3$, this automorphism induces an automorphism on E, and we need to show that under this morphism, denoted by i, if q is a degree 1 point, then $i(q)$ is the inverse.

To see this, first notice that it preserves the identity $p = [0 : 1 : 0]$. Now, suppose that $q = [a : b : c]$ is a degree 1 point on E, we know that it's inverse is computed by asking what is another point in the line $\overline{qp}$, but we know that if $q = [a : b : c]$ is on the line, we know that $q' = [a : -b : c]$ is on the line. But also notice that q' is the image of q under i. We are done.

Finally, the fact that this definition is independent of field extension just follows from that every morphism we are considering here can be interpreted by a morphism induced by morphisms of graded rings, and this is stable under field extension since you can just do it by straight-forwad computation. □

To describe the addition algebraically, we will need a trick, which is the lemma below. We will give it more generality than we need to use, but if you prefer, you can just think we are working with a regular cubic in $\mathbb{P}^2$ for $k = \overline{k}$.

Lemma 10.28. Suppose that $C \subset \mathbb{P}^2_k$ is a geometrically integral cubic curve (in particular, it contains no lines, since if it does, then the defining equation $F = l \times Q$ where l is a linear and Q is a quadratic, then topologically it's the union of $V(l)$ and $V(Q)$, if Q has no l factor, we know that this is not irreducible, and if Q has, this is not reduced, either way, this is impossible), then there is a unique morphism $C^{reg} \times C^{reg} \to C^{reg}$ such that if p, q are distinct regular k-valued points of C, then $t(p, q)$ is obtained by intersecting the line $\overline{pq}$ with C and take the third point. More precisely, $\overline{pq}$ meets C at three points counted with multiplicity, including p, q both with multiplicity at least 1, $t(p, q)$ is the third point. This property holds after extension to $\overline{k}$.

Moreover, $t(p, p)$ is where the tangent line l to C at p meets C again, or more precisely, l meets C with multiplicity 3, including p at least 2, $t(p, q)$ is the third point, this is also true after extending to $\overline{k}$.

Proof. There are several preparations we need to do to prove this theorem. Let's first prove that if p, q are two regular points on C, then the intersection of $\overline{pq}$ with C are all regular. First, we know that C doesn't contain a line, thus the intersection of a line with C is of degree 3, which is the dimension of the global sections of the closed subscheme, which is just a finite collection of closed points, thus we know that on each closed point, it's a vector space over k with dimension 1 or 2 or 3.

Now, if the third point r is p or q, then we are done, since p, q are regular. If not, we know that r is a point with multiplicity 1, i.e. the dimension of the vector space over r is 1. This implies that r is k-valued point, otherwise we know that the stuff over r is also a nonempty vector space of the residue field, if the residue field is not k, then the dimension is never 1. This implies r is regular in C, since the codimension of r is 1 and the dimension of m/m^2 over k is 1 as well. Then recall that C is an effective Cartier divisor,

the equation defining C is not a zero divisor locally, then we know that in a locally Noetherian scheme if a point is regular on an effective divisor it's regular in the original space.

Then, let's assume that $k = \overline{k}$ and deal with the general case later. One advantage of assuming this is that over an algebraically closed filed, checking morphisms between varieties are equal, you only have to look at how they map the closed points. Let's first assume $p \neq q$ are two distinct regular k-valued points in C, we will define a morphism for a neighborhood of $(p, q) \in C^{reg} \times C^{reg}$. Or to be more precise, this (p, q) the k-valued point in $C^{reg} \times C^{reg}$ defined by:

$$\begin{array}{ccccc} \{p\} \times \{q\} & \hookrightarrow & \{q\} \times C & \longrightarrow & q \\ \downarrow & & \downarrow & & \downarrow \\ C \times \{p\} & \hookrightarrow & C \times C & \longrightarrow & C \\ \downarrow & & \downarrow & & \downarrow \\ p & \hookrightarrow & C & \longrightarrow & k \end{array}$$

notice that the stuff on the top left corner can be interpreted as k as well ($k \otimes_k k$ is k), thus is indeed a k-valued point in $C \times C$. We will define the morphism locally for $C^{reg} \times C^{reg} \to C^{reg}$ around (p, q), and since this is a morphism between varieties over algebraically closed field, we check the overlapping by see where the map the closed points.

