Variétés abéliennes, D.E.A., 1999.

Bas Edixhoven, Université de Rennes I.

March 29, 1999

1 January 8, 1999

1.1 Introduction.

An abelian variety over a field k is a proper reduced connected k-scheme X that is equipped with a group law, i.e., with a morphism, called multiplication, $m\colon X \times_k X \to X$ that satisfies the usual axioms for groups. Such varieties play an important role in arithmetic. Let me mention just three examples: Weil's results on the zeta functions of curves over finite fields in the 1940's (see [MumAV, §21]), Faltings's proof of Mordell's conjecture and generalizations (see [CoSiAG] and [EdEvDA]), and Wiles's proof of Fermat's Last Theorem (which is a by-product of his results on the Shimura-Taniyama conjecture, see for example [CoSiSt]).

The aim of this course is to give a proof of Weil's result (or at least to give a sketch), and to give a proof of a result of Tate on morphisms between abelian varieties over finite fields (see [MumAV, Appendix I]). On the way, we will state the conjecture of Birch and Swinnerton-Dyer for abelian varieties over number fields, in its imprecise form (see [SiAE, VII, §10] for the case of elliptic curves). Of course, it will be impossible to give many details, so I will try to give references as much as possible. By the way, all the books in the bibliography are great for reading at home.

As far as I can foresee at this moment, we will first study elliptic curves, i.e., abelian varieties of dimension one, before going into higher dimensions. But we have a choice to make: do we want to stick to elliptic curves over fields, or even algebraically closed fields, in which case we could stick to the terminology of algebraic varieties, or do we want to make use of general scheme theory. As this is a course at the DEA level, my choice is clear: we will use schemes right from the start. Of course, this gives rise to more technicalities, but my feeling is that the problems with those are mostly psychological. Today, I want to talk about viewing schemes as functors, and about group schemes, giving examples that are very explicit. After that, our first goal is to develop the basic theory of elliptic curves (over arbitrary schemes) as in Chapter 2 of [KaMaAM]. But that means that we have to discuss cohomology of sheaves, differential forms, and the Riemann-Roch theorem for curves.

1.2 Scheme valued points.

1.2.1 Definition. Let S be a scheme. A scheme over S, also called S-scheme, is a morphism of schemes $f\colon X \to S$. In the case where S is affine, say $S = \mathrm{Spec}(A)$, we will also write A-scheme instead of S-scheme. A morphism of S-schemes from $f\colon X \to S$ to

$g\colon Y \to S$ is a morphism of schemes $h\colon X \to Y$ such that $f = g \circ h$. This gives us the category (Sch/S) of S-schemes.

1.2.2 Remark. This construction can be carried out in every category. One can also define what is an object under a given object. For example: the category of A-algebras. By abuse of language we will often speak of the S-scheme X, without mentioning the morphism f.

1.2.3 Exercise. Show that every scheme is, in a unique way, a $\mathbb{Z}$-scheme; show that (Sch) is isomorphic to $(\mathrm{Sch}/\mathbb{Z})$. Show that $(\mathrm{Sch}/\mathbb{Q})$ is isomorphic to the full subcategory of (Sch) whose objects are those schemes X such that for every non-zero integer n the morphism of sheaves $\mathcal{O}_X \to \mathcal{O}_X$, $f \mapsto nf$, is an isomorphism. Let X be a scheme; give a bijection between the set of morphisms from X to $\mathrm{Spec}(\mathbb{Z}[\sqrt{2}])$ and the set $\{f \in \mathcal{O}_X(X) \mid f^2 = 2\}$. Give an example of a scheme that does not admit a morphism to $\mathrm{Spec}(\mathbb{Z}[\sqrt{2}])$.

1.2.4 Definition. Consider an S-scheme X. Let T be an S-scheme. A point of X with values in T is a morphism of S-schemes $P\colon T \to X$. The set of these points will be denoted $X(T)$. A morphism $T' \to T$ of S-schemes induces a map $X(T) \to X(T')$. This gives a contravariant functor $(\mathrm{Sch}/S) \to (\mathrm{Set})$, that we will denote by X and that is nothing else than the functor $\mathrm{Hom}(*, X)$. A contravariant functor $f\colon (\mathrm{Sch}/S) \to (\mathrm{Set})$ is called representable if it is isomorphic to a functor of the form $T \mapsto X(T)$ with X an S-scheme.

1.2.5 Exercise. Take $S := \mathrm{Spec}(\mathbb{Z})$. Let $\mathbb{A}^1_{\mathbb{Z}}$ be the affine line over $\mathbb{Z}$: $\mathbb{A}^1_{\mathbb{Z}} := \mathrm{Spec}(\mathbb{Z}[x])$. Give an isomorphism between the functor $\mathbb{A}^1_{\mathbb{Z}}$ and the functor $\Gamma\colon X \mapsto \mathcal{O}_X(X)$. Find a scheme representing the functor (multiplicative group) $\mathbb{G}_{\mathrm{m}}\colon X \mapsto \mathcal{O}_X(X)^*$. Give a contravariant functor $F\colon (\mathrm{Sch}) \to (\mathrm{Set})$ that is not representable.

Let k be a field and X a k-scheme. Let $k \to K$ be an extension of fields. Show that giving a point of X with values in K is equivalent to giving a point x (of the underlying set) of X and a morphism of k-algebras $k(x) \to K$, where $k(x)$ is the residue field $\mathcal{O}_{X,x}/m_x$ of x. Special case: $K = k$; the set $X(k)$, that one can identify with $\{x \in X \mid k(x) = k\}$, is called the set of rational points of X.

Let k be a field and X a k-scheme of finite type. Let x be in X. Show that x is closed if and only if $k(x)$ is a finite extension of k. Show that the set of closed points of X is dense. Give an example of a k-scheme in which the set of closed points is not dense. Also give an example of a field k and a k-scheme X, of finite type, in which the set of rational points is not dense.

1.3 Construction of $\mathbb{P}^n_A$.

Let A be a ring and $n \geq 0$. We consider the A-algebra $B := A[x_0, \ldots, x_n]$, graded by the total degree: $B = \oplus_{d\geq 0} B_d$, with B_d the free A-module with basis the monomials of degree d. For f a homogeneous element of some degree $d > 0$, i.e., f in B_d, we write $B_{f,0}$ for the subring of degree zero elements in the localization $B_f = B[f^{-1}]$ (B_f has a unique grading such that $\deg(b/f^m) = \deg(b) - m\deg(f)$ for b homogeneous and $b/f^m \neq 0$). (More explicitly, for m in $\mathbb{Z}$, $B_{f,m} = \cup_{n\geq 0} f^{-n}\phi B_{m+nd}$, with $\phi\colon B \to B_f$ the localization morphism.) For example, $B_{x_0,0}$ is the A-algebra $A[x_1/x_0, \ldots, x_n/x_0]$ of polynomials in n variables. For such an f, we put $D_+(f) := \mathrm{Spec}(B_{f,0})$; note that it is an affine scheme.

Let now f and g be two homogeneous elements of B of degree > 0. Put $h := fg$. Then we have a natural morphism $B_f \to B_h$, compatible with graduations, hence also a morphism of A-algebras $B_{f,0} \to B_{h,0}$. Put $z := g^{\deg(f)}/f^{\deg(g)}$; this is an element of $B_{f,0}$. The image of z in $B_{h,0}$ is invertible, hence we have a morphism $(B_{f,0})_z \to B_{h,0}$. This morphism is an isomorphism, because $(B_{f,0})_z = ((B_f)_z)_0 = B_{h,0}$, where the first equality results from the more general statement: let z be an element of degree zero in a graded ring R, then $R_{z,0} = (R_0)_z$. This shows that $D_+(h)$ is a principal open of $D_+(f)$, and hence also of $D_+(g)$. We can now glue $D_+(f)$ and $D_+(g)$ along $D_+(fg)$. We can even glue all the $D_+(f)$, for f homogeneous of degree > 0 (do exercise 2.12 of [HarAG, II]). The A-scheme obtained by this construction is called the projective space of dimension n over A, and is denoted $\mathbb{P}^n_A$. This scheme is by construction the union of the open affine subschemes $D_+(f)$, and the intersection of $D_+(f)$ and $D_+(g)$ is $D_+(fg)$. In fact, $\mathbb{P}^n_A$ is covered by the open affines $D_+(x_i)$, which are all isomorphic to $\mathbb{A}^n_A$, the affine space of dimension n over A. See [HarAG, II.2] for another construction of $\mathbb{P}^n_A$.

1.3.1 Remark. The construction of $\mathbb{P}^n_A$ that we have just seen generalises trivially to the case of an arbitrary A-algebra S that is graded in positive degrees; the scheme thus obtained is called the projective spectrum of S and is denoted $\mathrm{Proj}(S)$. The importance of projective spaces is that we can use them to “compactify”. The following proposition is the analog of the theorem of Liouville that says that every holomorphic function on a complex projective space is constant.

1.3.2 Exercise. Show that the A-scheme $\mathbb{P}^0_A$ is equal to $\mathrm{Spec}(A)$. Give, for k a field and $n \geq 0$, a bijection between $\mathbb{P}^n_{\mathbb{Z}}(k)$ and the set of one-dimensional subspaces of the k-vector space k^{n+1}.

1.3.3 Proposition. *Let A be a ring and $n \geq 0$. Then $\mathcal{O}_{\mathbb{P}^n_A}(\mathbb{P}^n_A) = A$.*

Proof. Put $U_i := D_+(x_i)$ and $U_{i,j} := U_i \cap U_j = D_+(x_i x_j)$. Since $\mathcal{O}_{\mathbb{P}^n_A}$ is a sheaf, we have the exact sequence:

$$0 \to \mathcal{O}_{\mathbb{P}^n_A}(\mathbb{P}^n_A) \to \prod_i \mathcal{O}_{\mathbb{P}^n_A}(U_i) \to \prod_{i,j} \mathcal{O}_{\mathbb{P}^n_A}(U_{i,j}), \tag{1.3.4}$$

where s in $\mathcal{O}_{\mathbb{P}^n_A}(\mathbb{P}^n_A)$ is mapped to $i \mapsto s|_{U_i}$, and s in $\prod_i \mathcal{O}_{\mathbb{P}^n_A}(U_i)$ to $(i,j) \mapsto s(i)|_{U_{i,j}} - s(j)|_{U_{i,j}}$. The $D_+(f)$ are affine, hence $\mathcal{O}_{\mathbb{P}^n_A}(D_+(f)) = B_{f,0}$, in the notation of construction 1.3. Let s be in the kernel of the last morphism. Then every $s(i)$ can be written in the form $f_i/x_i^{d_i}$, with f_i homogeneous of degree d_i. After multiplying every f_i by a power of x_i, we can suppose that all the d_i are the same, say equal to d. The condition that s be in the kernel means that for all (i,j) we have the relation $f_i/x_i^d - f_j/x_j^d = 0$ in $B_{x_i x_j,0}$, which is equivalent to $f_i x_j^d = f_j x_i^d$ in B_{2d}. The A-module B_{2d} is free as A-module, with basis the monomials of degree $2d$ in $x_0, \ldots, x_n$. Take i and j distinct (the case $n = 0$ is left as an exercise). The only monomial that can occur both at the left and the right is $x_i^d x_j^d$. This implies that there exists an a in A such that for all i we have $f_i = a x_i^d$. It follows that $s(i) = a$ for all i. Conversely, it is clear that all such s are in the kernel. $\square$

1.4 The sheaves $\mathcal{O}(r)$ on $\mathbb{P}^n_A$.

Let A be a ring, $n \geq 0$ and r in $\mathbb{Z}$. For f in $B := A[x_0, \ldots, x_n]$ homogeneous of degree> 0 we have the quasi-coherent $\mathcal{O}_{D_+(f)}$-module $\widetilde{B_{f,r}}$, where $B_{f,r}$ is the homogenous part of degree r of B_f. These sheaves glue together in a natural way on $\mathbb{P}^n_A$: for $h = fg$ with g in B homogeneous of degree > 0 we have $B_h = (B_f)_z$, with $z = g^{\deg(f)}/f^{\deg(g)}$ as in (1.3), which shows that $B_{h,r}$ is the localization with respect to z of the $B_{f,0}$-module $B_{f,r}$. The sheaves $\mathcal{O}(r)$ are locally free $\mathcal{O}_{\mathbb{P}^n_A}$-modules of rank one: the restriction of $\mathcal{O}(r)$ to $D_+(x_i)$ is free with base x_i^r.

1.4.1 Exercise. Show that $\mathcal{O}(r_1) \otimes_{\mathcal{O}_{\mathbb{P}^n_A}} \mathcal{O}(r_2)$ is isomorphic to $\mathcal{O}(r_1 + r_2)$. Compute, as in the proof of Proposition 1.3.3, bases for the free A-modules $\mathcal{O}(r)(\mathbb{P}^n_A)$. Conclude that, for $n > 0$ and $A \neq 0$, the classes in $\mathrm{Pic}(\mathbb{P}^n_A)$ of the $\mathcal{O}(r)$ are all distinct. Find Cartier divisors D_r on $\mathbb{P}^n_A$ such that, in the notation of [HarAG, II, Prop. 6.13], $\mathcal{L}(D_r)$ is isormorphic to $\mathcal{O}(r)$ for all r.

1.5 Morphisms to $\mathbb{P}^n_A$.

Let $f\colon X \to Y$ be a morphism of ringed spaces. Let $\mathcal{L}$ be an invertible $\mathcal{O}_Y$-module; then the $\mathcal{O}_X$-module $f^*\mathcal{L}$ is invertible. Let $\mathcal{M}$ be an $\mathcal{O}_Y$-module. Interpreting $\mathcal{M}(Y)$ as

$\mathrm{Hom}_{\mathcal{O}_Y}(\mathcal{O}_Y, \mathcal{M})$ (morphisms of $\mathcal{O}_Y$-modules) one obtains a map $f^*\colon \mathcal{M}(Y) \to f^*\mathcal{M}(X)$, that we will denote $s \mapsto f^*(s)$. One has $f^*(s)_x = 1 \otimes s_{f(x)}$ in $(f^*\mathcal{M})_x = \mathcal{O}_{X,x} \otimes_{\mathcal{O}_{Y,f(x)}} \mathcal{M}_{f(x)}$.

Let X be a ringed space and $\mathcal{L}$ an invertible $\mathcal{O}_X$-module. For s in $\mathcal{L}(X)$ let $D(s)$ be the subset of x in X such that the germ s_x of s in x generates the fibre $\mathcal{L}_x$ of $\mathcal{L}$ in x: $\mathcal{L}_x = \mathcal{O}_{X,x} s_x$. This is an open subset of X. Let $\mathcal{M}$ be an $\mathcal{O}_X$-module and let $s_i \in \mathcal{M}(X)$, $i \in I$, be a set of global sections. We say that the s_i generate $\mathcal{M}$ if the morphism of $\mathcal{O}_X$-modules $\oplus_{i \in I} \mathcal{O}_X \to \mathcal{M}$ given by the s_i is surjective.

1.5.1 Exercise. Let A be a ring and $n, r \geq 0$. Let f in $A[x_0, \ldots, x_n]$ be homogeneous of degree r. We consider f as a global section of $\mathcal{O}(r)$ on $\mathbb{P}^n_A$. Show that $D_+(f)$ and $D(f)$ are equal.

Let A be a ring and $r \geq 0$ an integer. Let X be an A-scheme. We want to give a description of $\mathbb{P}^n_A(X)$ which is close to the classical definition of $\mathbb{P}^n(k)$ for k a field. We will do that in two steps.

First step (see also [HarAG, II, Thm. 7.1]). Let $\phi\colon X \to \mathbb{P}^n_A$ be a morphism of A-schemes. This gives us the invertible $\mathcal{O}_X$-module $\mathcal{L} := \phi^*\mathcal{O}(1)$ and sections $s_i := \phi^* x_i$, $0 \leq i \leq n$ of $\mathcal{L}$. Since the x_i generate $\mathcal{O}(1)$, the s_i generate $\mathcal{L}$. We have $\phi^{-1}D_+(x_i) = D(s_i)$. We will now see that one can reconstruct ϕ from $\mathcal{L}$ and the s_i.

So let $\mathcal{L}$ be an invertible $\mathcal{O}_X$-module, and $s_0, \ldots, s_n$ global sections generating $\mathcal{L}$. For $0 \leq i \leq n$ we define a morphism ϕ_i from $D(s_i)$ to $D_+(x_i)$. Recall that $D_+(x_i)$ is the spectrum of $A[\{x_j/x_i \mid j \neq i\}]$, hence to give ϕ_i is equivalent to giving n elements $f_{i,j}$, $i \neq j$, of $\mathcal{O}_X(D(s_i))$. For each pair (i,j) there exists a unique $f_{i,j}$ in $\mathcal{O}_X(D(s_i))$ such that $s_j|_{D(s_i)} = f_{i,j} s_i|_{D(s_i)}$; we take these $f_{i,j}$ to define ϕ_i. (It is reasonable and useful to introduce the notation $f_{i,j} = s_j/s_i$.) One verifies easily that the restrictions of ϕ_i and ϕ_j to $D(s_i) \cap D(s_j) = \phi^{-1}D_+(x_i x_j)$ coincide. One also sees that if $\mathcal{L}$ and the s_i come from a ϕ as above, they give us back ϕ.

1.5.2 Exercise. Let $\mathcal{L}$ and $\mathcal{L}'$ be invertible $\mathcal{O}_X$-modules, generated by global sections $s_0, \ldots, s_n$ and $s'_0, \ldots, s'_n$, respectively. Let ϕ and ϕ' be the two morphisms from X to $\mathbb{P}^n_A$ obtained from the construction above. Show that ϕ and ϕ' are equal if and only if there exists an isomorphism $\alpha\colon \mathcal{L} \to \mathcal{L}'$ such that for all i one has $\alpha(s_i) = s'_i$.

Step two. Let $\mathcal{L}$ be an invertible $\mathcal{O}_X$-module, generated by global sections $s_0, \ldots, s_n$. On the one hand, this gives us an element ϕ of $\mathbb{P}^n_A(X)$, and, on the other hand, a surjective morphism $f\colon \mathcal{O}_X^{n+1} \to \mathcal{L}$ of $\mathcal{O}_X$-modules. Let $\mathcal{L}'$ also be an invertible $\mathcal{O}_X$-module, generated by global sections $s'_0, \ldots, s'_n$, giving ϕ' in $\mathbb{P}^n_A(X)$ and $f'\colon \mathcal{O}_X^{n+1} \to \mathcal{L}'$. One sees that f and

f', viewed as quotients of $\mathcal{O}_X^{n+1}$, are isomorphic if and only if $\phi = \phi'$. This implies that we have constructed an isomorphism between the functor $\mathbb{P}^n_A\colon (\mathrm{Sch}/A) \to (\mathrm{Set})$ and the Grassmannian functor $\mathrm{Grass}(n+1,1)$ that sends X to the set of locally free quotients of rank one of $\mathcal{O}_X^{n+1}$.

