9. Hyperelliptic Cryptosystems

We will now work with a specific collection of examples of algebraic schemes that can be used for cryptosystems—hyperelliptic curves. In this case we can explicitly give a system of representatives for the elements of the K-group, a mechanism for "reducing" any element to one of these representing elements and also a bound for the size of the group. We will see in the next section how such information about a group can be used to make computations with the group efficient.

9.1. **Hyperelliptic curves.** Loosely speaking, hyperelliptic curves represent the solutions of the equations of the form

$$y^2 + a(x)y + b(x) = 0$$

where a and b are polynomials in x. To put this in the language of schemes developed earlier, we first restrict our attention to schemes over Spec($\mathbb{F}$) where $\mathbb{F}$ is a finite field called the *ground field*. Next we consider the $d - tuple$ Veronese embedding of $\mathbb{P}^1$ in $\mathbb{P}^d$; also known as the "rational normal curve of degree d"; this is given as the locus of $(1 : x : x^2 : \cdots : x^d)$ as $(1 : x)$ varies over $\mathbb{P}^1$. Alternatively, it is described by the system of equations $X_pX_q = X_rX_s$ for all p, q, r, s such that $p + q = r + s$. Let us consider $\mathbb{P}^{d+1}$ with $(X_0 : \cdots : X_d : Y)$ as its co-ordinates so that $\mathbb{P}^d$ is obtained by projecting from the point (vertex) $v = (0 : \cdots : 0 : 1)$. Let S_d denote the "cone" over the rational normal curve of degree d; it is the subvariety of $\mathbb{P}^d$ defined by the same set of equations as above (in other words the variable Y is "free"). Now suppose that $a(x) = \sum_i a_ix^i$ is a polynomial of degree at most d and $b(x) = \sum_i b_ix^i$ is a polynomial of degree at most $2d$. We consider the linear forms

$$\begin{aligned} A(X) &= \sum_{i=0}^{d} a_iX_i \\ B(X) &= \sum_{i=0}^{d} b_iX_i \\ C(X) &= \sum_{i=1}^{d} b_{d+i}X_i \end{aligned}$$

and the quadratic equation $Y^2 + A(X)Y + B(X)X_0 + C(X)X_d = 0$. The addition of this equation to the equations for S defines a subvariety T of S. It is clear that the vertex v does not lie on T so that projection gives a morphism on T which lands in the rational normal curve of degree d. Thus, we have a morphism $T \to \mathbb{P}^1$. There is an involution on $\mathbb{P}^{d+1}$ which fixes the X's and sends Y to $A(X) - Y$. Clearly this involution ι sends T to itself and pairs of points that are involutes of each other are sent to the same point in $\mathbb{P}^1$. The variety T is called a hyperelliptic curve, the involution is called the hyperelliptic involution and the morphism $T \to \mathbb{P}^1$ is called the canonical morphism.

Now it is clear that a solution (x, y) of the equation $y^2 + a(X)y + b(x) = 0$ gives rise to the solution $(1 : x : \cdots : x^d : y)$ of the above system. Conversely, if we have a solution $(X_0 : X_1 : \cdots : X_d : Y)$ of the system of equations with X_0 a unit, then we can put $(x, y) = (X_1/X_0, Y/X_0)$ to obtain a solution of the two variable equation. Similarly, if $(X_0 : \cdots : X_d : Y)$ is a solution of the system of equations and X_d is a unit then consider the pair $(u, v) = (X_{d-1}/X_d, Y/X_d)$; this pair satisfies a two variable equation $v^2+a'(u)v+b'(u)=0$, where $a'(u)=u^da(1/u)$ and $b'(u)=u^{2d}b(1/u)$. One sees from the above system that either X_0 or X_d must be a unit so we have covered all cases. The Jacobian criterion for regularity can be used to show that the curve defined by $y^2+a(x)y+b(x)=0$ is regular when either,

(1) the discriminant $a(x)^2-4b(x)$ has distinct roots, or
(2) the field $\mathbb{F}$ has characteristic 2, $a(x)$ has distinct roots and for each point (x_0,y_0) where x_0 is a root of $a(x)$, the polynomial $b(x)-b(x_0)-y_0a(x)$ vanishes with multiplicity one at 0.