To do this, the first step is to choose projective coordinates of $\mathbb{P}^2$ one of the opens $U_0 = Speck[x_1, x_2]$ contains p, q and r and the line $\overline{p, q}$ is not vertical in $Speck[x_1, x_2]$. More precisely, we can choose a line that misses these three degree 1 closed points, it's possible since we are working with an infinite field. Say this line is l_0. Then we also need to choose the coordinates such that p, q in the affine chart is not vertical. To satisfy this condition, we choose another line l_1 such that $l_0(q)l_1(p) \neq l_1(q)l_0(p)$ where $l_0(p)$ is defined by plugging in the projective coordinates of p to the linear form $l_0(p)$. We can indeed choose such a l_1 since we know that $l_0(q) \neq 0$, then we only require $l_1(p) \neq l_1(p)\frac{l_0(q)}{l_0(p)}$, for example, we can choose l_1 to be l_0 plus some linear form l' where $l'(p) = l'(q)$ and I will let you see why this works. The last coordinate l_2 can be chosen arbitrarily as long as it's independent to l_0, l_1. After this new change of coordinates, the points p, q has coordinates $(l_0(p), l_1(p), l_2(p))$ and $(l_0(q), l_1(q), l_2(q))$. This coordinate works since we know that in the affine chart $D_+(l_0)$, the coordinate of $p = (p_1, p_2)$ where $p_1 = l_0(p)/l_1(p)$ and the first coordinate of q is $l_0(q)/l_1(q)$ and we choose l_0, l_1 such that these are not equal.

In this new coordinate and affine chart U_0, C is again cut out by a cubic, which we sloppily denote by C and $C(x_1, x_2) = 0$. Now suppose that P, Q are two points of $C \cap U_0$, not necessarily our p, q, we attempt to compute the intersection of $\overline{PQ}$ with C, in a way that works on an open of $C \times C$ that includes p, q. We need some explicit by ugly high school algebra to explain this: In U_0, the line $\overline{PQ}$ is described by $x_2 = mx_1 + b$ where $m = \frac{P_2 - Q_2}{P_1 - Q_1}$, this is why we need to choose the coordinate such that $p_1 \neq q_1$, then we know that there is a open neighborhood of (p, q) in $C \times C$ such that all closed points in that open satisfies $P_1 \neq Q_1$ as this is an open condition. To be more precise, this condition is the complement of a closed condition. Let's just work locally with this affine chart $Speck[x_1, x_2]/C$, we know that the fibered product $Speck[x_1, x_2, y_1, y_2]/(C(x_1, x_2), C(y_1, y_2))$ contains (p, q) and we consider the regular function $x_1 - y_1$. We know that (p, q) is in $D(f)$ and any closed point in $D(f)$ satisfies $x_1 \neq y_1$, thus we are done.

Now we solve for $C \cap \overline{PQ}$, which requires some explicit algebra, but we can do some simplifications. We need to substitute $x_2 = mx_1 + b$ into the equations of C, this is a cubic in x_1 i.e.:

$$r(x_1) = Ax_1^3 + Bx_1^2 + Cx_1 + D = 0$$

We know that it has three roots as long as $A \neq 0$, since A is a polynomial of m, b, thus a rational function of P_1, P_2, Q_1, Q_2, therefore we are require a certain polynomial of P_1, P_2, Q_1, Q_2 is not 0, or in the fibered product we only have to use x_1, x_2 and y_1, y_2 to substitude P_1, P_2, Q_1, Q_2. Therefore, it's again an open condition. Recall that Q_1, P_1 are two solutions of $r(x_1)$ since P, Q are on the line. Recall that the sum of three roots of a cubic is $\frac{-B}{A}$, thus the third solution R_1 can be explicitly computed, thus $R_2 = mR_1 + b$. Recall that (p, q) intersect C with degree 3, thus p, q lies in that open, thus we have produced an open $(C^{reg} \cap U_0) \times (C^{reg} \cap U_0)$, which is an affine open (it's actually the restriction of the morphism $D \times D \to C \cap U_0$ where D is an affine open of $C \cap U_0$ and this morphism is defined algebraically using the above formula) we

don't want to go to the weeds of this, but the above argument should convince you that this is an algebraic map as it's defined from affine to affine, using ring maps. On over laps they agree on closed points since the above formula given is to compute the intersections point, but the intersection point is irrelevant of how you compute it.

This finishes the proof of the proposition when $k = \overline{k}$ and $p \neq q$. Let's try to extend this to arbitrary fields except for $k = \mathbb{F}_2$ (there will be a short discussion below about why $\mathbb{F}_2$ doesn't work or more general, if char$k = 2$, it may not work). And these morphism we define are actually insensitive to field extensions. The only place we are using algebraically closed is we want to conclude two morphisms are equal by saying that they agree on closed points. Therefore, we can first pass to the algebraic closure and then conclude that they are equal, but recall that for morphisms of k-schemes $X \to Y$, if they agree after base change to l/k, then they agree before the base change, we are done.

