Lecture 12 (March 6)

Let's first restate the result from last time. We were looking at the homomorphism $n_X\colon X \to X$, $x \mapsto nx$, and its kernel

$$X_n = \{\, x \in X \mid nx = 0 \,\},$$

which is the subgroup of n-torsion points on X.

Proposition 12.1. *Set $g = \dim X$ and $p = \operatorname{char}(k)$.*

(a) We have $\deg n_X = n^{2g}$.
(b) If $p \nmid n$, then n_X is separable and $X_n \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.
(c) If $p \mid n$, then n_X is not separable and there is an integer $r \in \{0, 1, \dots, g\}$ such that $X_{p^e} \cong (\mathbb{Z}/p^e\mathbb{Z})^r$.

Recall that a homomorphism $f\colon X \to Y$ between abelian varieties is called an *isogeny* if it is surjective with finite kernel (and therefore $\dim X = \dim Y$). We define the degree $\deg f$ as the degree of the field extension $f^*\colon k(Y) \to k(X)$. We say that f is a *separable isogeny* if the field extension is separable; this is always the case in characteristic zero, or when $\deg f$ is not a multiple of p. In that case, the number of elements in the subgroup $\ker f$ is equal to $\deg f$. If the field extension is not separable, we can let $L \subseteq k(X)$ be the subfield of all elements that are separable over $k(Y)$; the field extension $L \subseteq k(X)$ is purely inseparable. In general, the number of elements in $\ker f$ is only equal to the *separable degree* $\deg_s(f) = \big(L\colon k(Y)\big)$. Lastly, we need a basic fact from intersection theory: if $D_1, \dots, D_g$ are Cartier divisors on Y, then their pullbacks $f^*D_1, \dots, f^*D_g$ are Cartier divisors on X, and we have the equality of intersection numbers

$$(f^*D_1 \cdots f^*D_g)_X = \deg f \cdot (D_1 \cdots D_g)_Y.$$

Proof of the proposition. For (a), we pick an ample and symmetric divisor D; this means that $(-1)_X^* D \equiv D$. We showed last time that $n_X^* D \equiv n^2 D$. Now the formula from above gives

$$\deg n_X (D \cdots D)_X = \big(n_X^* D \cdots n_X^* D\big)_X = n^{2g} (D \cdots D)_X,$$

and so $\deg n_X = n^{2g}$. This part is the same as in the complex case. For (b), suppose that $p \nmid n$. The degree of n_X is then not divisible by p, and so n_X is separable, and the number of elements in $X_n = \ker(n_X)$ is therefore n^{2g}. From this, we see that X_n is a finite abelian group; the order of every element divides n; and for every divisor $m \mid n$, the number of elements whose order divides m is exactly m^{2g}. Looking at the classification of finite abelian groups, this is only possible if $X_n \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.

For (c), let's now assume that $p \mid n$. Let $T_{X,0}$ be the tangent space at the zero element, and Ω_0 the dual k-vector space. We showed in Lecture 8 that the differential

$$dn_X\colon T_{X,0} \to T_{X,0}$$

is multiplication by n, hence trivial if $p \mid n$. Because $\Omega^1_{X/k} \cong \Omega_0 \otimes_k \mathscr{O}_X$, it follows that $n_X^*\colon \Omega^1_{X/k} \to \Omega^1_{X/k}$ is trivial (as a morphism of sheaves). So if $f \in k(X)$ is a rational function, then f is regular on some open subset U, and so $df \in H^0(U, \Omega^1_{X/k})$. But then

$$0 = n_X^*(df) = d\big(n_X^* f\big),$$

and because we are in characteristic p (and k is algebraically closed), we must have $n_X^* f = g^p$ for some other rational function $g \in k(X)$. Therefore the field extension

$$n_X^*\colon k(X) \to k(X)$$

actually factors through the subfield $k(X)^p$, and so it is not separable. This means that X_n has fewer than n^{2g} elements.