1.6 Yoneda's lemma.

See also [GrDiEGA, 1] (the Springer edition). Let $\mathcal{C}$ be a category. For every object X of $\mathcal{C}$ we have the contravariant functor $h_X := \mathrm{Hom}(*, X)$ from $\mathcal{C}$ to (Set). Every morphism $f\colon X \to Y$ in $\mathcal{C}$ induces, in a covariant way, a morphism of functors $h(f)\colon h_X \to h_Y$. Hence we can consider h as a covariant functor from $\mathcal{C}$ to the category $\widehat{\mathcal{C}} := \mathrm{Hom}(\mathcal{C}^o, (\mathrm{Set}))$ whose objects are the contravariant functors from $\mathcal{C}$ to (Set), and whose morphisms are morphisms of functors. Yoneda's lemma says that h is fully faithful: all the maps $\mathrm{Hom}_{\mathcal{C}}(X,Y) \to \mathrm{Hom}_{\widehat{\mathcal{C}}}(h_X, h_Y)$ are isomorphisms. In fact, the statement is even a bit more general; one has natural bijections:

$$F(X) \xrightarrow{\sim} \mathrm{Hom}_{\widehat{\mathcal{C}}}(h_X, F). \tag{1.6.1}$$

1.6.2 Exercise. Construct morphisms (of bifunctors) $\alpha_{X,F}$ and $\beta_{X,F}$, inverses of each other, establishing the bijections (1.6.1).

Yoneda's lemma shows that to construct a morphism from X to Y, it suffices to construct maps, functorially in Z, of $X(Z)$ to $Y(Z)$. Of course, this is not at all a deep result (take $Z := X$), but the idea to view objects of $\mathcal{C}$ as objects of $\widehat{\mathcal{C}}$ is very useful. The essential image of h, i.e., the F that are isomorphic to some h_X, is the collection of representable functors. Many problems in algebraic geometry are related to the representability of certain functors. For example, jacobian varieties of curves represent "relative" Picard functors. From what we have seen, it follows that $\mathbb{A}^1_{\mathbb{Z}}$ represents the functor $X \mapsto \mathcal{O}_X(X)$, that $\mathbb{G}_{\mathrm{m}\,\mathbb{Z}}$ represents $X \mapsto \mathcal{O}_X(X)^*$, and that $\mathbb{P}^n_{\mathbb{Z}}$ represents the functor that associates to X the set of quotients of $\mathcal{O}_X^{n+1}$ that are locally free of rank one.

1.7 Fibered products, base change

See also [GrDiEGA, 1] (Springer edition). Let us consider the following diagram in a category $\mathcal{C}$: we have objects X, Y and S, and morphisms $f\colon X \to S$ and $g\colon Y \to S$. A fibered product of this diagram is then a triple (Z, f', g'), with Z in $\mathcal{C}$, $f'\colon Z \to Y$ and $g'\colon Z \to X$, such that $f \circ g' = g \circ f'$ and which is universal for this property: for every such triple (Z', f'', g'') there exists a unique $h\colon Z' \to Z$ such that $f'' = f' \circ h$ and

$g'' = g' \circ h$. From this definiton it follows immediately that (Z, f', g') is defined up to unique isomorphism, so that we can speak of "the fibered product", denoted $X \times_S Y$; f' and g' are called the projections on the second and first factor, respectively. Fibered products do not always exists (exercise: give an example where it does not exist). In the category of sets it exists always: it is the subset of $X \times Y$ consisting of the (x, y) with $f(x) = g(y)$. This explains the terminology: the fibre of Z over an element s of S is the product $X_s \times Y_s$ of the fibers of X and Y over s.

1.7.1 Exercise. Show that in the category (Top) of topological spaces fibered products always exist. Convince yourself that in the category of differentiable manifolds the fibered product does not always exist. Show that the fibered product is associative: $(X \times_S Y) \times_S Z$ is canonically isomorphic to $X \times_S (Y \times_S Z)$. Let $\mathcal{C}$ be a category, and $\widehat{\mathcal{C}}$ as in Section 1.6. Show that in $\widehat{\mathcal{C}}$ all fibered products do exist, and that one has the formula $(F \times_G H)(X) = F(X) \times_{G(X)} H(X)$.

Of course, there is also the dual notion of fibered product; it is the notion of amalgamated sum. For example, it exists in the category of commutative A-algebras: it is the tensor product.

A diagram:

(1.7.2)
$$\begin{array}{ccc} Z & \xrightarrow{f'} & Y \\ g' \downarrow & & g \downarrow \\ X & \xrightarrow{f} & S \end{array}$$

is called cartesian if (Z, f', g') is a fibered product of the rest of the diagram.

1.7.3 Exercise. Show that the diagram 1.7.2 is cartesian if and only if its image in $\widehat{\mathcal{C}}$ is. Consider the diagram:

$$\begin{array}{ccccc} A & \to & B & \to & C \\ \downarrow & & \downarrow & \square & \downarrow \\ D & \to & E & \to & F \end{array}$$

The square indicates that the square with corners B, C, E, and F is cartesian. Show that the square with corners A, B, D, and E is cartesian if and only if this is so for the square with corners A, C, D, and F. This fact can also be expressed in the formula: $D \times_E (E \times_F C) = D \times_F C$.

In (Sch) all fibered products exist, see [HarAG, II, Thm. 3.3] for a proof. That proof proceeds as follows. Suppose that we want to construct a fibered product of $f \colon X \to S$

and $g\colon Y \to S$. If all three are affine, say $S = \mathrm{Spec}(A)$, $X = \mathrm{Spec}(B)$ and $Y = \mathrm{Spec}(C)$, one shows that $\mathrm{Spec}(B \otimes_A C)$, with its natural morphisms to X and Y, has the required universal property (use that $\mathrm{Spec}(*)$ is the right adjoint of Γ; one even sees that $\mathrm{Spec}(B \otimes_A C)$ is a fibered product in the category of locally ringed spaces). Next one remarks that, if one knows how to construct a fibered product locally on S, one can do it globally, because the universal property gives glueing data for the local fibered products. So one can suppose that S is affine, say $\mathrm{Spec}(A)$. Arguments of the same type reduce the construction of a fibered product to the case where X and Y are affine, too. It is useful to know that if $U = \mathrm{Spec}(A)$, $V = \mathrm{Spec}(B)$ and $W = \mathrm{Spec}(C)$ are open affines in S, X and Y such that fV and gW are contained in U, then $V \times_U W = \mathrm{Spec}(B \otimes_A C)$ is an open affine of $X \times_S Y$. If U', V' and W' have the same property, then $V \times_U W \cap V' \times_{U'} W'$ is equal to $(V \cap V') \times_{U \cap U'} (W \cap W')$. The $\mathrm{Spec}(B \otimes_A C)$ cover $X \times_S Y$. It is not true in general that the underlying set of $X \times_S Y$ is the fibered product of the underlying sets of X and Y over that of S (see the exercise 1.7.5).

1.7.4 Definition. Let $f\colon X \to Y$ be a morphism of schemes. For y in Y we define the fibre of f at y, which is a $k(y)$-scheme, to be $X_y := \mathrm{Spec}(k(y)) \times_Y X$. For $Y' \to Y$ a morphism of schemes, put $X' := Y' \times_Y X$ and let $f'\colon X' \to Y'$ be the canonical morphism; we call f' the morphism obtained from f by the base change $Y' \to Y$. In the same style: let $f\colon X \to Y$ be a morphism of S-schemes, and S' an S-scheme; then the base change $S' \to S$ gives us a morphism $f'\colon X' \to Y'$, also denoted $f_{S'}\colon X_{S'} \to Y_{S'}$.

In the next exercise we will see that the underlying topological space of X_y is the preimage under f of y, with the induced topology.

1.7.5 Exercise. Do exercises 3.9 and 3.10 of [HarAG, II]. Let $A \to A'$ be a morphism of rings; show that the base change $\mathrm{Spec}(A') \to \mathrm{Spec}(A)$, applied to $\mathbb{P}^n_A \to \mathrm{Spec}(A)$, gives $\mathbb{P}^n_{A'} \to \mathrm{Spec}(A')$. This allows us to define, for S an arbirary scheme and $n \geq 0$, the projective space of dimension n over S as $\mathbb{P}^n_S := S \times_{\mathrm{Spec}(\mathbb{Z})} \mathbb{P}^n_{\mathbb{Z}}$. Let $f\colon X \to Y$ be a morphism of S-schemes, and S' an S-scheme; show that if f is a closed immersion given by a quasi-coherent sheaf of ideals $\mathcal{I}$ of $\mathcal{O}_Y$, then f' is the closed immersion defined by the sheaf of ideals $\mathcal{I}'$ of $\mathcal{O}_{Y'}$ which is the image of $g^*\mathcal{I} \to \mathcal{O}_{Y'}$, where g is the canonical morphism from Y' to Y.

1.8 Group schemes.

The objects that we want to study in this course, abelian varieties, are equipped with a group law. The easiest way to define what such a group law should be is to use the functor of points.

1.8.1 Definition. Let S be a scheme. A group scheme over S is an S-scheme G with a group law on $G(T)$ for every S-scheme T, functorially in T. This last condition means that, for every morphism of S-schemes $T' \to T$, the map $G(T) \to G(T')$ is a morphism of groups. Equivalently, and in more fancy terms, this means that a group law on an S-scheme G is the same as a factorization of the functor $h_G\colon (\mathrm{Sch}/S) \to (\mathrm{Set})$ via the forget functor $(\mathrm{Grp}) \to (\mathrm{Set})$ from the category of groups to that of sets. A morphism of group schemes over S is just a morphism of S-schemes that respects the group structure. In particular, to give a morphism of S-group schemes from G to G' is, by Yoneda's lemma, to give, for every S-scheme T, a morphism of groups from $G(T)$ to $G'(T)$, functorial in T.

1.8.2 Remark. Of course, this kind of definition has nothing to do with schemes: it works in every category. Also, one can replace the notion of group by ring, or similar things, and get the notion of ring object in a category.

1.8.3 Remark. If G/S is a group scheme, we get, by Yoneda's lemma, a morphism of S-schemes $m\colon G \times_S G \to G$, that sends (P, Q) in $G(T) \times G(T) = (G \times_S G)(T)$ to their product PQ in $G(T)$. The identity element e in $G(S)$ is a morphism of S-schemes $S \to G$. The inversion, for every S-scheme T, in $G(T)$, induces a morphism of S-schemes ι from G to G. These morphisms m, e and ι satisfy some conditions implied by the axioms for a group structure, that can be expressed in diagrams. This gives another definition of group scheme that one often finds in the literature, but it just makes the notion look more complicated. Note that Lie groups are usually defined by such diagrams, but one could as well define them in terms of group structures on functors.

1.8.4 Example. Let S be a scheme. Then the additive group over S, denoted $\mathbb{G}_{\mathrm{a}\,S}$, is the affine line $\mathbb{A}^1_S$ equipped with the group structure that corresponds to the functor $T \mapsto \mathcal{O}_T(T)$ from (Sch/S) to (Grp). Note that in fact each $\mathcal{O}_T(T)$ is actually a ring, so that $\mathbb{A}^1_S$ has the structure of a ring scheme.

1.8.5 Example. The S-group scheme $\mathbb{G}_{\mathrm{m}\,S}$, for S any scheme, is by definition the one that represents the functor $T \mapsto \mathcal{O}_T(T)^*$ from (Sch/S) to (Grp); it is called the multiplicative group over S.

1.8.6 Example. Let $n \geq 0$ be an integer. For any scheme S, we define $\mathrm{GL}_{n,S}$ to be the functor from S-schemes to (Grp) that sends T to the group $\mathrm{GL}_n(\mathcal{O}_T(T))$ of invertible n by n matrices with coefficients in $\mathcal{O}_T(T)$. Let us show that this functor is representable, so that it is a group scheme. By base change from $\mathrm{Spec}(\mathbb{Z})$ to S, it suffices to show that $\mathrm{GL}_{n,\mathbb{Z}}$ is representable. We claim that it is represented by

$$\mathrm{Spec}(\mathbb{Z}[\{x_{i,j} \mid 1 \leq i,j \leq n\} \cup \{y_{i,j} \mid 1 \leq i,j \leq n\}]/I),$$

where I is the ideal generated by the n^2 equations obtained from the equality of matrices $xy = 1_n$. The verification of this is an exercise.

1.8.7 Exercise. Let A be a ring. The group schemes $\mathbb{G}_{\mathrm{a}\,A}$, $\mathbb{G}_{\mathrm{m}\,A}$ and $\mathrm{GL}_{n,A}$ are affine. Give, in each case, a description of the associated morphisms of rings m^*, e^* and ι^*. Let us do the case of the multiplicative group here. It is represented by $\mathrm{Spec}(B)$ with $B := A[x,x^{-1}] = A[x,y]/(xy-1)$. Then $B \otimes_A B = \mathbb{Z}[x_1, x_1^{-1}, x_2, x_2^{-1}]$, $m^*(x) = x_1x_2$, $e^*(x) = 1$ and $\iota(x) = x^{-1}$.

1.8.8 Example. Let k be a field of characteristic different from 2, E a non-singular curve in $\mathbb{P}^2_k$ given by an equation of the form $y^2z = x^3 + axz^2 + bz^3$ with $4a^3 + 27b^2 \neq 0$. We will show later that E/k has a unique commutative group structure such that, for $k \to \overline{k}$ an algebraic closure, and for L any line in $\mathbb{P}^2_{\overline{k}}$, the three points of intersection of E with L have sum zero. In order to prove this, one can explicitly describe the morphisms m, e and ι. But that is not the way we want to do it. In fact, we will establish an isomorphism of functors between E and a functor that has, by construction, a group structure. But that will take weeks.

To finish this section, I want to show that $\mathbb{G}_{\mathrm{m}}$ and $\mathbb{G}_{\mathrm{a}}$ behave very differently when one considers their endomorphism rings.

1.8.9 Proposition. *Let A be a ring such that* $\mathrm{Spec}(A)$ *is connected. Then* $\mathrm{End}(\mathbb{G}_{\mathrm{m}\,A}) = \mathbb{Z}$.

Proof. Let f be an endomorphism of $\mathbb{G}_{\mathrm{m}\,A}$. Since $\mathbb{G}_{\mathrm{m}\,A} = \mathrm{Spec}(A[x,x^{-1}])$, f is of the form $\mathrm{Spec}(\phi)$, with $\phi\colon A[x,x^{-1}] \to A[x,x^{-1}]$ a morphism of A-algebras. We write $\phi(x) = \sum a_n x^n$, with n ranging through $\mathbb{Z}$, with almost all a_n equal to zero. We use the description we gave above for m^*. Because f is compatible with the group law, the following diagram is commutative:

$$\begin{array}{ccc} A[x,x^{-1}] & \xrightarrow{m^*} & A[x_1,x_1^{-1},x_2,x_2^{-1}] \\ \downarrow\phi & & \phi\otimes\phi\downarrow \\ A[x,x^{-1}] & \xrightarrow{m^*} & A[x_1,x_1^{-1},x_2,x_2^{-1}] \end{array} \tag{1.8.10}$$

Evaluating on x gives the identity:

$$\sum a_n(x_1x_2)^n = \left(\sum a_nx_1^n\right)\left(\sum a_mx_2^m\right) \tag{1.8.11}$$

in $A[x_1, x_1^{-1}, x_2, x_2^{-1}]$. This means that f is compatible with the group structure if and only if $a_n^2 = a_n$ for all n, and $a_na_m = 0$ if $n \neq m$. Since $\mathrm{Spec}(A)$ is connected, 0 and 1 are the only idempotents. Since $\sum a_nx^n$ must be invertible, we conclude that $\sum a_nx^n = x^m$ for some m. But then f is the "multiplication by m" map. □

1.8.12 Proposition. *Let A be a $\mathbb{Q}$-algebra. Then* $\mathrm{End}(\mathbb{G}_{\mathrm{a}\,A}) = A$.

Proof. Let f be an endomorphism of $\mathbb{G}_{\mathrm{a}\,A}$. Let ϕ be the morphism of rings $A[x] \to A[x]$ induced by f, and let $\sum a_nx^n$ be $\phi(x)$. Writing down that f is compatible with the group structure gives the identity:

$$\sum a_n(x_1 + x_2)^n = \sum a_nx_1^n + \sum a_mx_2^m \tag{1.8.13}$$

in $A[x_1, x_2]$. Since A is a $\mathbb{Q}$-algebra, it follows that a_n is zero if $n \neq 1$. □

1.8.14 Exercise. Let p be a prime number. Compute $\mathrm{End}(\mathbb{G}_{\mathrm{a}\,\mathbb{F}_p})$.

2 January 15, 1999

Since we want to discuss cohomology of sheaves, it is almost necessary to do that using derived functors. For what follows, good references are sections on homological algebra in advanced books on algebra, such as [LaA] and [JaA2]. As a general reference for categorical notions, let me give [MacCWM]. I also recommend the notes of a course "Algèbre homologique et théorie des faisceaux", given by Bernard Le Stum in 1994-1995, that were distributed to you. A very short review of derived funtors and cohomology of sheaves is given in [HarAG, II.1–2].

Of course, if one is interested only in cohomology, one could stick to the notion of Čech cohomology, but derived functors are bound to be necessary at some point anyway (Ext groups, for example).

As a motivation for the heavy (but very useful) machinery that follows, let us look at one example, the exponential sequence on the complex analytic variety $X := \mathbb{C} - \{0\}$:

$$0 \to \mathbb{Z}_X \to \mathcal{O}_X \to \mathcal{O}_X^* \to 0.$$

The cohomological machinery associates to this short exact sequence of sheaves (of abelian groups) a long exact cohomology sequence:

$$0 \to \mathbb{Z} \to \mathcal{O}_X(X) \to \mathcal{O}_X^*(X) \to \mathrm{H}^1(X, \mathbb{Z}_X) \to \mathrm{H}^1(X, \mathcal{O}_X) \to \mathrm{H}^1(X, \mathcal{O}_X^*) \to \cdots$$

One can compute the higher cohomology groups in this sequence, and get a good understanding of the obstruction against an invertible holomorphic function on X being the exponential of a holomorphic function on X. Or the other way around, if one understands that obstruction, one learns something about $\mathrm{H}^1(X, \mathbb{Z}_X)$. Dealing with cohomology is often like this, one needs to consider many long exact sequences in order to "compute" cohomology groups.

In what follows, the cohomology groups of a sheaf will be obtained as the derived functors of the functor of global sections, evaluated on the sheaf in question.

2.1 Derived functors.

Let us begin with the notions of additive and abelian categories, and additive functors. I follow the exposition in [LaA]. I should not omit to say that there is also the notion of derived category, but we won't go into that (a good reference for them is [IlCD]).

2.1.1 Definition. An additive category $\mathcal{C}$ is a category in which, for every pair of objects X and Y of $\mathcal{C}$, is equipped with the structure of abelian group, satisfying the following two conditions:

AB 1 The law of composition of morphisms is bilinear, and there exists a zero object (i.e., an object 0 such that for every object X, $\mathrm{Hom}(0, X)$ and $\mathrm{Hom}(X, 0)$ have just one element);

AB 2 Finite products and coproducts exist in $\mathcal{C}$.