To apply this to the equation $v^2+a'(u)v+b'(u)=0$, we note that

$$a'(u)^2-4b'(u)=u^{2d}(a(1/u)^2-4b(1/u))$$

Thus, if $a(x)^2-4b(x)$ has distinct roots, then the only multiple root of $a'(u)^2-4(b'(u)$ can be at $u=0$; moreover, this happens only if $a(x)$ has degree less than $d-1$ and $b(x)$ has degree less than $2d-1$. From now one we will assume the T is regular or non-singular; in fact we will assume that $b(x)$ has degree *equal* to $2d-1$. The point $(0:\cdots:0:1:0)$ is a point on the curve T is called the "point at infinity" and denoted ∞. The number $g=d-1$ is called the genus of the hyperelliptic curve. The points on T where $a(x)^2-4b(x)$ vanishes and the point at infinity are called the *Weierstrass points* of the hyperelliptic curve; these are precisely the fixed points of the Weierstrass involution.

9.2. **Closed points.** A proper closed reduced irreducible subscheme of T (or $\mathbb{P}^1$) is called a *closed point*. Let P be a closed point of T and Q be its image in $\mathbb{P}^1$. If U, V denote the coordinates on $\mathbb{P}^1$ then Q is defined as the vanishing locus of an irreducible homogeneous polynomial $F(U,V)$. Thus either $F=V$ and Q is the point at infinity on $\mathbb{P}^1$ or V does not divide F. In the latter case Q is contained in $\mathbb{A}^1$ which is the open subset of $\mathbb{P}^1$ where V is a unit (i. e. the complement of the point at infinity). The coordinate on $\mathbb{A}^1$ is given by $x=U/V$ and Q defined by the irreducible polynomial $f(x)=F(U,V)/V^{\deg(F)}$. Now, if Q is the point at infinity then the description in the previous paragraph shows that P must be the point at infinity on T. In the second case P is an irreducible closed subscheme of the subscheme of $\mathbb{A}^2$ defined by the equations

$$\begin{aligned} y^2+a(x)y+b(x) &= 0 \\ f(x) &= 0 \end{aligned}$$

In other words, let $E=\mathbb{F}[x]/(f(x))$ be the finite extension of the ground field $\mathbb{F}$ and let α and β be the images of $a(x)$ and $b(x)$ in E. The closed point P is given by solving the equation $y^2+\alpha y+\beta$ over E. Clearly, there are three cases to consider. The case when this equation has multiple roots (when $\alpha^2-4\beta=0$) is clear the case which corresponds to Weierstrass points. The case when this equation is irreducible over E is the case case when P is the full inverse image of Q under the morphism $T\to\mathbb{P}^1$. Finally, when the quadratic equation is solvable in E, there is an element γ in E that corresponds to the point P. Now γ is the image in E of a polynomial $g(x)$ in $\mathbb{F}[x]$, we can further choose g so that its degree is less than the degree of f. To summarise, a closed point of T takes one of the following forms:

(1) The point at infinity on T.
(2) An irreducible factor $f(x)$ of the discriminant $a(x)^{-}4b(x)$ is given. In this case there is a unique polynomial $g(x)$ of degree less than $\deg(f)$ so that

$y = g(x)$ represents the (unique) solution of the equation $y^2 + a(x)y + b(x)$ in the field $E = \mathbb{F}[x]/(f(x))$.

(3) We have an irreducible polynomial f that is co-prime to the discriminant and the quadratic equation $y^2 + a(x)y + b(x)$ is irreducible modulo $f(x)$.

(4) We have an irreducible polynomial $f(x)$ that is co-prime to the discriminant. Moreover, we are given a polynomial $g(x)$ of degree less than $\deg(f)$ so that $y = g(x)$ represents one of the two solutions of the equation $y^2 + a(x)y + b(x)$ in the field $E = \mathbb{F}[x]/(f(x))$.

We note that the first two cases above correspond to Weierstrass points on T.