Now consider $p_X \colon X \to X$. We sort of convinced ourselves in class that the (purely inseparable) field extension $k(X)^p \subseteq k(X)$ has degree at least p^g, because the transcendence degree of $k(X)$ is equal to $\dim X = g$. This means that the separable degree of $p_X^* \colon k(X) \to k(X)$ must be equal to p^r for some $0 \leq r \leq g$. Therefore X_p is a finite abelian group with p^r elements in which every element has order p; clearly $X_p \cong (\mathbb{Z}/p\mathbb{Z})^r$. Because X_n is divisible, it is easy to deduce by induction on $e \geq 1$ that $X_{p^e} \cong (\mathbb{Z}/p^e\mathbb{Z})^r$. □

Example 12.2. Elliptic curves over a field of characteristic p are a good example. By the general result above, the group X_p is either $\mathbb{Z}/p\mathbb{Z}$ or trivial. In the case when X_p is trivial, the elliptic curve is called *supersingular*.

We can always realize an elliptic curve as a nonsingular cubic curve in $\mathbb{P}^2$, defined by a cubic polynomial $f(x, y, z)$. If $p \neq 2, 3$, so that we can complete the square and the cube, we can put this polynomial into Weierstrass form

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

for constants $a, b \in k$; or into Legendre form

$$y^2 z = x(x - z)(x - \lambda z)$$

for a constant $\lambda \in k$. (In both cases, the polynomial on the right-hand side must not have any repeated roots; so for example $\lambda \neq 0, 1$.) Two such cubic curves are isomorphic (as abstract curves), if and only if there is an automorphism of $\mathbb{P}^2$ that takes one to the other, if and only if they have the same *j-invariant*; this is

$$j(A, B) = 1728 \frac{4A^3}{4A^3 + 27B^3}$$

for curves in Weierstrass form, and

$$j(\lambda) = 256 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}$$

for curves in Legendre form.

One can show that a nonsingular cubic curve is supersingular iff the coefficient of $(xyz)^{p-1}$ in the polynomial $f(x, y, z)^{p-1}$ vanishes. That allows us to give some concrete examples. (Note that actually computing the subgroup of p-torsion points by hand is very difficult: the geometric description of the group law is simple, but the formulas are not so simple.) For instance, consider the curve

$$y^2 = x^3 + 1.$$

Here $(y^2 z - x^3 - z^3)^{p-1}$ only contains terms of the form

$$(y^2 z)^a (x^3)^b (z^3)^c$$

with $a + b + c = p - 1$. To get $(xyz)^{p-1}$, we need $p - 1 = 2a$ and $a = 3b$, so $p = 6b + 1$. (And in that case, the coefficient is the product of two factorials that are not divisible by p.) So this curve is supersingular exactly when $p \equiv 1 \mod 6$.

How common are supersingular curves? Since the number of elements in X_p is equal to the separable degree, X is supersingular exactly when the field extension $p_X^* \colon k(X) \to k(X)$ is purely inseparable. Assume again that X is defined by a cubic polynomial $f(x, y, z)$. Define a new cubic polynomial $f_p(x, y, z)$ by the rule

$$f(x, y, z)^p = f_p(x^p, y^p, z^p);$$

in other words, all the coefficients of f get raised to the p-th power. We then have the Frobenius morphism

$$F \colon V(f) \to V(f_p), \quad F(x, y, z) = (x^p, y^p, z^p),$$

which is purely inseparable of degree p. By general theory, p_X purely inseparable of degree p^2 implies that $p_X = F^2$. In particular, the cubic curve defined by $f(x,y,z)$ must be isomorphic to the cubic curve defined by $f_{p^2}(x,y,z)$. For curves in Legendre form, for example, this means that

$$j(\lambda) = j(\lambda^{p^2}) = \big(j(\lambda)\big)^{p^2},$$

which is saying that $j(\lambda)$ lies in the subfield with p^2 elements. (Remember that k is algebraically closed.) This shows that there are rather few supersingular curves.

Quotients by finite groups. Our next goal is to construct $\operatorname{Pic}^0(X)$ as an abelian variety. The general idea is that $\phi_L \colon X \to \operatorname{Pic}^0(X)$ is surjective when L is ample, and so $\operatorname{Pic}^0(X)$ should be the quotient of X by the finite subgroup $K(L)$. Before we can do that, we have to review very quickly a few results about such quotients.

Let X be a variety, and let G be a finite group of automorphisms of X. The main technical assumption is that for all points $x \in X$, the orbit $Gx = \{\, gx \mid g \in G \,\}$ should be contained in some affine open subset of X. This is true for example when X is quasi-projective: take a projective completion, and remove a hyperplane section not containing any point of Gx.