A functor (covariant or contravariant) $F\colon \mathcal{A} \to \mathcal{B}$ between additive categories is additive if for every M and M' in $\mathcal{A}$ the map $\mathrm{Hom}_{\mathcal{A}}(M, M') \to \mathrm{Hom}_{\mathcal{B}}(FM, FM')$ is a morphism of groups.

In an additive category, one can define the notion of kernel and cokernel of a morphism, as follows.

2.1.2 Definition. Let $f\colon M \to N$ be a morphism in an additive category $\mathcal{C}$. A kernel of f is then a morphism $i\colon K \to M$ such that for every object P of $\mathcal{C}$ the sequence:

$$0 \to \mathrm{Hom}(P, K) \to \mathrm{Hom}(P, M) \to \mathrm{Hom}(P, N)$$

is exact. A cokernel of f is a morphism $p\colon N \to C$ such that for every object P in $\mathcal{C}$ the sequence:

$$0 \to \mathrm{Hom}(C, P) \to \mathrm{Hom}(N, P) \to \mathrm{Hom}(M, P)$$

is exact.

Another way to phrase this definition is that a kernel of f represents the functor $P \mapsto \ker(\mathrm{Hom}(P, M) \to \mathrm{Hom}(P, N))$, and a cokernel the functor $P \mapsto \ker(\mathrm{Hom}(N, P) \to \mathrm{Hom}(M, P))$. Of course, the definition does not say that each f has a kernel, or a cokernel, but if a kernel or cokernel exists, it is unique up to unique isomorphism. For example, the category of commutative Lie groups has kernels, but not every morphism in it has a cokernel. The category of vector bundles over a fixed manifold has neither kernels nor cokernels. By the way, this gives us a good reason to embed the category of vector bundles over X in that of sheaves of $\mathcal{O}_X$-modules, in which kernels and cokernels do exist.

2.1.3 Exercise. Show that, for A a ring (not necessarily commutative), the category A-Mod of (right) A-modules has a natural structure of additive category, and that the notions of kernel and cokernel are as before.

2.1.4 Definition. An abelian category is an additive category that satisfies:

AB 3 Kernels and cokernels exist.

AB 4 If f is a morphism with $\ker(f) = 0$ (i.e., f is a monomorphism), then f is the kernel of its cokernel. If f is a morphism with $\mathrm{coker}(f) = 0$ (i.e., f is an epimorphism), then f is the cokernel of its kernel. If f is a morphism with $\ker(f) = 0$ and $\mathrm{coker}(f) = 0$, then f is an isomorphism.

2.1.5 Exercise. Show that, for a ring A, the category A-Mod is abelian. Show that, for X a topological space with a sheaf of rings $\mathcal{O}_X$, the category $\mathcal{O}_X$-Mod of sheaves of $\mathcal{O}_X$-modules is abelian. Give an example of an additive category that is not abelian.

2.1.6 Definition. Let $\mathcal{A}$ be an abelian category. A *complex* in $\mathcal{A}$ is a sequence (M, d):

$$\cdots \longrightarrow M^{i-1} \xrightarrow{d^{i-1}} M^i \xrightarrow{d^i} M^{i+1} \longrightarrow \cdots$$

of objects M^i of $\mathcal{A}$, indexed by $\mathbb{Z}$, with morphisms $d^i\colon M^i \to M^{i+1}$, such that $d^{i+1}d^i = 0$. A *morphism of complexes* from a complex (M, d) to a complex (M', d') is a sequence of morphisms $f^i\colon M^i \to M'^i$ intertwining d and d'. This gives a category of complexes. A complex (M, d) is called *exact (or acyclic) at* i if $\ker(d^i) = \mathrm{im}(d^{i-1})$; it is called *exact* if it is so at all i. The *homology* of a complex (M, d) at i is the object $\mathrm{h}^i(M) := \ker(d^i)/\mathrm{im}(d^{i-1}$. So a complex is exact at i if and only if its ith homology is zero.

2.1.7 Example. The terminology of complexes has its origins, I think, in algebraic topology, or in differential geometry. So let us give two examples from there.

On a differentiable manifold X one has the de Rham complex of global differential forms. The homology of that complex is called the de Rham cohomology of X (one should suppose here that X is seperated and paracompact).

For a topological space X, and $n \geq 0$, consider the free abelian group $C'_n(X)$ with basis the continuous maps $f\colon I^n \to X$, with I the closed interval $[0, 1]$ in $\mathbb{R}$. For $n \geq 1$, we have a morphism $d_n\colon C'_n(X) \to C'_{n-1}(X)$ defined by:

$$d_n f = \sum_{i=1}^{n} (-1)^i (t^*_{n-1,i} f - s^*_{n-1,i} f),$$

where $s_{n-1,i}$ and $t_{n-1,i}$ are the maps $I^{n-1} \to I^n$ that stick in a zero or one at the ith coordinate. (It is a good thing to make some pictures for $n \leq 3$; this explains why one talks about boundary maps.) It is a standard exercise to show that (C', d) is a complex. Let $C''_n(X)$ be the submodule generated by the $f\colon I^n \to X$ that are degenerate, i.e., the f that are constant in one of the n variables. Then the $C''_n(X)$ form a subcomplex, and the $C_n(X) := C'_n(X)/C''_n(X)$ form a complex that whose homology groups are the *singular* *homology groups* of X. It is quite a miracle that such grotesquely defined groups are finitely generated $\mathbb{Z}$-modules if X is a compact manifold, whose $\mathbb{R}$-duals are canonically isomorphic to the de Rham cohomology groups of X. A reasonable reference for this stuff is [MasSH]. In order to compute the singular homology groups for concretely given topological spaces one usually uses homotopy invariance and Mayer-Vietoris sequences. For example, to compute these groups for a point is a trivial matter; any contractible topological space has the same homology groups as a point.

2.1.8 Definition. Let $F\colon \mathcal{A} \to \mathcal{B}$ be an additive covariant functor between abelian categories. Then F is *exact* if for every exact sequence $A' \to A \to A''$ in $\mathcal{A}$ the sequence $FA' \to FA \to FA''$ is exact. The functor F is called *left exact* if for every exact sequence $0 \to A' \to A \to A''$ in $\mathcal{A}$ the sequence $0 \to FA' \to FA \to FA''$ is exact. The functor F is called *right exact* if for every exact sequence $A' \to A \to A'' \to 0$ in $\mathcal{A}$ the sequence $FA' \to FA \to FA'' \to 0$ is exact. For a contravariant additive functor $F\colon \mathcal{A} \to \mathcal{B}$ one has the analogous notions. For example, such an F is called *left exact* if for every exact sequence $A' \to A \to A'' \to 0$ in $\mathcal{A}$ the sequence $0 \to FA'' \to FA \to FA'$ is exact.

2.1.9 Example. For $\mathcal{A}$ an abelian category and M in $\mathcal{A}$, both functors $\mathrm{Hom}(\cdot, M)$ and $\mathrm{Hom}(M, \cdot)$ from A-Mod to $\mathbb{Z}$-Mod are left exact, and usually not right exact. For A a commutative ring, and M an A-module, the functor $M \otimes_A \cdot$ from A-Mod to itself is right exact, but usually not left exact. For X a topological space, the global section functor Γ from the category $\mathrm{Sh}(X)$ of sheaves of abelian groups on X to $\mathbb{Z}$-Mod is left exact and usually not right exact. For X a topological space, and x in X, the functor $\mathcal{F} \mapsto \mathcal{F}_x$ from $\mathrm{Sh}(X)$ to $\mathbb{Z}$-Mod is exact.

2.1.10 Definition. Let $\mathcal{A}$ be an abelian category. An object I of $\mathcal{A}$ is *injective* if the functor $\mathrm{Hom}(\cdot, I)$ is exact. An object P of $\mathcal{A}$ is *projective* if the functor $\mathrm{Hom}(P, \cdot)$ is exact.

2.1.11 Exercise. Show that in $\mathbb{Z}$-Mod the injectives are the divisible $\mathbb{Z}$-modules (i.e., those for which $x \mapsto nx$ is surjective for all non-zero integers n), and that the projectives are the free modules. For A any ring, show that the projective A-modules are the direct summands of free modules.

2.1.12 Example. Let T denote the tangent bundle of the three sphere S^2, and N its normal bundle in $\mathbb{R}^3$. Since $T \oplus N$ is the restriction to S^2 of the tangent bundle of $\mathbb{R}^3$, it is trivial. Moreover, N is trivial. So here we have an example of a direct summand of a free bundle that is not trivial, and where even the other summand is free. However, T itself is not free, since it does not have a continuous section without zero's. Let A be the ring of C^∞-functions on the sphere S^3. Let M denote the sheaf of C^∞ sections of T. Then M is a projective A-module, not free, such that $M \oplus A$ is isomorphic to A^3.

2.1.13 Construction. Let $F\colon \mathcal{A} \to \mathcal{B}$ be an additive covariant left exact functor between abelian categories. Suppose that every object A in $\mathcal{A}$ can be embedded in an injective object (i.e., $\mathcal{A}$ has sufficiently many injectives). Let A be in $\mathcal{A}$. Choose an injective resolution $0 \to A \to I$, i.e., a complex

$$0 \to A \to I^0 \to I^1 \to I^2 \to \cdots$$

that is exact and with the I^n injectives. Then one puts, for $i \geq 0$, $(\mathrm{R}^i F)A := \mathrm{h}^i(FI)$ This is well defined, in the sense that for any other choice $0 \to A \to J$ of an injective resolution, there is a natural isomorphism between $\mathrm{h}^i(FI)$ and $\mathrm{h}^i(FJ)$. Moreover, $(\mathrm{R}^i F)A$ is functorial in A, and the functor $\mathrm{R}^i F$ is called the ith derived functor of F. Since F is left exact, one has $\mathrm{R}^0 F = F$. A most important property of this construction is that for every short exact sequence $0 \to A' \to A \to A'' \to 0$ in $\mathcal{A}$ one gets a long exact sequence:

$$0 \to FA' \to FA \to FA'' \to (\mathrm{R}^1 F)A' \to (\mathrm{R}^1 F)A \to (\mathrm{R}^1 F)A'' \to (\mathrm{R}^2 F)A' \to \cdots$$

that is functorial for morphisms of short exact sequences.

2.1.14 Remark. As always with categories, there is the dual notion of projective resolution, and left derived functors of covariant right exact additive functors (provided there are sufficiently many projectives). Likewise, one has the notion of right derived functors of a contravariant left exact functor (if there are sufficiently many projectives), and left derived functors of a contravariant right exact functor (if there are sufficiently many injectives).

The essential tool to show that derived functors are defined up to unique isomorphism is the notion of homotopy of complexes. This notion comes from topology, where one shows that if $f, g\colon X \to Y$ are homotopic, then $f^* = g^*$ from the singular homology from X to that of Y (and, likewise, for de Rham cohomology and all sorts of cohomology).

The notion of a sequence of functors that transform short exact sequences into long exact sequences can be axiomatized (delta functors). Under some mild hypothesis (effaceability, also called erasability by Lang, of the F^i for $i > 0$), derived functors are universal delta functors, which implies that they are characterized up to unique isomorphism by some properties (which is always good to know).

2.2 Examples of derived functors

2.2.1 Ext.

Let $\mathcal{A}$ be an abelian category, and A an object of it. The functor $\mathrm{Hom}(A, \cdot)$ from $\mathcal{A}$ to $\mathbb{Z}$-Mod is covariant and left exact. If $\mathcal{A}$ has sufficiently many injectives, then, for $i \geq 0$, $\mathrm{Ext}^i(A, \cdot)$ denotes $\mathrm{R}^i\mathrm{Hom}(A, \cdot)$. For B in $\mathcal{A}$ the functor $\mathrm{Hom}(\cdot, B)$ is contravariant and left exact. If $\mathcal{A}$ has sufficiently many projectives, then, for $i \geq 0$, $\mathrm{Ext}^i(\cdot, B)$ denotes $\mathrm{R}^i\mathrm{Hom}(\cdot, B)$. Of course, in order for this notation to be justified, it should be the case that if $\mathcal{A}$ has suficiently many injectives, and sufficiently many projectives, then $\mathrm{Ext}^i(A, B)$ has just one meaning; this is the case.

The name "Ext" comes from the word extension, which is explained by the following interpretation for $i = 1$. Of course, $\mathrm{Ext}^0(A, B)$ is just $\mathrm{Hom}(A, B)$. One can show that $\mathrm{Ext}^1(A, B)$ is functorially isomorphic to the set of isomorphism classes of extensions of A by B:

$$0 \to B \to E \to A \to 0,$$

where isomorphism means: morphism of complexes inducing the identity on A and on B. Exercise: associate to an isomorphism class of such extensions an element of $\mathrm{Ext}^1(A, B)$. There is an interpretation of $\mathrm{Ext}^i(A, B)$ in terms of "repeated extensions" of the form:

$$0 \to B \to E^1 \to \cdots \to E^i \to A.$$

These things are called Yoneda extensions. They are very useful for constructing a multiplicative structure on the Ext^i: one has bilinear maps:

$$\mathrm{Ext}^i(A, B) \times \mathrm{Ext}^j(B, C) \to \mathrm{Ext}^{i+j}(A, C).$$

But the equivalence relation on the set of such extensions is quite complicated, and, in fact, as complicated as the notion of morphism in the so-called derived category of $\mathcal{A}$. The next few lines are just included so that I myself do not forget what is in them. The cup product in the cohomology of sheaves is obtained, in terms of the derived category, as follows. So let $(X, \mathcal{O}_X)$ be a ringed space, let $\mathcal{A} := \mathcal{O}_X$-Mod and let $\mathcal{F}$ and $\mathcal{G}$ be $\mathcal{O}_X$-modules. We want to construct bilinear maps from $\mathrm{H}^i(X, \mathcal{F}) \times \mathrm{H}^j(X, \mathcal{G})$ to $\mathrm{H}^{i+j}(X, \mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G})$. One has $\mathrm{H}^i(X, \mathcal{F}) = \mathrm{Hom}_{D(\mathcal{A})}(\mathcal{O}_X[0], \mathcal{F}[i])$, and $\mathrm{H}^i(X, \mathcal{G}) = \mathrm{Hom}_{D(\mathcal{A})}(\mathcal{O}_X[0], \mathcal{G}[j])$. Then one uses that $\cdot \overset{\mathbb{L}}{\otimes} \cdot$ is a bifunctor from $D^-(\mathcal{A}) \times D^-(\mathcal{A})$ to $D^-(\mathbb{Z}_X)$, which gives us, for α in $\mathrm{H}^i(X, \mathcal{F})$, an element $\alpha \overset{\mathbb{L}}{\otimes} \mathrm{id}$ in $\mathrm{Hom}_{D(\mathcal{A})}(\mathcal{O}_X[0] \overset{\mathbb{L}}{\otimes} \mathcal{G}[j], \mathcal{F}[i]) \overset{\mathbb{L}}{\otimes} \mathcal{G}[j])$. Then one notes that $\mathcal{O}_X[0] \overset{\mathbb{L}}{\otimes} \mathcal{G}[j]$ is just $\mathcal{G}[j]$, and that there is a natural morphism from $\mathcal{F}[i]) \overset{\mathbb{L}}{\otimes} \mathcal{G}[j]$ to to $(\mathcal{F} \otimes \mathcal{G})[i + j]$.

This gives an element in $\mathrm{Hom}_{D(\mathcal{A})}(\mathcal{O}_X[0], (\mathcal{F}\otimes\mathcal{G})[i+j])$, hence in $\mathrm{H}^{i+j}(X, \mathcal{F}\otimes\mathcal{G})$. As I said, this stuff was not part of the course; from now on again it is.

Let us do an explicit example. Let $\mathcal{A}$ be $\mathbb{Z}$-Mod. Let n and m be integers. We want to compute the $\mathrm{Ext}^i(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$. First of all, we can do this using an injective resolution of $\mathbb{Z}/m\mathbb{Z}$. Here is one:

$$0 \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Q}/\mathbb{Z} \xrightarrow{.m} \mathbb{Q}/\mathbb{Z} \longrightarrow 0 \to \cdots$$

Suppose that $n \neq 0$. Applying $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \cdot)$ to this resolution gives the complex:

$$n^{-1}\mathbb{Z}/\mathbb{Z} \xrightarrow{.m} n^{-1}\mathbb{Z}/\mathbb{Z} \longrightarrow 0 \cdots.$$

Hence we have:

$$\begin{aligned}
\mathrm{Ext}^0(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) &\cong \mathbb{Z}/(n\mathbb{Z}+m\mathbb{Z})\\
\mathrm{Ext}^1(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) &\cong \mathbb{Z}/(n\mathbb{Z}+m\mathbb{Z})\\
\mathrm{Ext}^i(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) &\cong 0 \quad \text{if } i > 1.
\end{aligned}$$

Secondly, one can use a projective resolution of $\mathbb{Z}/n\mathbb{Z}$. I leave it as an exercise to take one, and to carry out the computation. One will see that the answer is the same. (I should say, however, that it is not so clear what the "canonical" isomorphism between the two is.)

2.2.2 Tor.

Let A be a commutative ring, and $\mathcal{A}$ be the category A-Mod. For M in A-Mod, the functor $\cdot\otimes_A M$ from A-Mod to itself is right exact and covariant. One defines $\mathrm{Tor}^i_A(\cdot, M)$ to be $\mathrm{L}^i(\cdot\otimes_A M)$. Since the tensor product has actually two arguments, one can prove that:

$$\mathrm{Tor}^i_A(N, M) = (\mathrm{L}^i(\cdot\otimes_A M))N = (\mathrm{L}^i(N\otimes_A \cdot))M.$$

An A-module M is called *flat* if the functor $M\otimes_A\cdot$ is exact. Note that projecive A-modules are flat, as they are direct summands of free modules.

Let us do an explicit example. Take $A := \mathbb{Z}$, $M := \mathbb{Z}/m\mathbb{Z}$ and N arbitrary. As a projective resolution for M we take:

$$\cdots \longrightarrow \mathbb{Z} \xrightarrow{m} \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow 0.$$

It shows that $\mathrm{Tor}^1_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, N) = \{x \in M \mid mx = 0\}$.

2.3 Derived categories

It would not do to not mention the fact that not only there are derived functors, but also derived categories. An excellent reference, for this as well as for homological algebra in general, is the volume “homological algebra” in the Springer series “Encyclopaedia of mathematics” [GeMaHA]. The idea is to localize the category of complexes, in the sense that one makes quasi-isomorphisms (i.e., morphisms that induce an isomorphism on homology) into isomorphisms. We do not go into this in this course, but I will try to deal as most as we can with complexes themselves in stead of their homology. Another point is that, in order to prove results we want about derived functors, we need the technique of spectral sequences. There, the idea is to study filtered complexes, and the induced filtration on the homology. A good reference for this is [LaA], and of course [GeMaHA]. I think that we will see a few spectral sequences at work later on in this course.