We still need to discuss the case where $P = Q$, but we can use our insight that for a regular plane curve, tangent lines are limits of the secant, and od similar algebras, we don't give the details here, but it's going to be similar to the above construction. The last possible case is where there is no such U_0 such that it contains p, q, r. I claim that there is always such a U_0 when the field has at least 3 elements, but it maybe bad if $k = \mathbb{F}_2$. If there are at least 3 elements in the field, and p, q, r are colinear, say on the line L. Notice that except the point $(0, 0, 0)$, if you solve:

$$ax + by + cz = 0$$

you get a two dimensional space, thus if $\mathbb{F}_2 = k$, there are only three points on the line, and any other line that intersects with L intersects at exactly one point, thus there is not way that there is a line missing p, q, r. But if there are at least 3 point, we have 5 points on the line, we can choose a point on the line that is not p, q, r, and let the line be a line passing through that point intersecting L exactly at that point. □

Remark 10.29. To solve the case where $k = \mathbb{F}_2$, we need to use some insight from descent theory, we don't include it here, but the above lemma remains true even if $k = \mathbb{F}_2$.

We now can use the above lemma to define the group variety structure on E:

Proposition 10.30. Suppose that (E, p) is an elliptic curve (geometrically regular, integral projective curve with genus 1 and a choice of a k-valued point p), take the Weierstrass embedding of E in $\mathbb{P}^2_k$, via the complete linear series $|\mathcal{O}_E(3p)|$, we define three morphisms:

1. Identity morphism:
$$Speck \to E$$
where the image is p.

2. Inverse morphism $i : E \to E$ where $q \mapsto t(p, q)$, or more precisely i is the composition:
$$E \xrightarrow{\simeq} Speck \times E \xrightarrow{e \times id} E \times E \xrightarrow{t} E$$
where t is the morphism we get by applying the previous proposition to E, which is a regular cubic which is geometrically integral in $\mathbb{P}^2_k$.

3. Multiplication morphism is defined by $E \times E \to E$ where (q, r) is mapped to $t(p, t(q, r))$, or more precisely it's the composition of:
$$Speck \times E \times E \xrightarrow{p \times id \times id} E \times E \times E \xrightarrow{id \times t} E \times E \xrightarrow{t} E$$

Then (E, e, i, m) defined above is a group variety over k, then if E is also smooth, it's an abelian variety, thus the multiplication map is also commutative.

Proof. Let's check that the morphisms defined above satisfies all the axioms of a group variety. For example, for the inverse axiom, we need to check that the two compositions:

$$m \circ (i, id) = m \circ (id, i)$$

which is the constant map from E to p, and you also need to check other morphism. Now, let's first assume that $k = \overline{k}$. Then we know that we only need to check that they agree on the level of closed points, or k-valued points.

Therefore, to check that, for example, $m \circ (i, id) = m \circ (id, i) = id$, consider a k-valued point of E, say q, it's mapped by (i, id) to the k-valued point on $E \times E$ at (q^{-1}, p) (this is because that we know that under i and id separately, q is mapped to the k-valued points q^{-1} and p, then for the product, it's a general fact that it's image is (q^{-1}, q)). Then we are applying t, but by the construction of t and our understanding of the group structure geometrically, the image of (q^{-1}, q) is the product of q^{-1}, q, which is p, thus the composition is the constant morphism to p, we are done since another one can be checked similarly.

The rest of the checking is all similar to the discussion above. □

Proposition 10.31. Suppose that p, q are k-valued points of a genus 1 curve, with our usual assumption, then there is an automorphism of E that sends p to q.

Proof. Consider the following morphism:

$$E \xrightarrow{\simeq} Speck \times E \xrightarrow{q \times id} E \times E \xrightarrow{m} E$$

I claim that this is an automorphism that takes p to q. To see why it's an automorphism, let's first assume $k = \overline{k}$, then consider the composition:

$$E \xrightarrow{\simeq} Speck \times E \xrightarrow{q \times id} E \times E \xrightarrow{m} E \xrightarrow{\simeq} Speck \times E \xrightarrow{q^{-1} \times id} E \times E \xrightarrow{m} E$$

we know that any x, which is a k-valued point on E, is mapped to:

$$x \cdot q \mapsto x \cdot q \cdot q^{-1} = x$$

therefore this composition agrees with the identity on each k-valued point they are equal as morphism of schemes, thus we are done.