Theorem 12.3. *Under these assumptions, there is a morphism $\pi \colon X \to Y$ to a variety Y, such that $Y = X/G$ as topological spaces, and such that the morphism $\mathscr{O}_Y \to \pi_* \mathscr{O}_X$ induces an isomorphism between $\mathscr{O}_Y$ and the subsheaf $(\pi_* \mathscr{O}_X)^G$ of G-invariant functions. The morphism π is finite, surjective, and separable; if G acts freely, then π is étale.*

We denote Y by the symbol X/G and call it the quotient of X by G. It has the following universal property: if $f \colon X \to Z$ is any morphis such that $f \circ g = f$ for all $g \in G$, then f factors uniquely through a morphism $h \colon Y \to Z$. The construction of the quotient is straightforward. The statement about orbits implies that we can cover X by affine open subsets that are invariant under the G-action. If $U = \operatorname{Spec} A$ is such an affine open, we define the quotient as the morphism $\operatorname{Spec} A \to \operatorname{Spec} A^G$, where $A^G \subseteq A$ is the subring of G-invariant functions. One shows that this has the universal property; for that reason, the individual quotients U/G then glue together into a variety Y with the desired properties.

We can also describe coherent sheaves on $Y = X/G$. Suppose that $\mathscr{F}$ is a coherent $\mathscr{O}_Y$-module. The pullback $\pi \mathscr{F}$ is a coherent $\mathscr{O}_X$-module, and for every $g \in G$, we have $\pi \circ g = \pi$, and therefore $g^* \pi^* \mathscr{F} \cong \pi^* \mathscr{F}$. We say that a coherent $\mathscr{O}_X$-module $\mathscr{G}$ is *G-equivariant* if we have a collection of isomorphisms

$$\phi_g \colon g^* \mathscr{G} \to \mathscr{G}$$

that are compatible with composition, in the sense that the diagram

$$\begin{array}{ccc} h^* g^* \mathscr{G} & \xrightarrow{h^* \phi_g} & h^* \mathscr{G} \\ \| & & \downarrow{\scriptstyle \phi_h} \\ (gh)^* \mathscr{G} & \xrightarrow{\phi_{gh}} & \mathscr{G} \end{array}$$

is commutative. In that case, G acts on the direct image sheaf $\pi_* \mathscr{G}$, and the subsheaf $(\pi_* \mathscr{G})^G$ of G-invariants is a coherent $\mathscr{O}_Y$-module.

Proposition 12.4. *Suppose that G acts freely on X. The functors $\mathscr{F} \mapsto \pi^* \mathscr{F}$ and $\mathscr{G} \mapsto (\pi_* \mathscr{G})^G$ define an equivalence between the category of coherent $\mathscr{O}_Y$-modules and the category of G-equivariant coherent $\mathscr{O}_X$-modules.*

For the study of abelian varieties, line bundles are of particular interest. When the group G is abelian, these are closely related to characters. For a finite abelian group G, we are going to write

$$\hat{G} = \mathrm{Hom}(G, k^\times)$$

for the group of characters of G with values in the field k. Suppose that X is complete and that G acts freely on X. Let L be a line bundle on Y whose pullback $\pi^* L$ is trivial. We get a G-equivariant structure on $\mathscr{O}_X$, namely a collection of isomorphisms $\phi_g \colon \mathscr{O}_X \to \mathscr{O}_X$, such that $\phi_{gh} = \phi_h \circ h^* \phi_g$. Because X is complete, each ϕ_g is multiplication by a nonzero constant $\alpha(g) \in k^\times$, and the compatibility condition means exactly that $\alpha \colon G \to k^\times$ is a character. Conversely, given such a character, we can recover the line bundle L as the subsheaf of G-invariants in $\pi_* \mathscr{O}_X$ (with the G-action depending on the character, of course); concretely,

$$L \cong \bigl\{ f \in \pi_* \mathscr{O}_X \bigm| g(f) = \alpha(g) \cdot f \text{ for all } g \in G \bigr\}.$$

These considerations prove the following proposition.