3 January 29, 1999

3.1 Cohomology of sheaves.

Let X be a topological space, and $\mathcal{O}_X$ a sheaf of rings on it. This gives us the abelian category $\mathcal{O}_X$-Mod of sheaves of $\mathcal{O}_X$-modules. On that category, we have the covariant left exact functor Γ, taking values in $\mathbb{Z}$-Mod, or in $\mathcal{O}_X(X)$-Mod, if one likes, sending $\mathcal{F}$ to $\Gamma(\mathcal{F}) = \mathcal{F}(X)$. The right derived functors of Γ are the higher cohomology functors, denoted $\mathrm{H}^i(X, \cdot)$. But, of course, we have to show that $\mathcal{O}_X$-Mod has sufficiently many injectives.

3.1.1 Remark. Let us note that, for $\mathcal{F}$ in $\mathcal{O}_X$-Mod, $\mathcal{F}(X)$ is the same as $\mathrm{Hom}(\mathcal{O}_X, \mathcal{F})$, hence, if they exist, $\mathrm{H}^i(X, \mathcal{F}) = \mathrm{Ext}^i(\mathcal{O}_X, \mathcal{F})$. So in fact, the existence of sufficiently many projectives would also suffice for defining cohomology groups. But, as we will see, $\mathcal{O}_X$-Mod does have sufficiently many injectives, and not necessarily sufficiently many projectives. Before going on, let us show that the interpretation of $\mathrm{H}^i(X, \mathcal{F})$ as $\mathrm{Ext}^i(\mathcal{O}_X, \mathcal{F})$ gives a multiplicative structure (called the cup product) on cohomology of sheaves. So let $\mathcal{F}$ and $\mathcal{G}$ be $\mathcal{O}_X$-modules. Then we have bilinear maps:

$$\mathrm{H}^i(X, \mathcal{F}) \times \mathrm{H}^j(X, \mathcal{G}) \longrightarrow \mathrm{H}^{i+j}(X, \mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}),$$

of which the general construction is not so easy to give at this moment. Exercise: give the construction in the special case where $\mathcal{F}$ and $\mathcal{G}$ are both equal to $\mathcal{O}_X$, and, a bit more generally, in the case where at least one of them is a flat $\mathcal{O}_X$-module.

In order to show that the category of $\mathcal{O}_X$-modules on a ringed space $(X, \mathcal{O}_X)$ has sufficiently many injectives, we start with a general principle, using the notion of adjoint functors.

3.1.2 Definition. Let $\mathcal{A}$ and $\mathcal{B}$ be two categories, and $f\colon \mathcal{A} \to \mathcal{B}$ and $g\colon \mathcal{B} \to \mathcal{A}$ be two covariant functors. Then f is called a right adjoint of g (and g a left adjoint of f) if, for all X in $\mathcal{B}$ and Y in $\mathcal{A}$, there are bijections:

$$\mathrm{Hom}_{\mathcal{A}}(gX, Y) \longrightarrow \mathrm{Hom}_{\mathcal{B}}(X, fY),$$

functorially in X and Y (i.e., one has an isomorphism of bifunctors).

3.1.3 Exercise. How unique are adjoints? Do they always exist?

3.1.4 Example. The functor Spec from (Ring) to (Sch) is a right adjoint of the functor $X \mapsto \mathcal{O}_X(X)$ in the other direction.

3.1.5 Exercise. Let A be a ring. Let $f\colon \mathbb{Z}\text{-Mod} \to A\text{-Mod}$ be the functor sending M to $\mathrm{Hom}_{\mathbb{Z}}(A, M)$. Let $g\colon A\text{-Mod} \to \mathbb{Z}\text{-Mod}$ be the functor $N \mapsto {}_{\mathbb{Z}}N$, where ${}_{\mathbb{Z}}N$ is just the underlying additive group of N. Then show that g is a left adjoint of f.

3.1.6 Lemma. *Let $f\colon \mathcal{A} \to \mathcal{B}$ be an additive functor between abelian categories. Suppose that f has a left adjoint g, and that g is exact. Then f maps injectives to injectives.*

Proof. Just write out the definitions. $\square$

3.1.7 Proposition. *For every ring A, the abelian category A-Mod has enough injectives.*

Proof. Let A be a ring. Put $I := \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$. This is an injective A-module. For M an A-module, let M^* be the A-module $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$. Let now N be an A-module. Choose a surjection:

$$\oplus_{i\in S} A \longrightarrow N^*.$$

Dualizing once more gives:

$$N \hookrightarrow N^{**} = \mathrm{Hom}_{\mathbb{Z}}(N^*, \mathbb{Q}/\mathbb{Z}) \hookrightarrow \prod_{i\in S} I,$$

an injection of N into an injective A-module (note that products of injectives are injectives, just as sums of projectives are projective). $\square$

3.1.8 Proposition. *([HarAG, III, Prop. 2.2]) Let $(X, \mathcal{O}_X)$ be a ringed space. Then $\mathcal{O}_X$-Mod has sufficiently many injectives.*

Proof. Let $\mathcal{F}$ be an $\mathcal{O}_X$-module. For every x in X, let i_x denote the inclusion map from $\{x\}$ in X, and let $\mathcal{F}_x \hookrightarrow I_x$ be an injection of $\mathcal{O}_{X,x}$-modules, with I_x injective. Then we have:

$$\mathcal{F} \hookrightarrow \prod_{x\in X} i_{x,*}\mathcal{F}_x \hookrightarrow \prod_{x\in X} i_{x,*}I_x,$$

and the last $\mathcal{O}_X$-module is injective, because products of injectives are injective, and each $i_{X,*}$ has an exact left-adjoint: i_x^{-1}. $\square$

3.1.9 Definition. Let $(X, \mathcal{O}_X)$ be a ringed space. For $i \geq 0$, the ith right derived functor of the global section functor $\mathcal{F} \mapsto \mathcal{F}(X)$ is called the ith cohomology functor, and is denoted $\mathrm{H}^i(X, \cdot)$.

3.2 First properties of sheaf cohomology.

In practice, one doesn't usually have explicit injective resolutions to compute cohomology with. So it is useful to know that other types of resolutions also suffice. One has the following proposition/definition about derived functors in general. For a proof that does not use spectral sequences, see [LaA] (Thm. 6.2 of Chapter IV in the 2nd edition).

3.2.1 Proposition. *Let $f\colon \mathcal{A} \to \mathcal{B}$ be an additive left exact functor between abelian categories. Suppose that $\mathcal{A}$ has sufficiently many injectives. An object A of $\mathcal{A}$ is called* f-acyclic *if, for all $i > 0$, $(\mathrm{R}^i f)A = 0$. Let A be in $\mathcal{A}$, and $A \to C$ be an f-acyclic resolution (i.e., a resolution with all C_i f-acyclic). Then the $(\mathrm{R}^i f)A$ are canonically isomorphic to the $\mathrm{h}^i(fC)$.*

In the case of cohomology of sheaves, we have the following class of acyclic objects.

3.2.2 Lemma. *([HarAG, III, Lemma 2.4, Prop. 2.5 and Prop. 2.6]) A sheaf $\mathcal{F}$ on a topological space X is called* flabby, *or* flasque, *if all restriction maps are surjective. For $(X, \mathcal{O}_X)$ a ringed space, flasque $\mathcal{O}_X$-modules are acyclic for the global section functor; moreover, every injective $\mathcal{O}_X$-module is flasque. In particular, the cohomology of an $\mathcal{O}_X$-module is the same as that of its underlying $\mathbb{Z}_X$-module.*

3.2.3 Example. On an irreducible topological space, constant sheaves are flasque.

An important tool for computing sheaf cohomology is the Mayer-Vietoris exact sequence.

3.2.4 Theorem. (Mayer-Vietoris for open subsets.) *Let X be a topological space, X_1 and X_2 two open subsets such that $X = X_1 \cup X_2$. Let $X_{1,2} := X_1 \cap X_2$, and let j_1, j_2 and $j_{1,2}$ be the inclusions. Let $\mathcal{F}$ be an abelian sheaf on X. Then we have a long exact sequence:*

$$\cdots \to \mathrm{H}^i(X, \mathcal{F}) \to \mathrm{H}^i(X_1, \mathcal{F}|_{X_1}) \oplus \mathrm{H}^i(X_2, \mathcal{F}|_{X_2}) \to \mathrm{H}^i(X_{1,2}, \mathcal{F}|_{X_{1,2}}) \to \mathrm{H}^{i+1}(X, \mathcal{F}) \to \cdots,$$

functorially in $\mathcal{F}$.

Proof. Let $\mathcal{F} \to I$ be an injective resolution. Then we have the short exact sequence of complexes:

$$0 \to I(X) \to I(X_1) \oplus I(X_2) \to I(X_{1,2}) \to 0,$$

because the I^i are sheaves (the first map takes the two restrictions, the second map the difference of the two restrictions). All we need to do now is to identify the associated long exact homology sequence as the sequence in the Theorem. This follows directly from the fact that, for $j\colon U \to X$ an open immersion, the functor j^{-1} is exact and preserves injectives (it preserves injectives because it has an exact left-adjoint, $j_!$, called extension by zero, see [HarAG, II, Ex. 1.19]. $\square$

3.2.5 Theorem. (Mayer-Vietoris for closed subsets.) *Let X be a topological space, X_1 and X_2 two closed subsets such that $X = X_1 \cup X_2$. Let $X_{1,2} := X_1 \cap X_2$, and let i_1, i_2 and $i_{1,2}$ be the injections, which are closed immersions. Let $\mathcal{F}$ be an abelian sheaf on X. Then we have a long exact sequence:*

$$\cdots \to \mathrm{H}^i(X, \mathcal{F}) \to \mathrm{H}^i(X_1, i_1^{-1}\mathcal{F}) \oplus \mathrm{H}^i(X_2, i_2^{-1}\mathcal{F}) \to \mathrm{H}^i(X_{1,2}, i_{1,2}^{-1}\mathcal{F}) \to \mathrm{H}^{i+1}(X, \mathcal{F}) \to \cdots,$$

functorially in $\mathcal{F}$.

Proof. For f a morphism of topological spaces, f_* is a left-adjoint of f^{-1}. This allows us to define a complex of sheaves:

$$0 \to \mathcal{F} \to i_{1,*}i_1^{-1}\mathcal{F} \oplus i_{2,*}i_2^{-1}\mathcal{F} \to i_{1,2,*}i_{1,2}^{-1}\mathcal{F} \to 0, \tag{3.2.6}$$

where the first map is the sum of the two tautological maps, and where the second map is the difference of the two tautological maps. One verifies that this complex is exact, by looking at the stalks. It remains to show that the long exact cohomology sequence is the one we want. To see that, note that for $i\colon Y \to X$ a closed immersion, and $\mathcal{F}$ an abelian sheaf on Y, we have a natural isormorphism between $\mathrm{H}^i(Y, \mathcal{F})$ and $\mathrm{H}^i(X, i_*\mathcal{F})$ (use that i_* of an injective resolution of $\mathcal{F}$ is an injective resolution of $i_*\mathcal{F}$). $\square$

Another important tool to compute sheaf cohomology is via the comparison with Cech cohomology with respect to suitable open covers. For the definition of Cech cohomology with respect to an open cover, see [HarAG, III, §4].

3.2.7 Theorem. *Let $(X, \mathcal{O}_X)$ be a ringed space, $\mathcal{F}$ an $\mathcal{O}_X$-module, and $U\colon I \to \mathrm{Open}(X)$ an open cover of X such that for all $p \geq 0$, for all $i_0, \ldots, i_p$ in I and all $i \geq 1$ one has $\mathrm{H}^i(U_{i_0,\ldots,i_p}, \mathcal{F}) = 0$, where $U_{i_0,\ldots,i_p}$ denotes the intersection of the U_{i_j} and $\mathcal{F}$ the restriction of $\mathcal{F}$ to it. Then for all $i \geq 0$ one has a natural isomorphism between $\mathrm{H}^i(X, \mathcal{F})$ and the Cech cohomology group $\mathrm{H}^i(U, \mathcal{F})$.*

Proof. One adapts the proof of [HarAG, III, Thm. 4.5] to this case. In that theorem, it is proved that Cech cohomology coincides with the real cohomology for quasi-coherent sheaves on separated schemes. Let us note that this proof does not use double complexes or spectral sequences. $\square$

3.3 Cohomology of quasi-coherent sheaves.

This last theorem applies very well to quasi-coherent $\mathcal{O}_X$-modules on separated noetherian schemes, because of the following theorem and the property that the intersection of two affine opens in a seperated scheme is affine ([HarAG, II, Ex. 4.3x]). (See also [HarAG, Thm. 3.7], which gives a cohomological characterization for noetherian schemes to be affine.)

3.3.1 Theorem. *([HarAG, III, Thm. 3.5]) Let X be a noetherian affine scheme. Then for all quasi-coherent $\mathcal{O}_X$-modules, and all $i > 0$, one has $\mathrm{H}^i(X, \mathcal{F}) = 0$.*

3.3.2 Remark. As does Hartshorne ([HarAG, III, Remark 3.5.1]), we remark that the preceding theorem is still true without the hypothesis that X be noetherian. The proof of this generalization consists in showing that the corresponding Cech cohomology groups are zero (using Koszul complexes), and using the following result. (The proof of this result is by induction on n, and uses a spectral sequence relating Chech cohomology to cohomology.)

3.3.3 Proposition. *([GrAH, III, Corollaire 3].) Let X be a topological space, U a basis for the topology of X with the property that for every $\mathbb{Z}_X$-module $\mathcal{F}$, for every finite intersection V of elements of U and for every $i > 0$ one has $\check{\mathrm{H}}^i(V, \mathcal{F}) = 0$. Then one also has $\mathrm{H}^i(V, \mathcal{F}) = 0$, and the natural maps $\check{\mathrm{H}}^n(X\mathcal{F}) \to \mathrm{H}^n(X, \mathcal{F})$ are isomorphisms for all i. (Here, $\check{\mathrm{H}}$ denotes Cech cohomology.)*

Using the theorem above, one can compute the cohomology of the invertible sheaves $\mathcal{O}(n)$ on projective space.

3.3.4 Theorem. *([HarAG, III, Thm. 5.1]) Let A be a noetherian ring, and $r \geq 0$. Let $X := \mathbb{P}^r_A$.*

1. *For every n in $\mathbb{Z}$, the natural map from $A[x_0, \ldots, x_r]_n$ to $\mathrm{H}^0(X, \mathcal{O}_X(n))$ is an isomorphism.*

2. *$\mathrm{H}^i(X, \mathcal{O}_X(n)) = 0$ for $0 < i < r$ and all n.*

3. *$\mathrm{H}^r(X, \mathcal{O}_X(-r-1))$ is isomorphic to A.*

4. *The natural map $\mathrm{H}^0(X, \mathcal{O}_X(n)) \times \mathrm{H}^r(X, \mathcal{O}_X(-n-r-1)) \to \mathrm{H}^r(X, \mathcal{O}_X(-r-1))$ is a perfect pairing between free A-modules of finite rank, for all n.*

For the general proof we refer to [HarAG]; we do the computation for $\mathbb{P}^1_A$, i.e., the case $r = 1$. (Let us remark that the proof of the general case, as given in [HarAG] and due to Serre, is by induction on r.)

Proof. (for $r = 1$.) By contruction of $X := \mathbb{P}^1_A = \mathrm{Proj}(B)$, with $B = A[x_0, x_1]$, we have $X = U_0 \cup U_1$, with $U_0 = D_+(x_0) = \mathrm{Spec}(A[x_1/x_0)$ and $U_1 = D_+(x_1) = \mathrm{Spec}(A[x_0/x_1)$. The intersection $U_{0,1}$ is $D_+(x_0x_1) = \mathrm{Spec}(A[x_1/x_0, x_0/x_1])$. Let n be an integer. By construction of $\mathcal{O}_X(n)$, we have $\mathcal{O}_X(n)(U_0) = B_{x_0,n}$, the degree n part of the localization of B with respect to x_0, etc. So the Cech complex reads:

$$B_{x_0,n} \oplus B_{x_1,n} \longrightarrow B_{x_0x_1,n},$$

where the two terms are in degree zero and one, respectively, and where the map sends (f, g) to $f - g$ (where we also denote by f and g their images in $B_{x_0x_1,n}$). Now all three modules that occur are free A-modules, with the following bases:

$$\{x_0^a x_1^b \mid a + b = n,\ b \geq 0\}, \quad \{x_0^a x_1^b \mid a + b = n,\ a \geq 0\}, \quad \{x_0^a x_1^b \mid a + b = n\}.$$

It follows that $\mathrm{H}^0(X, \mathcal{O}_X(n))$ is free over A with basis $\{x_0^a x_1^b \mid a + b = n,\ a \geq 0,\ b \geq 0\}$, and that $\mathrm{H}^1(X, \mathcal{O}_X(n))$ is the free A module with basis $\{x_0^a x_1^b \mid a + b = n,\ a < 0,\ b < 0\}$. (Let us remark that on $\mathbb{P}^r_A$ the computation of H^0 and H^r are as easy as in the case we treat; the problem is to show that the H^i of the $\mathcal{O}_X(n)$ vanish for $0 < i < r$.)

The pairing $\mathrm{H}^0(X, \mathcal{O}_X(n)) \times \mathrm{H}^1(X, \mathcal{O}_X(-n-2)) \to \mathrm{H}^1(X, \mathcal{O}_X(-2))$ sends the pair $(x_0^a x_1^b, x_0^i x_1^j)$ to $x_0^{a+i} x_1^{b+j}$. (To verify this, note that for X a ringed space and $\mathcal{F}$ and $\mathcal{G}$ two $\mathcal{O}_X$-modules, an element s of $\mathcal{F}(X)$ is a morphism from $\mathcal{O}_X$ to $\mathcal{F}$, hence defines a morphism $1 \otimes s$ from $\mathcal{G}$ to $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$, hence from $\mathrm{H}^i(X, \mathcal{G})$ to $\mathrm{H}^i(X, \mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G})$.) It follows that the pairing we're studying is perfect, because the bases we have are duals of each other. (A reminder: a bilinear map $b\colon M \times N \to A$ with M and N modules over a ring A is said to be perfect if the induced maps $M \to N^\vee$ and $N \to M^\vee$ are both isomorphisms.)
$\square$

3.3.5 Remark. The fact that $\mathcal{O}_X(-2)$ plays such a special role on $\mathbb{P}^1_A$ is "explained" by the fact that it is isomorphic to the sheaf of relative 1-forms $\Omega^1_{X/A}$. That this is so can easily be seen by noting that both sheaves can be obtained by the same glueing data for the cover by U_0 and U_1. More precisely, $\mathcal{O}_X(-2)$ has generators x_0^{-2} and x_1^{-2} on U_0 and U_1, respectively, which differ by tha factor $(x_0/x_1)^2$ on $U_{0,1}$. As for $\Omega^1_{X/A}$, is has generators $d(x_1/x_0)$ and $d(x_0/x_1) = d((x_1/x_0)^{-1})$, which differ by the factor $-(x_0/x_1)^2$. The minus sign can of course be removed by taking the generator $-d(x_0/x_1)$ on U_1. On $X := \mathbb{P}^r_A$, the

$\mathcal{O}_X$-module $\mathcal{O}_X(-r-1)$ is isomorphic to $\Omega^r_{X/A} := \Lambda^r_{\mathcal{O}_X}\Omega^1_{X/A}$, the sheaf of relative r-forms. We leave the verification of this as an exercise. Of course, one can give a proof of this using the exact sequence:

$$0 \longrightarrow \Omega^1_{X/A} \longrightarrow \mathcal{O}_X(-1)^{r+1} \longrightarrow \mathcal{O}_X \longrightarrow 0$$

of [HarAG, II, Thm. 8.13]. And one should even give a more natural construction of this exact sequence than Hartshorne gives. The next exercise proposes such a construction.