One should not be misled by the term "closed point"—when considering solutions over general finite rings (in our case rings that are finite dimensional vector spaces over $\mathbb{F}$ suffice), we can find that each closed point has many "elements". In fact, let $\mathbb{F}(P)$ denote the field $E = \mathbb{F}[x]/(f(x))$ in cases (2) and (4). In case (3) let $\mathbb{F}(P)$ be the quadratic extension of E where the irreducible quadratic polynomial $y^2+\alpha y+\beta$ has its roots. We note that $\mathbb{F}(P)$ is a finite extension of the finite field $\mathbb{F}$ and hence is a Galois extension; thus it contains *all* the roots of any polynomial which has *one* of root in it. From this one sees that $P(\mathbb{F}(P))$ is a finite set of cardinality equal to the degree $[\mathbb{F}(P) : \mathbb{F}]$; note that this is $\deg(f)$ in cases (2) and (4) and is $2\deg(f)$ in case (3). This number $\mathbb{F}(P) : P]$ is called the *degree* of the closed point P and denoted $\deg(P)$.

9.3. **Divisors.** Let Z be a proper closed subscheme of T and W be its image in $\mathbb{P}^1$. As before W is defined as the vanishing locus of a homogeneous polynomial $F(U, V)$. Let $F = V^k F_1^{k_1} \cdots F_r^{n_r}$ be a factorisation of F with F_i irreducible and distinct from each other and V. Clearly W is the disjoint union of closed subschemes W_i each defined by the vanishing of $F_i(U, V)^{k_i}$ and the scheme W_0 defined by $V^k = 0$. As before, we write $f_i(x) = F_i(U, V)/V^{\deg(F_i)}$, where $x = U/V$; let Q_i denote the closed point in $\mathbb{A}^1$ defined by f_i and Q_0 be the point in $\mathbb{P}^1$ defined by $V = 0$. We can decompose Z into the components Z_i that lie over the component W_i of W. We can then classify Z_i according to the classification of the polynomials f_i as above. In cases (1), (2) and (3) above there is exactly one closed point that lies over Q_i, thus the schemes Z_i are "thickenings" of the corresponding closed points P_i. In case (4) there are two closed points corresponding to the distinct roots; we denote these by $P_{i,1}$ and $P_{i,2}$. Let $P_{i,1}$ correspond to the solution $y = g(x)$ or $y^2 + a(x)y + b(x) = 0$ in $\mathbb{F}[x]/(f_i(x))$. By Hensel's lemma we can find $g_{k_i}(x)$ in $\mathbb{F}[x]/(f_i(x)^{k_i})$ which is a "lift" of the solution $g(x)$. Thus we have the closed subscheme $Z_{i,1}$ of Z_i defined by the solution $y = g_{k_i}(x)$. Similarly, we have $Z_{i,2}$ and it is clear that Z_i is the union of these two schemes. Thus each proper closed subscheme of T is the disjoint union of "thickened" closed points.

For any such closed subscheme Z of T we have a vector space scheme given by $(\mathbb{G}_a)_Z$ extended by zero on the rest of T. We denote this vector space scheme by (P) when Z is the subscheme associated to the a closed point P. The vector space scheme associated with the "thickened" closed points is equivalent, in the K-group, to $n(P)$ for some integer n. This can be shown by a "composition series argument". A similar Jordan–Hölder composition series can be used to show that the K-group of T is generated by $(\mathbb{G}_a)_T$ and the elements (P). Moreover, if we consider an element D of the form $\sum_i n_i(P_i)$ of the K-group then the number $\deg(D) = \sum n_i \deg(P_i)$ can be shown to be well-defined (independent of the representation of D). Thus the important group becomes the group of "divisors of degree 0" of the subgroup of the K-group consisting of elements of the form $\sum_i n_i(P_i)$ where $\sum_i n_i \deg(P_i) = 0$. This group is denoted $\mathrm{Pic}^0(T)$. An important theorem of Weil states that there is a group scheme J (called the Jacobian variety of T) such that $\mathrm{Pic}^0(T)$ can be naturally identified with $J(\mathbb{F})$. There is also a natural analogy of this with the divisor class group for quadratic number fields that we will consider in the next subsection.

To compute the group $\mathrm{Pic}^0(T)$ of divisors of degree 0, it enough to work modulo (∞) which is of degree 1, since any divisor can be converted to one of degree 0 by subtracting a suitable multiple of (∞). Thus, we see that this group is generated by the elements $[P] = (P) - \deg(P)(\infty)$. For a divisor D of degree d we introduce the notation $[D] = D - d(\infty)$ to denote the corresponding element in $\mathrm{Pic}^0(T)$.