Proposition 12.5. *Suppose that G acts freely on a complete variety X. For every character $\alpha \in \hat{G}$, consider the subsheaf*

$$L_\alpha = \bigl\{ f \in \pi_* \mathscr{O}_X \bigm| g(f) = \alpha(g) \cdot f \textit{ for all } g \in G \bigr\}.$$

Then L_α is a line bundle on X/G, and we have $L_\alpha \otimes L_\beta \cong L_{\alpha+\beta}$. Moreover,

$$\hat{G} \cong \ker\bigl(\pi^* \colon \mathrm{Pic}(Y) \to \mathrm{Pic}(X)\bigr)$$

are isomorphic groups.

Specializing further, suppose that G is a finite abelian group, whose order is not divisible by the characteristic $p = \mathrm{char}(k)$. In that case, every finite-dimensional representation of G on a k-vector space is a direct sum of characters. Indeed, every finite-dimensional representation is completely reducible, because for any given G-invariant subspace, we can write down a G-invariant complement (by an explicit formula whose denominator $|G|$ is invertible in the field k). Furthermore, every irreducible representation is 1-dimensional (because G is abelian), hence is given by a character. For exactly the same reason, the G-action on $\pi_* \mathscr{O}_X$ decomposes into a direct sum of line bundles, and so we get a decomposition

$$\pi_* \mathscr{O}_X \cong \bigoplus_{\alpha \in \hat{G}} L_\alpha.$$

Recall here that $\hat{G}$ and G have the same number of elements; because $\pi \colon X \to Y$ is separable, this number is just the degree of π. Because of the projection formula

$$\pi_* \pi^* \mathscr{F} \cong \mathscr{F} \otimes_{\mathscr{O}_Y} \pi_* \mathscr{O}_X,$$

it then follows that $\mathscr{F}$ is isomorphic to a direct summand in $\pi_* \pi^* \mathscr{F}$.

We can apply the results above to the case of abelian varieties.

Corollary 12.6. *Let X be an abelian variety. There is a one-to-one correspondence between finite subgroups $K \subseteq X$ and (isomorphism classes of) separable isogenies $f \colon X \to Y$. The correspondence sends $f \colon X \to Y$ to the finite subgroup* $\ker f$*; and it sends K to the quotient $\pi \colon X \to Y$.*

Here two isogenies $f_1 \colon X \to Y_1$ and $f_2 \colon X \to Y_2$ are isomorphic if there is an isomorphism $g \colon Y_1 \to Y_2$ such that $g \circ f_1 = f_2$.

Proof. A finite subgroup $K \subseteq X$ acts freely on X by translations, and so the quotient X/K is a nonsingular complete variety, and $\pi \colon X \to X/K$ is finite, surjective, and separable. Because K is a subgroup, X/K has the structure of a group. It is in fact an abelian variety. Indeed, the product $(X/K) \times (X/K)$ is isomorphic to $(X \times X)/(K \times K)$, and by the universal property of quotients, the group action $m\colon X \times X \to X$ descends to $n\colon (X/K) \times (X/K) \to X/K$:

$$\begin{tikzcd} X \times X \arrow[r, "m"] \arrow[d, "\pi \times \pi"] & X \arrow[d, "\pi"] \\ (X/K) \times (X/K) \arrow[r, "n"] & X/K \end{tikzcd}$$

It follows that $\pi\colon X \to X/K$ is a separable isogeny, and clearly $K = \ker \pi$.

Conversely, given a separable isogeny $f\colon X \to Y$, we let $K = \ker f$, and define $\pi\colon X \to X/K$ as the quotient. By the universal property of quotients, we get the following commutative diagram:

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\pi"] & Y \\ X/K \arrow[ur, bend right, "g"'] & \end{tikzcd}$$

Both X/K and Y are nonsingular, and g is finite and bijective, and therefore an isomorphism. This proves that the two operations are inverse to each other. $\square$

This result also shows that there is a sort of duality between X and line bundles on X, in the following sense. Consider a separable isogeny $f\colon X \to Y$, of degree prime to $p = \operatorname{char}(k)$. By the corollary, we have $Y \cong X/K$, where $K = \ker f$. Now Proposition 12.5 shows that

$$\hat{K} = \operatorname{Hom}(K, k^\times) \cong \ker\bigl(f^*\colon \operatorname{Pic}(Y) \to \operatorname{Pic}(X)\bigr).$$

So the kernel of $f\colon X \to Y$ and the kernel of $f^*\colon \operatorname{Pic}(Y) \to \operatorname{Pic}(X)$ have the same number of elements, and in fact, are "dual" to each other in the sense that one group is the group of characters on the other group.