3.3.6 Exercise. ("Hors cours".) Let $n \geq 0$. Let A be a ring. Let $X := \mathbb{P}^n_A$ and let Y be the open part of $\mathbb{A}^{n+1}_A$ which is the complement of the image of $0\colon \mathrm{Spec}(A) \to \mathbb{A}^{n+1}_A$. Let $p\colon Y \to X$ be the morphism sending, for every A-scheme S, $(a_0, \ldots, a_n)$ in $Y(S)$ to the class of the quotient $\mathcal{O}_S^{n+1} \to \mathcal{O}_S$, $(f_0, \ldots, f_n) \mapsto a_0f_0 + \cdots + a_nf_n$. (Here we use the Grassmannian interpretation of $\mathbb{P}^n$; see section 1). (Verify that the the map $\mathcal{O}_S^{n+1} \to \mathcal{O}_S$ is indeed surjective.) The A-group scheme $G := \mathbb{G}_{\mathrm{m}\,A}$ acts on Y, as follows. For S an A-scheme, for t in $G(S)$ and $(a_0, \ldots, a_n)$ in $Y(S)$, we put $t(a_0, \ldots, a_n) = (ta_0, \ldots, ta_n)$. Then $p\colon Y \to X$ is the quotient by the action of G in the sense that for every A-scheme S, the sheaf on S (for the Zariski topology) associated to the presheaf $U \mapsto Y(U)/G(U)$ is $U \mapsto X(U)$. (This is explained by the fact that $p\colon Y \to X$ has sections locally for the Zariski topology. Usually, quotients by group actions do not have this property.) The action of G on Y is free in the sense that for every A-scheme S, the action by $G(S)$ on $Y(S)$ is free. All this makes Y into a G_X-torsor over X: on $D_+(x_0) \subset X$, for example, the section $(a_1, \ldots, a_n) \mapsto (1 : a_1 : \cdots : a_n)$ of p induces an isomorphism between Y and G_X that translates the G_X-action on Y into the G_X-action on itself by translations. It follows that the category of $\mathcal{O}_X$-modules is equivalent to that of $\mathcal{O}_Y$-modules with G_X-action. (To a $\mathcal{O}_Y$-module $\mathcal{F}$ with G_X-action one associates the $\mathcal{O}_X$-module $U \mapsto (\mathcal{F}(p^{-1}U))^G$, with ^{G} indicating G-invariants, in the functorial sense: invariant under $G(V)$ after restricting to V, for all V.) Another way to associate a $\mathcal{O}_X$-module to an $\mathcal{O}_Y$-module with G_X-action is to take pullbacks via local sections of p; the G_X-action gives glueing data. This is what explains what happens in the proof of [HarAG, II, Thm. 8.13].

On Y, we have the exact sequence of $\mathcal{O}_Y$-modules:

$$0 \longrightarrow p^*\Omega^1_{X/A} \longrightarrow \Omega^1_{Y/A} \longrightarrow \Omega^1_{Y/X} \longrightarrow 0.$$

(See [HarAG, II, Prop. 8.11]; the exactness at the left follows from the existence of local sections.) The $\mathcal{O}_Y$-modules $\Omega^1_{Y/A}$ and $\Omega^1_{Y/X}$ are free, with bases $(dx_0, \ldots, dx_n)$ and "$x_0^{-1}dx_0 = \cdots x_n^{-1}dx_n$", respectively. The exact sequence is G_X-equivariant, hence induces an exact sequence of $\mathcal{O}_X$-modules. That is the desired sequence. One gets $\mathcal{O}_X(-1)$'s in the middle, because of the identies $d(tx_i) = tdx_i$. One gets $\mathcal{O}_X$ at the right because of $d(tx_i)/(tx_i) = dx_i/x_i$.

3.3.7 Theorem. *([HarAG, III, Thm. 5.2]) Let X be a projective scheme over a noetherian ring A, and let $\mathcal{O}_X(1)$ be a very ample invertible sheaf on X over* $\mathrm{Spec}(A)$. *Let $\mathcal{F}$ be a coherent $\mathcal{O}_X$-module. Then:*

1. *for each $i \geq 0$, $\mathrm{H}^i(X, \mathcal{F})$ is a finitely generated A-module.*
2. *there is an integer n_0 such that, for all $n \geq n_0$ and all $i > 0$, $\mathrm{H}^i(X, \mathcal{F}(n)) = 0$.*

Before we way anything about the proof of this theorem, let us explain a few terms in the statement of it. First of all, a morphism of schemes $f\colon X \to S$ is called quasi-projective if X, viewed as S-scheme, is isomorphic to a subscheme of $\mathbb{P}^n_S$, for some n; it is called projective if X is isomorphic, as S-scheme, to a closed subscheme of some $\mathbb{P}^n_S$ (see [HarAG, II, §4]; as remarked there, this definition is not equivalent to Grothendieck's, but it is when S is quasi-projective (with Hartshorne's definition), over some affine scheme). An invertible $\mathcal{O}_X$-module on an S-scheme is called very ample if it is isomorphic to one of the form $i^*\mathcal{O}_{\mathbb{P}^n_S}(1)$, with $i\colon X \to \mathbb{P}^n_S$ an immersion of S-schemes. One can phrase this more intrinsically, using the description of $\mathbb{P}^n_S$ as functor: an invertible $\mathcal{O}_X$-module is very ample (relative to S, one should say), if it has a finite number of global sections that generate it and that define an immersion of X into the corresponding projective space over S (see [HarAG, II, §7]).

3.3.8 Exercise. Let A be a ring. Show that the morphism of A-schemes from $\mathbb{P}^1_A$ to $\mathbb{P}^2_A$ given by $\mathcal{O}_{\mathbb{P}^1_A}(2)$ with the sections x_0^2, x_0x_1 and x_1^2 defines an isomorphism with the closed subscheme $V(x_1^2 - x_0x_2)$ of $\mathbb{P}^2_A$.

Let A be a ring. Let X denote the A-scheme $\mathbb{P}^1_A \times_A \mathbb{P}^1_A$, with its two projections pr_1 and pr_2 to $Y := \mathbb{P}^1_A$. Show that the invertible $\mathcal{O}_X$-module $\mathrm{pr}_1^*\mathcal{O}_Y(1) \otimes_{\mathcal{O}_X} \mathrm{pr}_2^*\mathcal{O}_Y(1)$ with its sections $x_0 \otimes x_0$, $x_0 \otimes x_1$, $x_1 \otimes x_0$ and $x_1 \otimes x_1$ give an isomorphism from X to the closed subscheme $V(x_0x_3 - x_1x_2)$ of $\mathbb{P}^3_A$. Hint: just show that an inverse exists locally on $V(x_0x_3 - x_1x_2)$. This explains that it is easy to construct the hyperboloid strucures that one always sees next to nuclear power plants, using concrete armed with straight iron rods: there are two families of straight lines on such things. By the way, these surfaces, over the reals, are minimal in the sense that they minimize surface area among all surfaces passing through two horizontal circles with centers on the z-axis. This seems to imply that they are very good for cooling.

Let us now get back to the proof of the last theorem above. We'll just mention what kind of techniques are involved in it. First of all, since there is a closed immersion $i\colon X \to \mathbb{P}^n_A$, it suffices to treat the case $X = \mathbb{P}^n_A$, since the cohomology of an $\mathcal{O}_X$-module is the same as that of its direct image on $\mathbb{P}^n_A$ (i_* is exact and maps injectives to injectives). So from now $X = \mathbb{P}^n_A$.

For $\mathcal{F}$ a coherent $\mathcal{O}_X$-module there exists a surjection $\mathcal{E} \to \mathcal{F}$, with $\mathcal{E}$ a finite direct sum of $\mathcal{O}_X(r_i)$ (this just uses that for $r \gg 0$, $\mathcal{F}(r)$ is generated by global sections, see [HarAG, II, Thm. 5.17]). Then one has a short exact sequence

$$0 \longrightarrow \mathcal{G} \longrightarrow \mathcal{E} \longrightarrow \mathcal{F} \longrightarrow 0,$$

with $\mathcal{G}$ also a coherent $\mathcal{O}_X$-module. The long exact cohomology sequence reads:

$$\cdots \longrightarrow \mathrm{H}^i(X,\mathcal{E}) \longrightarrow \mathrm{H}^i(X,\mathcal{F}) \longrightarrow \mathrm{H}^{i+1}(X,\mathcal{G}) \longrightarrow \cdots$$

This means that descending induction on i finishes the job (note that, there is a suitable Cech complex whose terms are zero in degrees $> n$).

Since, in this course, we want to define abelian varieties as proper schemes, not necessarily projective, we also need some finiteness results for proper morphisms (abelian varieties will turn out to be projective, so one could say "why bother?", but I find that very unsatisfactory, and, anyway, abelian schemes are not necessarily projective).

3.3.9 Theorem. *([GrDiEGA, III, Thm. 3.3.2]) Let A be a noetherian ring, let X/A be proper, and $\mathcal{F}$ a coherent $\mathcal{O}_X$-module. Then the $\mathrm{H}^i(X,\mathcal{F})$ are finitely generated A-modules for all $i \geq 0$.*

As with the preceding theorem, we only mention what goes into the proof. First of all, in order to relate proper and projective, one applies "Chow's Lemma" ([HarAG, II, Exer. 4.10]). Secondly, one uses the Leray spectral sequence, that relates, for $f\colon X \to Y$ a morphism of ringed spaces, and $\mathcal{F}$ an $\mathcal{O}_X$-module, the $\mathrm{H}^n(X,\mathcal{F})$ to the $\mathrm{H}^p(Y, \mathrm{R}^q f_*\mathcal{F})$. More precisely, each $\mathrm{H}^n(X,\mathcal{F})$ has a filtration whose successive quotients are expressed in terms of the $\mathrm{H}^p(Y, \mathrm{R}^q f_*\mathcal{F})$ and suitable morphisms between those. For details about spectral sequences, see for example [LaA], or [GeMaHA]. In order to get the information one needs out of this spectral sequence, one applies the last part of the preceding theorem, and one performs a "dévissage" in the category of coherent $\mathcal{O}_X$-modules.

4 February 12, 1999

4.1 Curves over fields.

Let k be a field, and $k \to \overline{k}$ an algebraic closure. A curve over k will be a k-scheme that is locally of finite type and everywhere of dimension one. A k-scheme X is said to be geometrically irreducible if $X_{\overline{k}}$ is irreducible (the same terminology applies to notions such as geometrically integral, etc.). For the notion of smoothness of a morphism of schemes we refer to Le Stum's course. Let it suffice to say that $f\colon X \to Y$ is smooth if and only if locally on X and Y it is of the form $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ with B of the form $A[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$, with $\Omega^1_{B/A}$ free of rank $n - m$ as B-module (this last condition is equivalent to the jacobian matrix J with $J_{i,j} = \partial_i f_j$ having rank m everywhere on $\mathrm{Spec}(B)$). Whether a morphism of schemes is smooth or not can also be formulated purely in terms of X viewed as a functor on Y-schemes. In [HarAG] smooth morphisms are not very well treated; in fact, the notion of smoothness is defined only for schemes that are of finite type over a field, which is not good in order to apply algebraic geometry to arithmetic. For k a field, a k-scheme X that is locally of finite type is smooth if and only if $X_{\overline{k}}$ is non-singular in the sense that its local rings are regular. In particular, smooth k-schemes are geometrically reduced.

In this section we will study proper smooth geometrically irreducible curves over fields. Let us first give some examples. One can remark that for X smooth over a field k, the conditions of being geometrically irreducible, geometrically integral, or geometrically connected are all equivalent.

4.1.1 Example. Let k be a field, $d \geq 1$, $F \in k[x_0, x_1, x_2]_d$ such that $V(F, \partial_0 F, \partial_1 F, \partial_2 F) \subset \mathbb{P}^2_k$ is empty. Then $V(F)$ is a proper smooth geometrically irreducible curve over k. (Hint: use Bezout.)

If $k \to k'$ is a nontrivial finite extension of fields, and X a non-empty k'-scheme, then X, viewed as a k-scheme is not smooth and geometrically irreducible. Namely, for it to be geometrically irreducible, $k \to k'$ has to be purely inseparable, and for it to be smooth, $k \to k'$ has to be separable (see [HarAG, II, exer. 3.15]). For example, $\mathbb{P}^1_{\mathbb{Q}(i)}$ is not geometrically orreducible as $\mathbb{Q}$-scheme.

4.1.2 Proposition. *Let k be a field, and X a non-empty proper, smooth and geometrically irreducible k-scheme. Then $\mathcal{O}_X(X) = k$.*

Proof. Let $k \to \overline{k}$ be an algebraic closure. We first claim that $\mathcal{O}_{X_{\overline{k}}}(X_{\overline{k}}) = \overline{k} \otimes_k \mathcal{O}_X(X)$. Indeed, this follows from the fact that one can compute $\mathcal{O}_X(X)$ from the Cech complex given by a finite cover by open affines; tensoring this complex over k by $\overline{k}$ gives the corresponding complex for $X_{\overline{k}}$. Then one uses that $\overline{k} \otimes_k \cdot$ is exact. This reduces the proof to the case where k is algebraically closed.

So now k is algebraically closed. Let f be in $\mathcal{O}_X(X)$. We view $\mathcal{O}_X(X)$ as $\mathrm{Hom}_{k-\mathrm{Sch}}(X, \mathbb{A}^1_k)$. Let $\overline{f}\colon X \to \mathbb{P}^1_k$ be the composition of f with the inclusion of $\mathbb{A}^1_k$ into $\mathbb{P}^1_k$. Since X/k is proper, $\overline{f}X$ is closed in $\mathbb{P}^1_k$. It is also contained in $\mathbb{A}^1_k$, and irreducible. Hence it is a closed point, x say. Since k is algebraically closed, $k(x) = k$. Since X is reduced, f factors through $x\colon \mathrm{Spec}(k) \to X$, hence f is in k. □

Our next objective is to show that the kind of curves that we study are actually projective. This is something special about curves; the corresponding statement for higher dimensions is false, see for example [HarAG, II, 4.10.2].

4.1.3 Proposition. *Let X/k be a proper, smooth and geometrically irreducible curve. Then X/k is projective.*

We will not give a detailed proof of this result. One can obtain a proof by adapting [HarAG, I, Thm. 6.9]. In that case, one covers X by finitely many non-empty affine open subsets $U_i = \mathrm{Spec}(A_i)$. Each U_i admits a closed immersion into some $\mathbb{A}^{n_i}_k$. These closed immersions extend uniquely to morphisms $f_i\colon X \to \mathbb{P}^{n_i}_k$, since the local rings of $\mathcal{O}_X$ at the finitely many points in $X - U_i$ are discrete valuation rings. The f_i give a morphism f from X to the product $\mathbb{P}$ of all $\mathbb{P}^{n_i}_k$. Since X/k us proper, the image of f is closed. Since f is an immersion on each U_i, it is a closed immersion. Another strategy would be to prove that there exists a finite morphism $f\colon X \to \mathbb{P}^1_k$, and then deduce the projectiveness of X from this.

Anyway, it is also very useful to know about the correspondence between (irreducible smooth projective) curves and function fields. For details, see [HarAG, I, §6]. Formulated in our context, this gives the following.

4.1.4 Theorem. *Let k be a field. The contravariant functor that associates, to each proper smooth geometrically irreducible curve X over k its function field $k(X) := k(\eta_X)$ (with η_X the generic point of X) induces an anti-equivalence of categories between that of projective smooth geometrically irreducible curves over k, with non-constant morphisms, and that of finitely generated field extensions $k \to K$ of transcendence degree one with the property that $\overline{k} \otimes_k K$ is a field. (Here, $k \to \overline{k}$ is an algebraic closure.)*

Let us just give a description of how one associates a curve to an extension $k \to K$. To do this, one has to understand how to recover X from $k(X)$. First one tries to recover the set X, then the topology on it, and then the sheaf $\mathcal{O}_X$. The set X is the disjoint union of $\{\eta_X\}$ and the set of closed points of X. Let x be a closed point of X. The local ring $\mathcal{O}_{X,x}$ is then discrete valuation ring, i.e., one has a map $v_x\colon k(X)^* \to \mathbb{Z}$ that sends f to its order at x. One proves that each discrete valuation $v\colon k(X)^* \to \mathbb{Z}$ that is trivial on k^* is necessarily one of the v_x. So let now $k \to K$ be as in the theorem. Let V be the disjoint union of the set $\{\eta\}$ with the set V^0 of all discrete valuations $v\colon k(X)^* \to \mathbb{Z}$ that are trivial on k^*. Equip V with the Zariski topology: the closed sets are the finite subsets of V^0, and the set V itself. Equip this with a sheaf $\mathcal{O}_V$: for each open $U \subset V$ one puts

$$\mathcal{O}_V(U) := \{f \in K \mid v(f) \geq 0 \text{ for all } v \text{ in } V^0 \cap U\}.$$

One proves that $(V, \mathcal{O}_V)$ is a projective, smooth and geometrically irreducible curve over k.

4.2 Divisors and line bundles.

We will not develop a general theory of divisors here; if one is interested in that, one should see [HarAG, II, §6]. Instead, we just do what we need for proper, smooth geometrically irreducible curves.

So let X be a proper, smooth and geometrically irreducible curve over some field k. We let X^0 denote the set of closed points of X. Then we define the group $\mathrm{Div}(X)$ of divisors on X to be the free $\mathbb{Z}$-module with basis X^0:

$$\mathrm{Div}(X) := \oplus_{x \in X^0} \mathbb{Z} = \mathbb{Z}^{(X_0)} \subset \mathbb{Z}^{X_0}.$$

We will view $\mathrm{Div}(X)$ as the $\mathbb{Z}$-module of $\mathbb{Z}$-valued functions on X^0 with finite support, but we will also write divisors as formal linear combinations of elements of X^0. Of course, as group alone this construction is of no interest. Divisors are interesting because they are related to rational functions and to invertible $\mathcal{O}_X$-modules, as we will see now. First of all, we have a map "degree" from $\mathrm{Div}(X)$ to $\mathbb{Z}$:

$$\deg\colon \mathrm{Div}(X) \longrightarrow \mathbb{Z}, \quad D \mapsto \sum_{x \in X^0} D(x) \dim_k(k(x)).$$

The factor $\dim_k(k(x))$ means that the closed point x counts as $\dim_k(k(x))$ k-rational points, which makes sense if one performs a base change to an algebraically closed field.