9.4. **Computing with the divisor class group.** Let Q be any closed point in $\mathbb{P}^1$ that is different from the point ∞ at infinity. As we saw above Q is given as a closed subscheme of $\mathbb{A}^1 = \mathbb{P}^1 - \infty$ as the vanishing locus of an irreducible polynomial $f(x)$. If $k = \deg(f)$ then consider the f-fold Veronese embedding of $\mathbb{P}^1$ in $\mathbb{P}^k$. We see that Q is precisely the intersection of the image of $\mathbb{P}^1$ with the hyperplane $V(a_0X_0 + \cdots + a_kX_k)$ (if $f(x) = a_0 + \cdots + a_kX^k$). Moreover, $V(X_0)$ intersects the image of $\mathbb{P}^1$ in a k-tuple thickening of ∞. From earlier remarks on the K-group we see that $(Q) = k(\infty)$ in $K(\mathbb{P}^1)$.

Now the morphism $T \to \mathbb{P}^1$ is flat and so we get a group homomorphism $K(\mathbb{P}^1) \to K(T)$. In particular, in the various cases enumerated above, for closed points P in T that lie over closed points Q in $\mathbb{P}^1$ we have:

(1) The image of the element (∞) under this homomorphism is $2(\infty)$.
(2) If Q is the closed point corresponding to an irreducible factor of $a(x)^2 - 4b(x)$, then the image of (Q) is $2(P)$.
(3) If $f(x)$ is an irreducible polynomial so that $y^2 + a(x)y + b(x)$ is irreducible modulo $f(x)$, then the image of (Q) is (P).
(4) If $f(x)$ is an irreducible polynomial so that $y^2 + a(x)y + b(x)$ has distinct roots $g(x)$ and $h(x)$ modulo $f(x)$, then there are two closed points P and P' that lie over Q and the image of (Q) is $(P) + (P')$.

From the relation $(Q) = \deg(Q)(\infty)$ we obtain relations in each case as follows. In case (2) we see that $\deg(P) = \deg(Q)$ so that $(Q) - \deg(Q)(\infty)$ has the image $2[P] = 2(P) - 2\deg(P)(\infty)$; thus $[P]$ is a two torsion point in this case. In case (3), we have $\deg(P) = 2\deg(Q)$ and so that $(Q) - \deg(Q)(\infty)$ has image $[P] = (P) - \deg(P)(\infty)$; thus $[P]$ is 0 in this case. In case (4) $\deg(P) = \deg(P') = \deg(Q)$ and the image of $(Q) - \deg(Q)(\infty)$ is $[P] + [P']$ which gives us the identity $[P] + [P'] = 0$.

Thus, elements of $\mathrm{Pic}^0(T)$ can be written in the form $\sum_i n_i[P_i] + \sum_j [P_j]$ where the former $[P_i]$ are all of type (4) and the latter $[P_j]$ are of type (2). As we saw above, Hensel's lemma allows us to lift the solution $y = g(x)$ of the equation $y^2 + a(x)y + b(x)$ modulo $f(x)$ in case (4) to a solution $y = g_k(x)$ modulo $f(x)^k$ for any k. Combining this with the Chinese remainder theorem, we see that divisors are characterised as solutions $y = g(x)$ of $y^2 + a(x)y + b(x)$ modulo $f(x)$, where $f(x)$ is not necessarily irreducible. Conversely, given such a solution, let $Z = V(y - g(x), f(x))$ and we have the divisor $(Z) - \deg(f)(\infty)$ in $\mathrm{Pic}^0(T)$.

To summarise, each divisor class in $\mathrm{Pic}^0(T)$ is represented by a pair of polynomials $(f(x), g(x))$, where $g(x)$ has degree less than that of $f(x)$ and $g(x)^2 + a(x)g(x) + b(x)$ is divisible by $f(x)$; as we shall see below this representation is *not* unique. We can further assume that any irreducible factor of $f(x)$ that divides $a^2(x) - 4b(x)$ divides $f(x)$ at most once. Moreover, it is clear that the inverse of this class in $\mathrm{Pic}^0(T)$ is represented by $(f(x), g_1(x))$, where $g_1(x)$ is the reduction modulo $f(x)$ of $a(x) - g(x)$.