For k not algebraically closed, all of the group morphisms are stable under base change since to $\overline{k}$ t is, therefore we first base change, conclude they agree after the base change, then conclude they are equal before the base change. □

This above morphism tells you that if you want an automorphism of elliptic curves (E, p), things are more restrictive, as you will want the automorphism to preserve the identity p, and below is result you can say about the automorphism group:

Proposition 10.32. Suppose that (E, p) is an elliptic curve over an algebraically closed field k of characteristic not 2 or 3, then the automorphism group of (E, p) is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/6\mathbb{Z}$.

Proof. Here this automorphism of (E, p) is an automorphism that fixes p scheme theoretically or equivalently fixing the k-valued point p in the sense that if α is this automorphism, then the composition below:

$$Speck \longrightarrow E \xrightarrow{\alpha} E$$

still maps the point of $Speck$ to p in E.

To see what are these automorphisms, let's fix one hyperelliptic map:

$$h : E \to \mathbb{P}^1$$

induced by $\mathcal{O}(2p)$, we know that by an automorphism of $\mathbb{P}^1$, we can assume that by an automorphism of $\mathbb{P}^1$, one of the ramification point is at ∞ and there are three distinct ramification points $\{p_1, p_2, p_3\}$. Let's assume that ∞ is the image of the point p.

Then suppose that you have an automorphism of E that preserves p, then you have the following diagram:

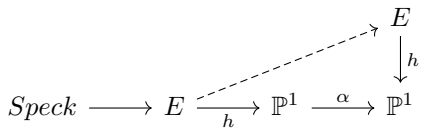
$$\begin{array}{ccccc} Speck & \longrightarrow & E & \longrightarrow & \mathbb{P}^1 \\ & & \downarrow{\scriptstyle \alpha} & & \vdots \\ & & E & \longrightarrow & \mathbb{P}^1 \end{array}$$

where the two morphism from E to $\mathbb{P}^1$ are the same map, which is the fixed hyperelliptic map. Most importantly, the pullback of $\mathcal{O}(2p)$ by α is still $\mathcal{O}(2p)$ since α preserves p, therefore we know that there is a unique automorphism of $\mathbb{P}^1$ such that the square is commutative. Then you also need to prove that this unique automorphism must preserve the set of the other 3 branch points. The key here is to recall that the ramification ponts on E are precisely the 2-torsion points. Then the fact that α preserve p is exactly the condition we need for α to preserve the 2 torsion point. The reason is suppose q is E below, is a two torsion point, then $\mathcal{O}(q) \neq \mathcal{O}(p)$, but $\mathcal{O}(2q) \simeq \mathcal{O}(2p)$, then when you pullback $\mathcal{O}(q)$, you just get $\mathcal{O}(\alpha^{-1}q)$ and when you pullback $\mathcal{O}(p)$, you get $\mathcal{O}(p)$, this shows you that $\alpha^{-1}q$ is still a 2-torsion point.

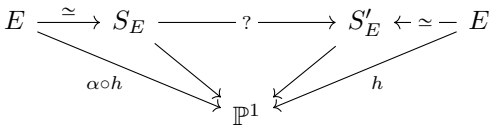
Moreover, this is obviously a group morphism between:

$$\mathrm{Aut}(E,p) \to \{\psi \in \mathrm{Aut}\mathbb{P}^1 : \psi(\infty) = \infty, \psi(\{p_1,p_2,p_3\}) = \{p_1,p_2,p_3\}\}$$

This is obviously surjective since for each automorphism of $\mathbb{P}^1$ that preserve ∞ and p_1, p_2, p_3, we can consider the following diagram:



the existence of the dotted map is guaranteed by Riemann-Hurwitz, and you can think of the existence by the following diagram below:



where S_E, S'_E are the standard hyperelliptic maps, and the morphism with a question mark in the middle is possibly the identity or the hyperelliptic involution, the composition of the three gives you the automorphism of (E,p) that you want.

Then we are interested in the kernel. Say α is mapped to id, we would like to know that kind of map α is, well, you still use the diagram above, the only difference is that $\alpha \circ h$ is now h, then Riemann-Hurwitz tells you that the top morphism only has two possibilities, differing by this hyperelliptic involution, thus the kernel is $\mathbb{Z}/2\mathbb{Z}$. Now we only need to characterize the last term in the homomorphism, which plus the kernel gives us full information on $\mathrm{Aut}(E,p)$.