We have a morphism of groups that associates to non-zero rational functions a divisor:

$$\mathrm{div}\colon k(X)^* \longrightarrow \mathrm{Div}(X), \quad f \mapsto (x \mapsto v_x(f)).$$

The image of this map is called the group of principal divisors. One can also associate to a divisor D an invertible $\mathcal{O}_X$-module $\mathcal{O}_X(D)$ as follows (I'm sorry for the notation $\mathcal{O}_X(D)$; [HarAG] uses $\mathcal{L}(D)$, but that is not better):

$$(\mathcal{O}_X(D))U = \{f \in k(X) \mid \text{for all closed } x \text{ in } U\colon\ v_x(f) + D(x) \geq 0\}.$$

For D_1 and D_2 in $\mathrm{Div}(X)$, one has an isomorphism:

$$\mathcal{O}_X(D_1) \otimes_{\mathcal{O}_X} \mathcal{O}_X(D_2) \xrightarrow{\sim} \mathcal{O}_X(D_1 + D_2), \quad f_1 \otimes f_2 \mapsto f_1 f_2.$$

The definition of $\mathcal{O}_X(D)$ implies immediately that for x in X^0 one has $\mathcal{O}_X(-x) = I_x$, the subsheaf of ideals of $\mathcal{O}_X$ corresponding to the closed immersion $i\colon \mathrm{Spec}(k(x)) \to X$ given by the exact sequence:

$$0 \longrightarrow I_x \longrightarrow \mathcal{O}_X \longrightarrow i_* k(x) \longrightarrow 0.$$

Let us note that all $\mathcal{O}_X(D)$ are subsheaves of $\mathcal{O}_X$-modules of the constant sheaf $k(X)_X$. One should add that for D in $\mathrm{Div}(X)$ the invertible $\mathcal{O}_X$-module $\mathcal{O}_X(D)$ is equipped with the given rational section 1 in $\mathcal{O}_X(D)_\eta$; conversely, an invertible $\mathcal{O}_X$-module $\mathcal{L}$ with a non-zero rational section does determine a divisor (see the proof of the theorem below). The following theorem relates divisors to rational functions and invertible line $\mathcal{O}_X$-modules. Recall that the Picard group $\mathrm{Pic}(X)$ of a ringed space $(X, \mathcal{O}_X)$ is defined to be the set of isomorphism classes of invertible $\mathcal{O}_X$-modules, with the tensor product as group law.

4.2.1 Theorem. *Let X be a proper, smooth, geometrically irreducible curve over some field k. Then the sequence*

$$0 \longrightarrow k^* \longrightarrow k(X)^* \xrightarrow{\mathrm{div}} \mathrm{Div}(X) \longrightarrow \mathrm{Pic}(X) \longrightarrow 0$$

is exact, and the degree map from $\mathrm{Div}(X)$ *to* $\mathbb{Z}$ *factors through* $\mathrm{Pic}(X)$.

Proof. Let f be in $k(X)^*$ such that $\mathrm{div}(f) = 0$. Then f is in $\mathcal{O}_X(X)$, hence f is in k, and non-zero, hence in k^*.

Let us show that $\mathrm{Div}(X) \to \mathrm{Pic}(X)$ is surjective. Let $\mathcal{L}$ be an invertible $\mathcal{O}_X$-module. Then we have, for every x in X^0, a map $v_x\colon \mathcal{L}_\eta - \{0\} \to \mathbb{Z}$ given by an arbitrary choice of isomorphism $\mathcal{O}_{X,x} \to \mathcal{L}_x$ of $\mathcal{O}_{X,x}$-modules (this just means that a non-zero rational section of $\mathcal{L}$ has a well-defined order at every x in X^0). This gives a map $\mathrm{div}_\mathcal{L}$ from $\mathcal{L}_\eta - \{0\}$ to $\mathrm{Div}(X)$ that associates to each non-zero rational section s of $\mathcal{L}$ its divisor of zeroes and poles. Take now $s \neq 0$ in $\mathcal{L}_\eta$, and put $D := \mathrm{div}_\mathcal{L}(s)$. Then one has an isomorphism:

$$\mathcal{O}_X(D) \xrightarrow{\sim} \mathcal{L}, \quad f \mapsto fs.$$

Let now D be in $\mathrm{Div}(X)$ such that $\mathcal{O}_X(D)$ is isomorphic to $\mathcal{O}_X$. Choose an isomorphism $\alpha\colon \mathcal{O}_X \to \mathcal{O}_X(D)$, and let $f := \alpha(1)$ in $\mathcal{O}_X(D)(X)$. Then one has:

$$0 = \mathrm{div}_{\mathcal{L}}(f) = \mathrm{div}(f) + D,$$

hence $D = \mathrm{div}(f^{-1})$. Finally, let f be in $k(X)^*$, and let $D := \mathrm{div}(f)$. Then one has

$$\mathcal{O}_X \xrightarrow{\sim} \mathcal{O}_X(D), \quad g \mapsto gf^{-1}.$$

The fact that the degree map factors through the Picard groups will be shown below. $\square$

4.3 Riemann-Roch, weak version.

We can now state a weak version of the famous theorem of Riemann and Roch. We call it a weak version because it involves an H^0 and an H^1; a much more useful version is the one that we will see later, replacing the H^1 by the dual of an appropriate H^0 (Serre duality). Of course, Riemann and Roch did not state their theorem with an H^1.

Let us introduce some notation. For $\mathcal{F}$ a sheaf of $\mathcal{O}_X$-modules on a ringed space $(X, \mathcal{O}_X)$ with $\mathcal{O}_X$ a sheaf of k-algebras for some field k, with the property that $\mathrm{H}^i(X, \mathcal{F})$ has finite k-dimension for all i and is zero for almost all i, we define the Euler characteristic $\chi(\mathcal{F})$ by:

$$\chi(\mathcal{F}) := \sum_{i \geq 0} (-1)^i \dim_k \mathrm{H}^i(X, \mathcal{F}).$$

The importance of this notion is that it behaves very well with respect to short exact sequences. If

$$0 \longrightarrow \mathcal{F}' \longrightarrow \mathcal{F} \longrightarrow \mathcal{F}'' \longrightarrow 0$$

is a short exact sequence, with all three sheaves satisfying the hypotheses above, then the long exact cohomology sequence gives:

$$\chi(\mathcal{F}) = \chi(\mathcal{F}') + \chi(\mathcal{F}'').$$

For X a proper, smooth, geometrically irreducible curve over a field k, and $\mathcal{F}$ a coherent $\mathcal{O}_X$-module, the $\mathrm{H}^i(X, \mathcal{F})$ are finite dimensional k-vector spaces. Since X is projective, X can be covered by 2 open affines (just embed X into some $\mathbb{P}^n_k$, and take the complements of two suitably chosen hypersurfaces). Then the $\mathrm{H}^i(X, \mathcal{F})$ are calculated by a Cech complex that is concentrated in degrees zero and one. Hence all $\mathrm{H}^i(X, \mathcal{F})$ with $i > 1$ are zero, hence $\chi(\mathcal{F}) = \dim_k(\mathrm{H}^0(X, \mathcal{F})) - \dim_k \mathrm{H}^1(X, \mathcal{F})$.

4.3.1 Theorem. *(Riemann-Roch, weak version.) Let X be a proper, smooth, geometrically irreducible curve over a field k. Then for every D in $\mathrm{Div}(X)$ one has:*

$$\chi(\mathcal{O}_X(D)) = \deg(D) + \chi(\mathcal{O}_X).$$

Proof. Note that the formula is true for $D = 0$. Let P be a closed point of X, and $i \colon \mathrm{Spec}(k(P)) \to X$ the corresponding closed immersion. Then we have the exact sequence:

$$0 \longrightarrow I_P \longrightarrow \mathcal{O}_X \longrightarrow i_*k(P) \longrightarrow 0.$$

Now let D be in $\mathrm{Div}(X)$. Since $\mathcal{O}_X(D)$ is locally free as $\mathcal{O}_X$-module, tensoring over $\mathcal{O}_X$ with $\mathcal{O}_X(D)$ is exact, hence we get the exact sequence:

$$0 \longrightarrow \mathcal{O}_X(D-P) \longrightarrow \mathcal{O}_X(D) \longrightarrow i_*i^*\mathcal{O}_X(D) \longrightarrow 0.$$

Now note that $i^*\mathcal{O}_X(D)$ is a one-dimensional $k(P)$-vector space, hence a k-vector space of dimension $\dim_k k(P)$. The long exact cohomology sequence then shows that the Riemann-Roch formula is true for D if and only if it is true for $D - P$. Induction on $\sum_x |D(x)|$ finishes the proof. $\square$

4.3.2 Corollary. *Let X be a proper, smooth, geometrically irreducible curve over a field k. The map $\deg \colon \mathrm{Div}(X) \to \mathbb{Z}$ factors through $\mathrm{Div}(X) \to \mathrm{Pic}(X)$, i.e., the degree of a divisor depends only on the isomorphism class of $\mathcal{O}_X(D)$. Equivalently, the degree of a principal divisor is zero. For every invertible $\mathcal{O}_X$-module $\mathcal{L}$ one has:*

$$\chi(\mathcal{L}) = \deg(\mathcal{L}) + \chi(\mathcal{O}_X).$$

To finish this section, let us look a bit at the number $\chi(\mathcal{O}_X)$ that appears in the Riemann-Roch formula. Since $\mathcal{O}_X(X) = k$, it is $1 - \dim_k(\mathrm{H}^1(X, \mathcal{O}_X)$. We define the genus of X to be $\dim_k(\mathrm{H}^1(X, \mathcal{O}_X)$. We will show that this is compatible to the topologically defined genus if $k = \mathbb{C}$, and also equal to $\dim_k \Omega^1_{X/k}(X)$.

4.3.3 Exercise. Try to compute the genus of some curves, and try to show that it is equal to $\dim_k \Omega^1_{X/k}(X)$ and to the topological genus. For example, for a smooth plane curve of degree d the genus is $(d-1)(d-2)/2$.

5 February 19, 1999

5.1 Serre duality for line bundles.

Let X be a smooth proper geometrically irreducible curve over a field k. Then Serre's duality states that for invertible $\mathcal{O}_X$-modules $\mathcal{L}$ there are isomorphims

$$\mathrm{H}^1(X,\mathcal{L}) \xrightarrow{\sim} \mathrm{H}^0(X,\Omega^1_{X/k}\otimes\mathcal{L}^\vee)^\vee,$$

functorial in $\mathcal{L}$ and functorial, in a certain way, under morphisms of curves. One way this can be proved is as follows (we just sketch the approach). There are natural pairings:

$$\mathrm{H}^1(X,\mathcal{L})\times\mathrm{H}^0(X,\Omega^1_{X/k}\otimes\mathcal{L}^\vee)\longrightarrow\mathrm{H}^1(X,\Omega^1).$$

One wants to prove that $\mathrm{H}^1(X,\Omega^1)$ is one-dimensional, and in some sense canonically isomorphic to k. After that one wants to prove that the pairings above are perfect. One "computes" $\mathrm{H}^1(X,\Omega^1)$ via the short exact sequence (see [HarAG, III, 7.14∗]):

$$0\to\Omega^1\longrightarrow\Omega^1_{k(X)/k,X}\longrightarrow\bigoplus_{x\in X^0} i_{x,*}(\Omega^1_{k(X)/k}\Omega^1_x)\longrightarrow 0,$$

with $\Omega^1_{k(X)/k,X}$ the constant sheaf on X with stalk the $k(X)$-module of differentials of the function field $k(X)$ over k. Since $\Omega^1_{k(X)/k,X}$ is constant, and X irreducible, it is flasque, hence it has trivial H^1. So one has the exact sequence:

$$\Omega^1_{k(X)/k}\longrightarrow\bigoplus_{x\in X^0} i_{x,*}(\Omega^1_{k(X)/k}/\Omega^1_x)\longrightarrow\mathrm{H}^1(X,\Omega^1)\longrightarrow 0,$$

giving a quite explicit description of $\mathrm{H}^1(X,\Omega^1)$ as a cokernel. Then one introduces residues to see that k is also a cokernel. Let us describe these residues. So let x be in X^0, and let t be a uniformizer at x, i.e., an element of $m_x\subset\mathcal{O}_{X,x}$ such that dt is a basis of the $\mathcal{O}_{X,x}$ module Ω^1_x (if $k(x)$ is a separable extension of k it suffices that t be a generator of m_x). Then the $t^{-n}dt$ with $n\geq 1$ form a $k(x)$-basis of $\Omega^1_{k(X)/k}/\Omega^1_x$. The residue at x of an element ω of $\Omega^1_{k(X)/k}$ is then $\mathrm{tr}_{k(x)/k}(a_{-1})$, where $\mathrm{tr}_{k(x)/k}$ is the trace from $k(x)$ to k, and a_{-1} the coefficient of $t^{-1}dt$ of the class of ω in $\Omega^1_{k(X)/k}/\Omega^1_x$; of course, one has to show that this does not depend on the choice of t. Over the complex numbers, this independence is clear, since the residue of ω at x is the integral of ω along a small oriented loop around x, divided by $2\pi i$; in the general case, one has to work. Anyway, one proves that the sequence:

$$\Omega^1_{k(X)/k}\longrightarrow\bigoplus_{x\in X^0} i_{x,*}(\Omega^1_{k(X)/k}/\Omega^1_x)\longrightarrow k\longrightarrow 0,$$

given by the sum of the residues at all x in X^0, is exact, giving indeed an isomorphism between k and $\mathrm{H}^1(X,\Omega^1)$. Remains the perfectness of the pairings. This too requires a non-trivial proof, see for example [SeGA].

5.2 Duality on $\mathbb{P}^1_k$.

We will follow the proof of Serre duality that is given in [HarAG, III, §7], with the modification that we will use a finite morphism of X to $\mathbb{P}^1_k$ in stead of a closed immersion into some $\mathbb{P}^n_k$. A detailed proof without too much technicalities using this approach is given in [Li]. The approach itself is due to Grothendieck, and one of its main ideas is simply that the functor $\mathcal{F} \mapsto \mathrm{H}^1(X, \mathcal{F})^\vee$, from the category coh-$\mathcal{O}_X$-Mod of coherent $\mathcal{O}_X$-modules to k-vector spaces is represented by Ω^1_X. (Indeed, for $\mathcal{L}$ an invertible $\mathcal{O}_X$-module, one has $\mathrm{H}^0(X, \Omega^1 \otimes \mathcal{L}^\vee) = \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{L}, \Omega^1)$.) We will first prove this representability result for $Y := \mathbb{P}^1_k$. Recall that we have seen that $\Omega^1_{Y/k}$ is isomorphic to $\mathcal{O}(-2)$ (we did fix an isomorphism), and that we gave an isomorphism from k to $\mathrm{H}^1(Y, \Omega^1)$.

5.2.1 Theorem. *Let $Y := \mathbb{P}^1_k$. The canonical pairings:*

$$\mathrm{H}^1(Y, \mathcal{F}) \times \mathrm{Hom}_{\mathcal{O}_Y}(\mathcal{F}, \Omega^1) \longrightarrow \mathrm{H}^1(X, \Omega^1) \xrightarrow{\sim} k$$

are perfect for all coherent $\mathcal{O}_X$-modules $\mathcal{F}$; in particular, they induce isomorphisms

$$\mathrm{Hom}_{\mathcal{O}_Y}(\mathcal{F}, \Omega^1) \xrightarrow{\sim} \mathrm{H}^1(Y, \mathcal{F})^\vee.$$

Proof. We have seen that this is true for $\mathcal{F}$ of the form $\mathcal{O}(n)$, $n \in \mathbb{Z}$. For general $\mathcal{F}$, take a presentation $\mathcal{E}_1 \to \mathcal{E}_0 \to \mathcal{F} \to 0$, with $\mathcal{E}_0$ and $\mathcal{E}_1$ finite direct sums of $\mathcal{O}(n_i)$'s. Then, since both $\mathrm{Hom}_{\mathcal{O}_Y}(\cdot, \Omega^1)$ and $\mathrm{H}^1(Y, \cdot)^\vee$ are left exact, the result follows. $\square$

5.3 Existence of a finite morphism to $\mathbb{P}^1_k$.

We want to show that the functor $\mathrm{H}^1(X, \cdot)^\vee$ on the category coh-$\mathcal{O}_X$-Mod is representable. In order to do so, we will use a finite morphism from X to $\mathbb{P}^1_k$, of which we show the existence in this section.

5.3.1 Proposition. *Let X be a smooth proper geometrically irreducible curve over a field k. Then there exists a finite morphism $f\colon X \to Y := \mathbb{P}^1_k$.*

Proof. We have already seen that X/k is projective, hence we can embed X into some $\mathbb{P}^n_k$. We may assume that there is a $n-2$-dimensional hyperplane L in $\mathbb{P}^n_k$ such that $L \cap X$ is empty (take n large enough, if k is finite). Let D be a line in $\mathbb{P}^n_k$ that does not meet L, and let $\pi\colon \mathbb{P}^n_k - L \to D = \mathbb{P}^1_k$ denote the projection. (If $L = V(x_{n-1}, x_n)$ and $D = V(x_0, \ldots, x_{n-2})$, then π sends $(a_0 : \cdots : a_n)$ to $(a_{n-1} : a_n)$.) We claim that the morphism $f\colon X \to \mathbb{P}^1_k$ induced by π is finite. Well, it is affine, as $\pi^{-1}D_+(x_0) = D_+(x_{n-1})$, $\pi^{-1}D_+(x_1) = D_+(x_n)$, and X is closed in $\mathbb{P}^n_k - L$. It is finite since $f_*\mathcal{O}_X$ is coherent (since X/k is projective). $\square$

5.3.2 Remark. Actually, every non constant morphism from X to $\mathbb{P}^1_k$ is finite, see [HarAG, II, Prop. 6.8] for the case $k = \overline{k}$.

5.4 Intermezzo on affine morphisms.

A morphism $f\colon X \to Y$ of schemes is affine if, for every open affine U of Y, $f^{-1}U$ is affine. For $f\colon X \to Y$ to be affine it suffices that there exists an open affine cover of Y of which the inverse image under f of every element in it is affine (see [HarAG, II, Exer 5.17]). In particular, finite morphisms (and hence closed immersions) are affine.

5.4.1 Lemma. *([HarAG, II, Exer. 5.17(e)].) Let $f\colon X \to Y$ be an affine morphism of schemes. Then the functor f_* induces an equivalence from the category* q.c.-$\mathcal{O}_X$-Mod *of quasi-coherent $\mathcal{O}_X$-modules to* q.c.-$f_*\mathcal{O}_X$-Mod, *that of $f_*\mathcal{O}_X$-modules that are quasi-coherent as $\mathcal{O}_Y$-modules. An inverse is given as follows: for $\mathcal{M}$ in* q.c.-$f_*\mathcal{O}_X$-Mod, *one has $\mathcal{M}^\sim$ in* q.c.-$\mathcal{O}_X$-Mod *defined by*

$$\mathcal{M}^\sim|_{f^{-1}U} = \mathcal{M}(U)^\sim,$$

for every affine open U in Y, where $\mathcal{M}(U)$ is considered as $\mathcal{O}_X(f^{-1}U)$-module.

Proof. Observe that we can also view q.c.-$f_*\mathcal{O}_X$-Mod as the category of quasi-coherent $\mathcal{O}_Y$-modules that are equipped with a structure of $f_*\mathcal{O}_X$-module, compatible with $\mathcal{O}_Y \to f_*\mathcal{O}_X$.