If $(f_1(x), g_1(x))$ and $(f_2(x), g_2(x))$ are two such pairs, then we can form their sum in $\mathrm{Pic}^0(T)$ as follows.

(1) Assume that $f_1(x)$ and $f_2(x)$ are co-prime. We find $h_1(x)$ and $h_2(x)$ so that $h_1 f_1 + h_2 f_2 = 1$. Let $g(x)$ be the reduction of $h_1 f_1 g_2 + h_2 f_2 g_1$ modulo $f_1 f_2$. We see that $g(x)$ reduces to $g_1(x)$ modulo f_1 and to $g_2(x)$ modulo f_2. Hence, by the Chinese Remainder Theorem it follows that $g(x)^2 + a(x)g(x) + b(x)$ is divisible by $f(x) = f_1(x) f_2(x)$. Thus the sum is $(f(x), g(x))$.

(2) Now suppose that $h(x)$ is a common factor of $f_1(x)$ and $f_2(x)$. We further write $h(x) = h_1(x)h_2(x)$ where $h_1(x)$ is the common factor of $h(x)$ with $a^2(x) - 4b(x)$. Since the corresponding elements $[P]$ (in case (2) as above) are of order 2 it follows that this factor disappears when the sum is taken in $\mathrm{Pic}^0(T)$. In other words, let $f_1'(x)$ and $f_2'(x)$ be the quotients of $f_1(x)$ and $f_2(x)$ by $h_1(x)$ respectively, and let $g_1'(x)$ and $g_2'(x)$ be the reductions of $g_1(x)$ by $f_1(x)$ and $g_2(x)$ by $f_2(x)$ respectively. The sum of the pairs $(f_1'(x), g_1'(x))$ and $(f_2'(x), g_2'(x))$ is the same as the sum we want to compute.

(3) Assume that the common factor $h(x)$ of $f_1(x)$ and $f_2(x)$ is co-prime to $a^2(x) - 4b(x)$. Let h_1 be the highest common factor of h with $g_1 + g_2 - a$ and let $h_1 = h/h_2$. Now, both g_1 and g_2 a solutions of $y^2 + a(x)y + b(x) = 0$ modulo $h_1(x)$ and their sum is $a(x)$. It follows that these are complementary solutions as in case (4) above. Thus these cancel out when the sum is taken in $\mathrm{Pic}^0(T)$. As in the previous case, we can replace the pairs (f_1, g_1) and (f_2, g_2) by another pair with the same sum, with the property that the f_1, f_2 and $g_1 + g_2 - a$ have no common factor.

(4) Assume that the common factor $h(x)$ of $f_1(x)$ and $f_2(x)$ is co-prime to $a^2(x) - 4b(x)$ and to $g_1(x) + g_2(x) - a(x)$. Now, both g_1 and g_2 are solutions of $y^2 + a(x)y + b(x) = 0$ modulo $h(x)$ and they are not complementary modulo any factor of $h(x)$. By the uniqueness part of Hensel's lemma it follows that $g_1(x)$ and $g_2(x)$ is have the same reduction $m(x)$ modulo $h(x)$. Another application of Hensel's lemma allows us to lift $m(x)$ to a solution $m_k(x)$ of the above equation modulo $h(x)^k$, for every power k. Now, we can write $f_1(x) = n_1(x) f_1'(x)$ where $f_1'(x)$ has no factor in common with $h(x)$, moreover $n_1(x)$ is the greatest common factor of $f_1(x)$ with $h(x)^{k_1}$ for a suitable power k_1; similarly $f_2(x) = n_2(x) f_2'(x)$. Let k be such that $h(x)^k$ is divisible by $n_1(x)n_2(x)$. By using the Chinese Remainder theorem as before, we can find $g'(x)$ which lifts the solutions $m_k(x)$ modulo $h(x)^k$, $g_1(x)$ modulo $f_1'(x)$ and $g_2(x)$ modulo $f_2'(x)$ to a solution modulo $h(x)^k f_1'(x) f_2'(x)$. Reducing this solution modulo $f_1 f_2 = n_1 n_2 f_1' f_2'$, we obtain the required pair $(f(x), g(x))$.