Let's now deal with this, what you know is that since you want the automorphism to first preserve $[0:1]$, we can assume that you just work in $Speck[x] = D_+(x_0)$ where the automorphism is just $ax+b$ for all possible $a, b \in k$ at least one is not 0. Say that $\{p_1,p_2,p_3\}$ are three k-valued points (since we work with algebraically closed field, closed points are k-valued points) in this affine affine chart. What we require is that this affine change of coordinates to permute p_1, p_2, p_3. Let's first notice that there is a change of coordinates that sends p_1, p_2, p_3 to $0, 1, \lambda$ for some λ. We only require $ap_1 + b = 0$ and $ap_2 + b = 1$ since $p_1 \neq p_2$, we can take $a \neq 0$. Then we can try to find those a, b such that $0, 1, \lambda$ is preserved. There are several possible cases, for example, it's can happen that $0, 1$ is transposed but λ is fixed. in this case $\lambda = \frac{1}{2}$, and there are only two such affine change of coordinates. Or you can assume that there is a 3 cycle on $\{0, 1, \lambda\}$, in this case, there are 3 possible transformations. But for other S_3 actions on $\{0, 1, \lambda\}$, you can show that there is only the identity that fixes these three points. Therefore, times $\mathbb{Z}/2$, you get:

$$\mathbb{Z}/2, 4, 6$$

□

Proposition 10.33. Genus 1 curves (not elliptic so we don't choose a special p point!) over algebraically closed fields are classified up to isomorphism by j-invariants.

Proof. Since we are over algebraically closed fields, we can choose a k-valued point. Suppose that E, E' are two genus 1 curves, then we choose p, p' and use $\mathcal{O}(2p)$ and $\mathcal{O}(2p')$ to give a hyperelliptic map to $\mathbb{P}^1$.

If we first assume that they have the same j-invariant, this implies that the branch points of these two hyperelliptic maps are the same, up to automorphisms of $\mathbb{P}^1$, then we know that then E', E are isomorphic by Riemann-Hurwitz.

Then, let's assume that $\alpha : E \simeq E'$, we want to show that they have the same j-invariant. Let's assume that p, p' are the k-valued points we choose for E, E' such that $\alpha(p) = p'$. Then consider the following diagram:

$$\begin{array}{ccc} E & \xrightarrow{\quad\alpha\quad} & E' \\ & \searrow \quad \swarrow & \\ & \mathbb{P}^1 & \end{array}$$

this commutes by the fact that morphisms to $\mathbb{P}^1$ correspond to line bundles and nonvanishing sections. Therefore, E, E' have the same j-invariant as they have the same branch points. □

Proposition 10.34. Let k be an algebraically closed field of characteristic not 2, consider the genus 1 curve C in $\mathbb{P}^2$ define by $y^2z = x^3 + x^2z$ with the choice of identity $p = [0 : 1 : 0]$. Then, we consider $C - \{[0 : 0 : 1]\}$, it's a group variety isomorphic to $\mathbb{G}_m$.

Proof. Let's first compute the Jacobian, we know that the partials are:

$$3x^2 + 2xz, 2yz, y^2 + x^2$$

Then if we solve for when these are all 0, we know that it's $[0 : 0 : 1]$, therefore, this curve is not regular at this point! But it's will be regular at all the other points, thus this is the reason we want to take out this point. Degenerate just means this is not regular at $[0 : 0 : 1]$.

Then away from this point q, we know that each closed point is regular, thus we know that $\mathcal{O}(x)$ will be a degree 1 line bundle. Similarly, we know that a degree 1 line bundle vanishes at a degree 1 point of order 1, thus we can define a group structure on the degree 1 points by tensor products, and this is again can be geometrically interpreted by intersecting lines. Then we use the general argument before that there is a morphism from $C^{reg} \times C^{reg} \to C^{reg}$ such that (x, y) is mapped to the third intersection point, we can rebuild the group variety structure basically the same as any other elliptic curves.

To proceed further, one trick is to consider the following map:

$$\mathbb{P}^1 \to \mathbb{P}^2$$

where $x \mapsto 4uv(v - u)$, $y \mapsto 4uv(v + u)$, $z \mapsto (v - u)^3$, this map is the normalization of this curve, with an isomorphism on $\mathbb{P}^1$ minus the inverse image of $[0 : 0 : 1]$, which is $0, \infty$, thus is $\mathbb{G}_m$. To show that under this diagram, the group morphisms is preserved. Notice that the inverse image of $[0 : 1 : 0]$ is $[1 : 1]$, which is the identity in $\mathbb{G}_m$ and you can similarly check other group maps. □

11 Counter Examples Using Elliptic Curves

References