Assume that Y is affine, $\mathrm{Spec}(A)$ say, then X is affine too, say $\mathrm{Spec}(B)$. Then q.c.-$\mathcal{O}_X$-Mod is equivalent to B-Mod via $\mathcal{M} \mapsto \mathcal{M}(X)$ and $M \mapsto M^\sim$, and similarly for q.c.-$\mathcal{O}_Y$-Mod and A-Mod. Via these equivalences, f_* is the functor that sends a B-module M to its underlying A-module ${}_AM$, equipped with its structure of B-module. Clearly, associating to an A-module equipped with the structure of B-module just that B-module is an inverse.

Now the general case. On every open affine U of Y we have constructed an inverse of f_*. It suffices to prove that these are compatible with localization, so that the local inverses of f_* can be glued to a global one. The compatibility with localizations is left to the reader. $\square$

5.5 Duality on X.

5.5.1 Theorem. *Let X be a proper smooth geometrically irreducible curve over a field k. The functor $\mathcal{F} \mapsto \mathrm{H}^1(X, \mathcal{F})^\vee$ from* coh-$\mathcal{O}_X$-Mod *to k-vector spaces is representable.*

Proof. Let $f\colon X \to Y := \mathbb{P}^1_k$ be a finite morphism. We define a coherent $\mathcal{O}_X$-module ω_X as follows. Note that $\mathbf{Hom}_{\mathcal{O}_Y}(f_*\mathcal{O}_X, \Omega^1_Y)$ is a coherent $f_*\mathcal{O}_X$-module. (For $\mathcal{F}$ and $\mathcal{G}$ sheaves on a topological space X, $\mathbf{Hom}(\mathcal{F}, \mathcal{G})$ is the sheaf $U \mapsto \mathrm{Hom}_U(\mathcal{F}|_U, \mathcal{G}|_U)$; see [HarAG, II, Exer. 1.15].) We let ω_X be the coherent $\mathcal{O}_X$-module that corresponds to it via the equivalence given above (so $\omega_X = (\mathbf{Hom}_{\mathcal{O}_Y}(f_*\mathcal{O}_X, \Omega^1_Y))^{\sim}$). Now consider the following diagram of categories:

$$\begin{tikzcd}
\text{coh-}\mathcal{O}_X\text{-Mod} \arrow[r, "\mathbf{Hom}_{\mathcal{O}_X}(\cdot,\omega_X)"] \arrow[d, "f_*"'] & \text{coh-}\mathcal{O}_X\text{-Mod} \arrow[d, "f_*"] \\
\text{coh-}\mathcal{O}_Y\text{-Mod} \arrow[r, "\mathbf{Hom}_{\mathcal{O}_Y}(\cdot,\Omega^1_Y)"] \arrow[d, "\mathrm{H}^1(Y,\cdot)"'] & \text{coh-}\mathcal{O}_Y\text{-Mod} \arrow[d, "\mathrm{H}^0(Y,\cdot)"] \\
k\text{-Mod} \arrow[r, "\mathrm{Hom}_k(\cdot,k)"] & k\text{-Mod}
\end{tikzcd}$$

We claim that both squares in the diagram are commutative, in the sense that we do have an isomorphism between the two functors from their upper left to their lower right corners. For the lower square, this is just rephrasing the duality on $\mathbb{P}^1_k$ that we have seen above. So look at the upper square. To get an isomorphism of functors here, it is sufficient to have isomorphisms on open affines that glue. But that is simple, since on open affines this becomes the fact that, for $A \to B$ a morphism of rings, M a B-module and N an A-module, one has:

$$\mathrm{Hom}_A({}_AM, N) = {}_A(\mathrm{Hom}_B(M, \mathrm{Hom}_A(B, N))),$$

i.e., that the functor $M \mapsto {}_AM$ is a left-adjoint of $N \mapsto \mathrm{Hom}_A(B, N)$.

Now note that $\mathrm{H}^1(Y, \cdot) \circ f_*$ is just $\mathrm{H}^1(X, \cdot)$ (use for example [HarAG, III, Exer 8.2]), and that $\mathrm{H}^0(Y, \cdot) \circ f_* \circ \mathbf{Hom}_{\mathcal{O}_X}(\cdot, \omega_X)$ is just $\mathrm{Hom}_{\mathcal{O}_X}(\cdot, \omega_X)$. □

5.6 The dualizing sheaf is given by the differentials.

(This section is "Hors cours", since it uses spectral sequences and talks about derived categories.) So now we know that the functor $\mathcal{F} \mapsto \mathrm{H}^1(X, \mathcal{F})^\vee$ is representable, by some coherent $\mathcal{O}_X$-module ω_X. Of course, this determines ω_X up to unique isomorphism. We would like to see now that ω_X is isomorphic to Ω^1_X, and that there is a unique isomorphism that corresponds to the residue map from $\mathrm{H}^1(X, \Omega^1)$ to k. On $\mathbb{P}^1_k$, one easily checks that this is so. On X, one can use the construction of ω_X given above to do the checking, but that is not very easy (it amounts to see that two so-called differents of $f\colon X \to Y$ are equal; see [Li]). A more satisfying way to prove what we want is to use more directly that we know the functor that ω_X represents.

The proof I want to give starts with the following observation that the functor $\mathrm{H}^1(X,\cdot)$ is part of a δ-functor (see [HarAG, III, §1] for this notion). Namely, for a short exact sequence

$$0 \longrightarrow \mathcal{F}' \longrightarrow \mathcal{F} \longrightarrow \mathcal{F}'' \longrightarrow 0,$$

we have the exact sequence:

$$\begin{aligned} 0 \longrightarrow \mathrm{H}^1(X,\mathcal{F}'')^\vee \longrightarrow \mathrm{H}^1(X,\mathcal{F})^\vee \longrightarrow \mathrm{H}^1(X,\mathcal{F}')^\vee \longrightarrow& \\ \longrightarrow \mathrm{H}^0(X,\mathcal{F}'')^\vee \longrightarrow \mathrm{H}^0(X,\mathcal{F})^\vee \longrightarrow \mathrm{H}^0(X,\mathcal{F}')^\vee \longrightarrow 0,& \end{aligned}$$

obtained by dualizing the usual one. This δ-functor is universal, because $\mathrm{H}^0(X,\mathcal{F})^\vee$ is effaceable: every $\mathcal{F}$ admits a surjection $\mathcal{E} \to \mathcal{F}$ with $\mathrm{H}^0(X,\mathcal{E}) = 0$ (see [HarAG, III, Thm. 1.3A] and the proof of [HarAG, III, Thm. 7.1].) It follows that we have canonical isomorphisms:

$$\mathrm{H}^0(X,\mathcal{F})^\vee \xrightarrow{\sim} \mathrm{Ext}^1_{\mathcal{O}_X}(\mathcal{F},\omega_X),$$

for all coherent $\mathcal{F}$ on X. Using this, we can compute the fibre $\omega_X(x)$ of ω at all x in $X(k)$. Namely, for $\mathcal{F} := x_*k$, we get:

$$\mathrm{Ext}^1_{\mathcal{O}_X}(x_*k,\omega_X) = k, \quad \mathrm{Hom}_{\mathcal{O}_X}(x_*k,\omega_X) = 0. \tag{5.6.1}$$

The second equality implies that $\omega_{X,x}$ is a free $\mathcal{O}_{X,x}$-module. Hence $\mathbf{Hom}_{\mathcal{O}_X}(x_*k,\omega_X) = 0$, and $\mathrm{Ext}^1_{\mathcal{O}_X}(x_*k,\omega_X) = \mathrm{H}^0(X,\mathbf{Ext}^1_{\mathcal{O}_X}(x_*k,\omega_X))$, by the local to global spectral sequence for Ext's. Since x_*k is supported at x, the sheaf $\mathbf{Ext}^1_{\mathcal{O}_X}(x_*k,\omega_X)$ is supported at x too. Hence its rH^0 is the same as its stalk at x. To compute this stalk, one uses the short exact sequence:

$$0 \longrightarrow m_x \longrightarrow \mathcal{O}_{X,x} \longrightarrow x_*k \longrightarrow 0.$$

That gives an exact sequence:

$$\mathrm{Hom}_{\mathcal{O}_{X,x}}(\mathcal{O}_{X,x},\omega_{X,x}) \longrightarrow \mathrm{Hom}_{\mathcal{O}_{X,x}}(m_x,\omega_{X,x}) \longrightarrow \mathrm{Ext}^1_{\mathcal{O}_X}(x_*k,\omega_{X,x}) \longrightarrow 0,$$

from which one easily concludes that $\mathrm{Ext}^1_{\mathcal{O}_X}(x_*k,\omega_{X,x})$ is the same as $(m_x/m_x^2)^\vee \otimes_k \omega_X(x)$ (write $\mathrm{Hom}_{\mathcal{O}_{X,x}}(m_x,\omega_{X,x})$ as $m_x^\vee \otimes_{\mathcal{O}_{X,x}} \omega_{X,x}$; in higher dimension one would use the Koszul resolution to compute the Ext group, see [HarAG, III, Thm. 7.11]). Since $m_x/m_x^2 = \Omega^1_X(x)$, the first equality in (5.6.1) gives us:

$$\omega_X(x) = \Omega^1_X(x),$$

for all x in $X(k)$. Of course, this is a good indication that ω_X and Ω^1_X are isomorphic, but it is no proof. To make this kind of argument into a proof, one should generalize it to work after base change from k to $S := X$ itself, and apply it to the universal point, i.e., the diagonal $P := \Delta_{X/k}\colon S \to X \times_k S$. But then the naive dual $\mathbf{Hom}(\cdot, \mathcal{O}_S)$ on coh-$\mathcal{O}_S$-Mod is not exact, which is a problem. This problem is solved by using derived categories. The fact that ω_{X_S} is dualizing is then expressed by the commutative diagram:

$$\begin{array}{ccc}
\mathrm{D}^b(\text{coh-}\mathcal{O}_{X_S}\text{-Mod}) & \xrightarrow{\mathrm{R}\mathbf{Hom}(\cdot,\omega_{X_S}[1])} & \mathrm{D}^b(\text{coh-}\mathcal{O}_{X_S}\text{-Mod}) \\
{\scriptstyle \mathrm{R}\pi_*}\downarrow & & \downarrow{\scriptstyle \mathrm{R}\pi_*} \\
\mathrm{D}^b(\text{coh-}\mathcal{O}_S\text{-Mod}) & \xrightarrow{\mathrm{R}\mathbf{Hom}(\cdot,\mathcal{O}_S[0])} & \mathrm{D}^b(\text{coh-}\mathcal{O}_S\text{-Mod})
\end{array}$$

(For what these notations really mean, one has to look in [HarRD].) Let us just try to see what happens with our test-sheaf $\mathcal{F} := P_*\mathcal{O}_S$. First of all, we should view $\mathcal{F}$ as a the complex of coherent $\mathcal{O}_X$-modules $\mathcal{F}[0]$, with $\mathcal{F}$ in degree zero, and zero in all other degrees. In order to compute $\mathrm{R}\mathbf{Hom}(\mathcal{F}, \omega_{X_S}[1])$, we view the short exact sequence:

$$0 \longrightarrow I_P \longrightarrow \mathcal{O}_{X_S} \longrightarrow \mathcal{F} \longrightarrow 0$$

as a quasi-isomorphism from the complex $I_P \to \mathcal{O}_{X_S}$, with $\mathcal{O}_{X_S}$ in degree zero, to $\mathcal{F}[0]$. Note that both terms of this complex are locally free, hence acyclic for the $\mathbf{Ext}^i$ with $i > 0$. The definition of derived functors between derived categories tells us that we should apply $\mathbf{Hom}_{\mathcal{O}_{X_S}}(\cdot, \omega_{X_S})$ to this complex. That gives us the complex:

$$\mathbf{Hom}_{\mathcal{O}_{X_S}}(\mathcal{O}_{X_S}, \omega_{X_S}) \longrightarrow \mathbf{Hom}_{\mathcal{O}_{X_S}}(I_P, \omega_{X_S}),$$

with the first term in degree -1 (because of the "1" in $\omega_{X_S}[1]$). A similar argument as above gives that this complex is quasi-isomorphic to $P_*P^*(\Omega^1_{X_S/S} \otimes_{\mathcal{O}_{X_S}} \omega_{X_S})[0]$.

Let's now think of $\mathrm{R}\pi_*\mathcal{F}[0]$. This is easy, since $\mathcal{F}$ is acyclic for the $\mathrm{R}^i\pi_*$ with $i > 0$. (For general $\mathcal{F}$, one could use a Cech complex given by a cover of X by two open affines, in order to get a finite resolution by acyclics.) Hence $\mathrm{R}\pi_*\mathcal{F}[0]$ is the complex $\pi_*\mathcal{F}[0] = \mathcal{O}_S[0]$. In the same way, $(\mathrm{R}\pi_*)P_*P^*(\Omega^1_{X_S/S} \otimes_{\mathcal{O}_{X_S}} \omega_{X_S})[0] = \Omega^1_{X_S/S}(P) \otimes_{\mathcal{O}_S} \omega_{X_S}(P)$. But that tells us:

$$\Omega^1_{X_S/S}(P) \otimes_{\mathcal{O}_S} \omega_{X_S}(P) = \mathcal{O}_S.$$

This finishes the proof, since $S = X$, $\Omega^1_{X_S/S}(P) = \Omega^1_{X/k}$ and $\omega_{X_S}(P) = \omega_X$.

5.7 Some conclusions.

After all these technicalities, let us state the results we want to use, and some direct consequences.

5.7.1 Theorem. *Let X be a proper smooth geometrically irreducible curve over a field k. Let $\mathcal{L}$ be an invertible $\mathcal{O}_X$-module. Then we have:*

$$\mathrm{h}^0(X, \mathcal{L}) - \mathrm{h}^0(X, \Omega^1_{X/k} \otimes_{\mathcal{O}_X} \mathcal{L}^\vee) = \deg(\mathcal{L}) + 1 - g(X),$$

with $g(X) = \mathrm{h}^0(X, \Omega^1_{X/k}) = \mathrm{h}^1(X, \mathcal{O}_X)$.

Applying this to $\mathcal{L} = \Omega^1_{X/k}$, one gets the following.

5.7.2 Corollary.

$$\deg(\Omega^1_{X/k}) = 2g(X) - 2.$$

It follows right from the definitions that $\mathcal{L}(X) \neq 0$ implies $\deg(\mathcal{L}) \geq 0$.

5.7.3 Corollary.

$$\deg(\mathcal{L}) < 0 \Longrightarrow \mathrm{h}^0(X, \mathcal{L}) = 0,$$
$$\deg(\mathcal{L}) > 2g(X) - 2 \Longrightarrow \mathrm{h}^1(X, \mathcal{L}) = 0.$$

6 March 5, 1999

6.1 Hurwitz's formula.

In this section, we prove and give some examples of Hurwitz's formula. We follow more or less [HarAG, IV, §2]. One of our reasons to prove this formula is to prove that, over the complex numbers, the algebraically defined genus (i.e., the dimension of the space of global differential forms) coincides with the topologically defined genus (i.e., the number of handles, or, equivalently, half the dimension of the first singular cohomology group).

Since Hartshorne works over an algebraically closed field k, we will do the same now. This is harmless, since for X a proper smooth geometrically irreducible curve over a field k, and $k \to K$ a field extension, we have $g(X) = g(X_K)$ (use an argument that we have seen in the proof that $\mathrm{H}^0(X, \mathcal{O}_X) = k$ to show that $\mathrm{H}^0(X_K, \Omega^1_{X_K/K}) = K \otimes_k \mathrm{H}^0(X, \Omega^1_{X/k})$). So I repeat, in this section k is algebraically closed.

6.1.1 Definition. Let $f\colon X \to Y$ be a finite morphism of proper smooth and geometrically irreducible curves over k. Then the degree $\deg(f)$ is defined to be the degree of the corresponding field extension $k(Y) \to k(X)$. The morphism f will be called separable if and only if $k(Y) \to k(X)$ is. For P in $X(k)$ we define the ramification index e_P by:

$$e_P := v_P(f^\# t),$$

where $f^\#\colon \mathcal{O}_{Y,fP} \to \mathcal{O}_{X,P}$ is the induced morphism, where t in $\mathcal{O}_{Y,fP}$ is a uniformizer and v_P the valuation at P. It is a simple trivial exercise to verify that the result does not depend on the choice of t. For all P, one has $e_P \geq 1$. The point P is called a ramification point of f if $e_P > 1$.

6.1.2 Proposition. *Let f be as above. A point P in $X(k)$ is ramified if and only if $\Omega^1_{X/Y,P} \neq 0$. For every Q in $Y(k)$ one has:*

$$\sum_{P \in f^{-1}Q} e_P = \deg(f).$$

The morphism $f^*\colon f^*\Omega^1_Y \to \Omega^1_X$ is injective if and only if f is separable. The number of ramification points is finite if f is separable.

Proof. Since f is finite, $f_*\mathcal{O}_X$ is a coherent $\mathcal{O}_Y$-module; inparticular, it is locally of finite type. Since X is integral, and the $\mathcal{O}_{Y,Q}$ discrete valuation rings, $f_*\mathcal{O}_X$ is a locally free $\mathcal{O}_Y$-module of rank $\deg(f)$ (use that a finitely generated module over a discrete valuation ring is isomorphic to the direct sum of a finitely generated torsion module and a free module of finite rank).

Let Q be in $Y(k)$, and let X_Q be the fibre (scheme-theoretic of course) of f over Q, i.e., X_Q is given as the fibred product:

$$\begin{array}{ccc} X_Q & \longrightarrow & X \\ \downarrow & & \downarrow \\ \mathrm{Spec}(k) & \xrightarrow{Q} & Y \end{array}$$

Since f is finite, and $f_*\mathcal{O}_X$ locally free of rank $\deg(f)$ as $\mathcal{O}_Y$-module, we have $X_Q = \mathrm{Spec}(A)$, with A a k-algebra that has dimension $\deg(f)$ as k-vector space. As any such k-algebra, A is the product of its local rings, hence:

$$A = \prod_{P\in f^{-1}Q} A_P.$$

Applying definitions gives $\dim_k A_P = e_P$ (note that A_P is isomorphic to $\mathcal{O}_{X,P}/m_P^{e_P} \cong k[[x]]/(x^{e_P})$. Hence the sum of the e_P equals $\deg(f)$. (See also [HarAG, II, Prop.6.9] for this proof.)

By the basic properties of modules of differentials, $\Omega^1_{X/Y,P}$ is zero if and only if A_P is reduced, i.e., equal to k itself, hence if and only if P is unramified. Let η_X be the generic point of X. Then $\Omega^1_{X/Y,\eta_X}$ is the same as $\Omega^1_{k(X)/k(Y)}$. Now, if $K \to L$ is an algebraic field extension, $\Omega^1_{L/K} = 0$ if and only if $K \to L$ is separable. For example, if $L = K[x]/(f)$, then $\Omega^1_{L/K} = Ldx/L\overline{f'}dx$, which is zero if and only if $\overline{f'} \neq 0$. Now consider the exact sequence:

$$f^*\Omega^1_Y \xrightarrow{f^*} \Omega^1_X \longrightarrow \Omega^1_{X/Y} \longrightarrow 0.$$

Since X and Y are smooth curves, $f^*\Omega^1_Y$ and Ω^1_X are invertible $\mathcal{O}_X$-modules. It follows that f^* is injective if and only if f is separable.