Finally we need to "reduce" divisors to a bounded collection. For this we use our original description of the hyperelliptic curve T as a closed subscheme of the cone S_d in $\mathbb{P}^{d+1}$. We have noted earlier that if L is any $\mathbb{P}^d$ sitting linearly in $\mathbb{P}^{d+1}$, then we have an exact sequence

$$0 \to (\mathbb{V}^1 \times L)_{\mathbb{P}^{d+1}} \to \mathbb{V}^1 \times \mathbb{P}^{d+1} \to H \to 0$$

Now the restriction of $(\mathbb{V}^1 \times L)_{\mathbb{P}^{d+1}}$ to T is $(\mathbb{V}^1 \times D)_T$ where D is the divisor on T given by the intersection of L and T. As remarked earlier, this shows that the class in $K_0(T)$ of $(L \cap T)$ is independent of L. One such L is $V(X_0)$ which intersects T in $2d(\infty)$. Thus, we note that if $(L \cap T) = \sum_i n_i(P_i)$ then $\sum_i n_i[P_i] = 0$ in $\mathrm{Pic}^0(T)$.

Now, any collection of $d+1$ points in $\mathbb{P}^{d+1}$ lie on an L which contains them. More generally, on can show the same for a divisor of degree $d+1$ on T. Now any L intersects T in a divisor of degree $2d$. In particular, given any divisor D of degree d, we can find an L that contains $D + (\infty)$, so that L intersects T in $D + (\infty) + E$ where E has degree $d-1$. Thus, we see that $[D] + [E] = 0$ in $\mathrm{Pic}^0(T)$. The inverse of $[D]$ for a divisor D of degree d is thus represented by $[E]$ where E has degree $d-1$. This is the basic geometric idea behind the reduction of divisors. The algebraic steps for this reduction are described below.

As we saw above, elements of $\mathrm{Pic}^0(T)$ are represented by pairs $(f(x), g(x))$, where $g(x)$ has degree less than the degree of $f(x)$ and $h(x) = g(x)^2 + a(x)g(x) + b(x)$ is divisible by $f(x)$. Moreover, we can also assume that $f(x)$ is divisible at most once by any irreducible factor that it has in common with $a(x)^2 - 4b(x)$. Now if $f(x)$ has degree $d+k$, then $h(x)$ has degree at most the maximum of $\{2(d+k-1), (d-1)+(d+k-1), 2d-1\}$. Thus writing $h(x) = f(x)f'(x)$ we see that $f'(x)$ has degree at most the maximum of $\{d+k-2, d-1\}$. Moreover, if $g'(x)$ is the reduction of $g(x)$ modulo $f'(x)$, then $(f'(x), g'(x))$ is another pair representing an element of $\mathrm{Pic}^0(T)$. Now, let $g(x) = \sum_i a_i x^i$ have degree at most d and put $G(X) = \sum_i a_i X_i$. Then $(f(x)f'(x), g(x))$ represents the divisor $L \cap T$ where $L = V(Y - G(X))$, thus we see that $(f'(x), g'(x))$ represents the inverse of the element of $\mathrm{Pic}^0(T)$ that is represented by $(f(x), g(x))$ in this case. This argument can be generalised to the case g has degree more than d as well (by using the k-tuple Veronese embedding of $\mathbb{P}^{d+1}$ and using linear subspaces from there) to show the same result.

To summarise, we have two ways of representing the inverse of an element of $\mathrm{Pic}^0(T)$ that is represented by the pair $(f(x), g(x))$. One method is to let $g_1(x)$ be the reduction modulo $f(x)$ of $a(x) - g(x)$ and take the pair $(f(x), g_1(x))$. The other method is to take $f'(x)$ to be the quotient of $g(x)^2 + a(x)g(x) + b(x)$ by $f(x)$ and $g'(x)$ to be the reduction of $g(x)$ modulo $f(x)$. Combining these let $f_2(x)$ be the quotient by $f(x)$ of

$$(a(x) - g(x))^2 + a(x)(a(x) - g(x)) + b(x) = g(x)^2 - a(x)g(x) + b(x)$$

and $g_2(x)$ be the reduction modulo $f_2(x)$ of $a(x) - b(x)$. We see that the pair $(f(x), g(x))$ and the pair $(f_2(X), g_2(x))$ represent the same element in $\mathrm{Pic}^0(T)$. Moreover, if $f(x)$ has degree $d+k$ for some $k \geq 0$, then $f_2(x)$ has strictly smaller degree. Thus we have a method to reduce all pairs representing elements of $\mathrm{Pic}^0(T)$ to pairs $(f(x), g(x))$ where $f(x)$ has degree at most $d-1$.

9.5. **Frobenius Endomorphism.** Since all our varieties are defined over a finite field $\mathbb{F}$, there is a special endomorphism to consider. Let q be the number of elements of the field, then for any element of the field $a = a^q$. Thus for any polynomial $f(t_1, \ldots, t_r)$ with coefficients in $\mathbb{F}$ we have

$$f(t_1, \ldots, t_r)^q = f(t_1^q, \ldots, t_r^q)$$

Now consider the endomorphism of $\mathbb{P}^k$ given by $(X_0 : \cdots : X_k) \mapsto (X_0^q : \cdots : X_k^q)$. If $X = V(F_1, \ldots, F_p; G_1, \ldots, G_q)$ is a subscheme of $\mathbb{P}^k$ and the polynomials F_i

and G_j have coefficients in $\mathbb{F}$, then this endomorphisms sends X to itself. This endomorphism of X is called the Frobenius Endomorphism $F : X \to X$.

If A is any finite dimensional $\mathbb{F}$-algebra, then $a \mapsto a^q$ gives a ring homomorphism from A to itself. Moreover if A is local, then the only elements of A that are fixed under this homomorphism are elements of $\mathbb{F}$. From this one can show that the intersection of the diagonal Δ_X with the graph Γ_F of the Frobenius in $X \times X$ is precisely $X(\mathbb{F})$; the points of X over $\mathbb{F}$.

Now for any regular scheme X over $\mathbb{F}$, the Frobenius F is a flat morphism and thus gives an endomorphism of $K_0(X)$. The latter group thus acquires some "structure" in addition to being an abelian group. In the case when X is a curve (or more specifically a hyperelliptic curve) this has additional consequences. As we remarked above $K_0(X)$ is decomposed as the free group on $\mathbb{G}_a$ plus the free group on $[\infty]$ (which can be any $\mathbb{F}$ point of X) and the group $\mathrm{Pic}^0(X)$. Moreover, there is a group scheme J so that $\mathrm{Pic}^0(X) = J(\mathbb{F})$. Thus, one way to determine the order of the group $\mathrm{Pic}^0(X)$ is to determine the fixed points for the action of Frobenius on this group scheme. Now, let ℓ be a prime that is invertible the field $\mathbb{F}$. On can show that the points of order ℓ in $J(E)$ for a large enough field extension E of $\mathbb{F}$ form a vector space of rank $2g$ over $\mathbb{Z}/\ell\mathbb{Z}$ (here g is the genus of the curve X). Moreover, there is a polynomial $P(T)$ of degree $2g$ with *integer coefficients* that is satisfied by the automorphism of this vector space that is given by the Frobenius endomorphism; the important point is that this polynomial is *independent* of ℓ. Another important fact is that this polynomial has roots that are complex numbers of absolute value $q^{1/2}$. Finally, given $P(T)$ one can determine the number of elements in $J(E)$ for any finite extension of $\mathbb{F}$. These results were proved by Weil and were generalised to other varieties in the form of the "Weil conjectures" which were proved by Grothendieck, Deligne and others.

This approach was used by Schoof to calculate the order of $\mathrm{Pic}^0(T)$ in the case T is an elliptic curve (or a hyperelliptic curve of genus 1). In this case $P(T)$ is a quadratic polynomial of the form $T^2 + aT + q$; moreover, $J = T$ in this case. One can write polynomials $f_\ell(x)$ that are satisfied by the x co-ordinates of points of order l. Thus we can use the action of the Frobenius on this polynomial to determine a modulo ℓ for a number of primes ℓ. The additional inequality $|a| \leq q^{1/2}$, can then we used to determine a. One could attempt to generalise this to other hyperelliptic curves. One must write down the equations that define the ℓ-torsion in the Jacobian J. From the action of the Frobenius on this we can write down the coefficients of $P(T)$ modulo ℓ. The inequalities resulting from the knowledge of the absolute value of the complex roots can then be used to bound the number of ℓ for which this needs to be done in order to determine the coefficients uniquely.