Assume now that f is separable. Then $\Omega^1_{X/Y}$ is a coherent $\mathcal{O}_X$-module, whose stalk at η_X is zero. This implies that its support (which is closed) is a finite set. Hence the number of ramification points is finite. Another way to say this is as follows: take a non-empty affine open U of X on which $f^*\Omega^1_Y$ and Ω^1_X are trivial; then f^* corresponds to multiplication by some non-zero function g on U; but then the ramification points are among the finitely many zeros of g and the finitely many points in the complement of U. $\square$

Suppose from now on that f is separable. Then we have the exact sequence:

$$0 \longrightarrow f^*\Omega^1_Y \xrightarrow{f^*} \Omega^1_X \longrightarrow \Omega^1_{X/Y} \longrightarrow 0.$$

We want to use this sequence to relate the degrees of Ω^1_X and Ω^1_Y to the torsion sheaf $\Omega^1_{X/Y}$. For P in $X(k)$, let $R(P) := \dim_k \Omega^1_{X/Y,P}$, and call R the ramification divisor of f. Another way to express the $R(P)$ is as follows: let t be a uniformizer at $f(P)$, then $R(P) = v_P f^*dt$, with $v_P f^*dt$ the valuation at P of the local section f^*dt of the invertible $\mathcal{O}_X$-module Ω^1_X.

6.1.3 Theorem. *Let $f\colon X \to Y$ be a finite separable morphism between proper smooth irreducible curves over an algebraically closed field k. Then one has:*

$$2g(X) - 2 = \deg(f)\,(2g(Y) - 2) + \deg(R).$$

For P with $e_P \neq 0$ in k, one has:

$$R(P) = e_P - 1.$$

Proof. Apart from the last statement, the proof of this theorem is a direct application of the following two lemmas.

6.1.4 Lemma. *Consider a short exact sequence of $\mathcal{O}_X$-modules*

$$0 \longrightarrow \mathcal{L}' \longrightarrow \mathcal{L} \longrightarrow \mathcal{F} \longrightarrow 0,$$

with $\mathcal{L}'$ and $\mathcal{L}$ invertible. Then $\mathcal{F}$ is a torsion sheaf, and $\deg(\mathcal{L}) = \deg(\mathcal{L}') + \sum_P \dim_k \mathcal{F}_P$.

Proof. We can use the weak version of the theorem of Riemann-Roch. We have, because of the long exact cohomology sequence, plus the fact that $\mathrm{H}^1(X, \mathcal{F}) = 0$ (because $\mathcal{F}$ has support in a zero-dimensional closed subset):

$$\chi(\mathcal{L}) = \chi(\mathcal{L}') + \mathrm{h}^0(X, \mathcal{F}), \quad \text{and} \quad \mathrm{h}^0(X, \mathcal{F}) = \sum_P \dim_k \mathcal{F}_P.$$

Combining this with:

$$\chi(\mathcal{L}) = \chi(\mathcal{O}_X) + \deg(\mathcal{L}), \quad \text{and} \quad \chi(\mathcal{L}') = \chi(\mathcal{O}_X) + \deg(\mathcal{L}')$$

gives the result. One can also prove the result without using Riemann-Roch, as in the proof of [HarAG, IV, Prop. 2.3], but one should not forget that in order to prove the existence of the degree map on $\mathrm{Pic}(X)$, we have used Riemann-Roch. Let us note, by the way, that Prop. 6.1.2 gives a new proof that pricipal divisors have degree zero, by interpreting a non-constant f in $k(X)^*$ as a morphism to $\mathbb{P}^1_k$, and $\mathrm{div}(f)$ as $f^{-1}0 - f^{-1}\infty$. $\square$

6.1.5 Lemma. *For every invertible $\mathcal{O}_Y$-module $\mathcal{L}$, one has* $\deg(f^*\mathcal{L}) = \deg(f)\deg(\mathcal{L})$.

Proof. We know that every invertible $\mathcal{O}_Y$-module $\mathcal{L}$ is isomorphic to some $\mathcal{O}_Y(D)$, with D a divisor on Y. Hence it sufffices to prove the statement for $\mathcal{L} := I_Q = \mathcal{O}_Y(-Q)$, with Q in $Y(k)$. But in that case, $f^*\mathcal{L}$ is the ideal sheaf of the closed subscheme $X_Q = f^{-1}Q$ of X. As we have seen above, $\mathcal{O}_{X_Q}$ is a torsion $\mathcal{O}_X$-module with $\dim_k(\mathcal{O}_{X_Q}) = \deg(f)$. The preceding lemma tells us that $\deg f^*\mathcal{L} = -\deg(f)$, which is what we had to prove. □

Let us now prove the last statement of the theorem. So let P be in $X(k)$, and let Q be its image in $Y(k)$. Let t be a uniformizer at Q, and u be a uniformizer at P. Then we have:

$$f^{\#}t = u^{e_P}g, \quad \text{with} \quad g \in \mathcal{O}_{X,P}^*.$$

It follows that:

$$f^{\#}dt = df^{\#}t = d(u^{e_P}g) = e_P u^{e_P-1}gdu + u^{e_P}dg.$$

Now note that du is an $\mathcal{O}_{X,P}$-basis of $\Omega^1_{X,P}$, and that dg is in $\Omega^1_{X,P}$, so that $u^{e_P}dg$ has valuation at least e_P at P. It follows that if e_P is non-zero in k, then $f^{\#}d$ has valuation $e_P - 1$ at P. □

6.2 First example.

Let us consider the case where $Y = \mathbb{P}^1_k$, $X = V(-Y^2Z + X^3 + aXZ^2 + bZ^3)$ in $\mathbb{P}^2_k$, with k not of characteristic two, and $f\colon X \to Y$ the projection on $V(Y)$ from $(0:1:0)$. In fact, this point lies on X, but since X is a smooth curve, the projection to $\mathbb{P}^1_k$ that is defined outside $(0:1:0)$ extends (as our computation will show anyway).

Let us first study what happens on $D_+(Z)$. We view $D_+(Z)$ as $\mathbb{A}^2_k$, with coordinates $x := X/Z$ and $y := Y/Z$. In these coordinates, our curve X is given by the equation $y^2 = x^3 + ax + b$, and the projection f sends (α, β) to $(\alpha, 0)$ (note that $(\alpha, \beta, 1)$, $(0, 1, 0)$ and $(\alpha, 0, 1)$ are colinear). For a given α, the degree two equation $y^2 = \alpha^3 + a\alpha + b$ describes the fibre of f over $(\alpha, 0)$. It follows that $\deg(f) = 2$. Where is the ramification? Well, exactly at the zeros of the differential form dx. Now note that $2ydy = (3x^2 + a)dx$ on $D_+(Z) \cap X$. Since X is smooth, dx and dy are not both zero at a point of X, hence if dx is zero at P, then y must be zero at P. Vice versa, if y is zero at P, then $3x^2 + a$ is not zero at P because X is smooth ($2y$ and $3x^2 + a$ are the two partial derivatives of the equation of $X \cap D_+(Z)$), hence dx is zero at P. The conclusion is that there are exactly three ramification points in $D_+(Z)$: $(r_1, 0)$, $(r_2, 0)$ and $(r_3, 0)$, with r_1, r_2 and r_3 the three roots of $x^3 + ax + b$ (there are three roots because X is smooth). Since the degree of f is two, each of these three ramification points P_i must have $R(P_i) = 2$. That this is so also follows from the equality:

$$2ydy = (3x^2 + a)dx,$$

since $3x^2 + a$ is not zero at the ramification points, hence is invertible in the corresponding local rings, showing that

$$dx = ygdy$$

with y a uniformizer and g invertible at the ramification points.

Note that $D_+(Z) \cap X$ is all of X except the single point $\infty := (0 : 1 : 0)$. Namely, $V(Z) \cap X$ is given by the equations $Z = 0$ and $X^3 = 0$ (which indicates that $V(Z)$ intersects X with multiplicity three at ∞). To see what happens at ∞, we have to work in $D_+(Y)$ (the only one of the three basic open affines that contains it). We view $D_+(Y)$ as $\mathbb{A}^2_k$ with coordinates $u = X/Y$ and $v = Z/Y$. In those coordinates, X is given by the equation

$$-v + u^3 + au^2v + bv^3 = 0.$$

Note that the u-axis $V(v)$ intersects X at $\infty = (0, 0)$ with multiplicity three, as it should. Hence u is a uniformizer at ∞. The projection f is given, in these coordinates, by $(\alpha, \beta) \mapsto \beta/\alpha$, hence by the function v/u. Now note that v/u has a zero of order two at ∞, since v and u have valutions 3 and 1, respectively. So this shows that indeed f extends at ∞, and that ∞ has ramification index 2. It follows that $R(\infty) = 1$. Now Hurwirz's formula reads:

$$2g(X) - 2 = 2(2g(Y) - 2) + \deg(R) = 2(0 - 2) + 4 = 0,$$

hence $g(X) = 1$.

6.3 Second example.

Let now k be a field of characteristic two. As in the previous example, we consider the projection of a plane curve of degree three from $\infty := (0 : 1 : 0)$ to $\mathbb{P}^1_k = V(Y)$. This time, the curve X is $V(Y^2Z + YZ^2 + X^3)$. The three partial derivatives of $Y^2Z + YZ^2 + X^3$ are X^2, Z^2 and Y^2, hence the curve is smooth. On $D_+(Z)$, the curve is given by the equation $y^2 + y = x^3$, and the projection is as before: $(\alpha, \beta) \mapsto \alpha$. In this case we have: $x^2dx = dy$, which shows that dx has no zero on $D_+(Z) \cap X$. Hence the only possible ramification point is ∞. (By the way, we know in a sense that we must have $R(\infty) = 4$, since X is a plane curve of degree three, hence of genus one.) So let's look at $D_+(Y)$, with the coordinates $u = X/Y$ and $v = Z/Y$. In those coordinates, X is given by $v + v^2 = u^3$. The line $V(v)$ intersects X with multiplicity three in $\infty = (0, 0)$, hence u is a uniformizer at ∞. The projection f is given by the function v/u, as before, which has valuation two at ∞; hence $e_\infty = 2$. The computation of $R(\infty)$ is a bit more involved. In $\mathcal{O}_{X,\infty}$ we have:

$$v = u^3 + v^2 = u^3 + (u^3 + v^2)^2 = u^3 + u^6 + v^4.$$

In the completion $\mathcal{O}_{X,\infty}^\wedge$ we have: $v = \sum_{n\geq 1} u^{3\cdot 2^n}$, but we won't use this (I include it as an example of how one can write every element of $\mathcal{O}_{X,\infty}$ as a formal series in u). Anyway, in $\mathcal{O}_{X,\infty}$ we have:

$$v/u = u^2 + u^5 + u^{11}g,$$

with g in $\mathcal{O}_{X,\infty}^*$. It follows that:

$$d(v/u) = u^4 du + u^{10} g du + u^{11} dg,$$

from which one concludes that $R(\infty) = 4$. Hence $g(X) = 1$, as we should have expected.

6.4 Topological genus equals algebraic genus over $\mathbb{C}$.

Let now $k = \mathbb{C}$. Then Hurwitz's formula reads:

$$2g(X) - 2 = \deg(f)(2g(Y) - 2) + \sum_P (e_P - 1),$$

simply because $\mathbb{C}$ is of characteristic zero. We denote by $g^{\mathrm{top}}(X)$ the topological genus of the complex analytic variety $X(\mathbb{C})$; hence one can view $g^{\mathrm{top}}(X)$ as the number of handles one has to add to the sphere in order to get a surface homeomorphic to $X(\mathbb{C})$, or as half of the dimension of $\mathrm{H}^1(X(\mathbb{C}), \mathbb{Q})$.

6.4.1 Theorem. *Let X be a smooth proper irreducible curve over $\mathbb{C}$. Then $g(X) = g^{\mathrm{top}}(X)$.*

Proof. For $X = \mathbb{P}^1_\mathbb{C}$, the result is clear, since $\mathbb{P}^1(\mathbb{C})$ is homeomorphic to the sphere. (Note that we have computed that $\mathrm{h}^0(\mathbb{P}^1_\mathbb{C}, \Omega^1) = 0$.) Hence it suffices to show that under a finite morphism, g^{top} satisfies Hurwitz's formula. So let $f\colon X \to Y = \mathbb{P}^1_\mathbb{C}$ be a finite morphism of smooth proper irreducible curves over $\mathbb{C}$. Let $P_1, \ldots, P_r$ be its ramification points, and let $Q_1, \ldots, Q_t$ be their distinct images. We triangulate the topological manifold $\mathbb{P}^1(\mathbb{C})$ in such a way that the vertices are among the vertices $\{Q_1, \ldots, Q_t, Q_{t+1}, \ldots, Q_s\}$. (This is not hard; by an automorphism of $\mathbb{P}^1_\mathbb{C}$ one may suppose that ∞ is not the image of a ramification point, and then one can triangulate simply in $\mathbb{C}$, adding ∞ as a vertex if one wants to.) Let U denote $\mathbb{P}^1(\mathbb{C}) - \{Q_1, \ldots, Q_t\}$. The important observation is now that $f\colon f^{-1}U \to U$

is a covering map, in the sense that locally on U, $f\colon f^{-1}U \to U$ is isomorphic to a disjoint union of $\deg(f)$ copies of the base. It follows then that we get a triangulation of $X(\mathbb{C})$ simply by taking the inverse images of the vertices, edges and faces of that of $\mathbb{P}^1(\mathbb{C})$. Let v, e and f be the numbers of vertices, edges and faces of the triangulation of $\mathbb{P}^1(\mathbb{C})$, and let v', e' and f' be those numbers for $X(\mathbb{C})$. Then we have:

$$\begin{aligned} v' &= \deg(f)v - \sum_{i=1}^{r}(e_{P_i} - 1) \\ e' &= \deg(f)e \\ f' &= \deg(f)f \end{aligned}$$

Now one notes that $2g^{\mathrm{top}}(X) - 2$ is minus the Euler characteristic of $X(\mathbb{C})$, hence:

$$2g^{\mathrm{top}}(X) - 2 = -v' + e' - f', \quad \text{and} \quad -2 = 2g^{\mathrm{top}}(\mathbb{P}^1_{\mathbb{C}}) - 2 = -v + e - f.$$

A simple computation finishes the proof. $\square$

7 March 10, 1999

7.1 Explicit computation of a genus.

Let us verify, by an explicit computation, that for $X := V(F) \subset \mathbb{P}^2_k$, with $F = -Y^2Z + X^3 + aXZ^2 + bZ^3$, $4a^3 + 27b^2 \neq 0$, and k not of characteristic two or three, we have $\dim_k(\Omega^1_X(X)) = 1$. Note that until now we have used that $\deg(\Omega^1_X) = 2g(X) - 2$ in order to compute the genus of X, via Hurwitz's formula.

So we first work on $D_+(Z)$. We view $X \cap D_+(Z)$ as the closed subscheme of $D_+(Z) = \mathbb{A}^2_k$ defined by the equation $y^2 = f(x)$, with $f(x) = x^3 + ax + b$, with $x = X/Z$ and $y = Y/Z$. As always, let η be the generic point of X. By the basic properties of the sheaf of differentials, we have:

$$\Omega^1_X(X \cap D_+(Z)) = \frac{k[x,y]dx \oplus k[x,y]dy}{k[x,y](-2ydy + f'(x)dx)}.$$

Hence in $\Omega^1_{X,\eta}$ we have:

$$\omega := \frac{dy}{f'(x)} = \frac{dx}{2y}.$$

Now note that $2y$ and $f'(x)$ have no zero in common on $X \cap D_+(Z)$, since X is smooth over k (use the jacobian criterion). This shows that ω is in $\Omega^1_X(X \cap D_+(Z))$. I claim that ω has no zeros on $X \cap D_+(Z)$. Since the zeros of dx on $X \cap D_+(Z)$ are the zeros of y, it suffices to check that ω has no zero at the zeros of y. But at each of the three zeros of y, dy is a generator, hence $\omega = f'(x)^{-1}dy$ too. So we conclude that ω is a $\mathcal{O}_X$-basis of Ω^1_X on $X \cap D_+(Z)$. Now we check what happpens at the only remaining point: $\infty = (0:1:0)$. There, we work in $D_+(Y) = \mathbb{A}^2_k$ with coordinates $u = X/Y$ and $v = Z/Y$. In these coordinates, $X \cap D_+(Y)$ is given by the equation $-v + u^3 + auv^2 + bv^3$. We have:

$$x = \frac{X}{Z} = \frac{X/Y}{Z/Y} = \frac{u}{v}, \quad \text{and} \quad y = \frac{Y}{Z} = v^{-1}.$$

It follows that $v_\infty(v) = 3$ and $v_\infty(u) = 1$. Hence $v_\infty(x) = v_\infty(u/v) = -2$ and $v_\infty(y) = v_\infty(1/v) = -3$. It follows that:

$$v_\infty(dx) = -3, \quad \text{and} \quad v_\infty(\omega) = v_\infty(dx/2y) = -3 - (-3) = 0.$$

Hence ω has neither a pole nor a zero at ∞. We conclude that ω is an $\mathcal{O}_X$-basis of Ω^1_X. Hence $\dim_k(\Omega^1_X(X)) = 1$, which is what we wanted to prove. Note that our computation has also shown directly that the degree of the divisor of ω is zero, which confirms once more that the degree of Ω^1_X is zero.

7.1.1 Exercise. Try to verify in this way that a smooth plane curve of degree four has genus three.

7.2 Embeddings in projective space.

Let X be a proper smooth irreducible curve over an algebraically closed field k. Let $\mathcal{L}$ be an invertible $\mathcal{O}_X$-module. If $s_0, \ldots, s_n$ are global sections of $\mathcal{L}$, we say that they generate $\mathcal{L}$ if the associated morphism of $\mathcal{O}_X$-modules:

$$\mathcal{O}_X^{n+1} \longrightarrow \mathcal{L}, \quad f \mapsto \sum_i f_i s_i$$

is surjective. If this is so, then the s_i give a morphism $\phi\colon X \to \mathbb{P}^n_k$, as we have seen before. Concretely, an element P in $X(k)$ is sent to the point $\phi(P) = (s_0(P) : \cdots : s_n(P))$, where we view the $s_i(P)$ as elements in the one-dimensional k-vector space $\mathcal{L}(P) := P^*\mathcal{L}$. (Note that indeed an $n+1$-tuple of elements, not all zero, of a one-dimensional k-vector space do define a point in $\mathbb{P}^n(k)$.)

7.2.1 Theorem. *([HarAG, IV, Prop. 3.1]) In the above situation, suppose that the s_i form a k-basis of $\mathcal{L}(X)$, and that they generate $\mathcal{L}$. Then the morphism ϕ is a closed immersion if and only if, for all P and Q in $X(k)$, $\mathrm{h}^0(X, \mathcal{L} \otimes \mathcal{O}_X(-P-Q)) = \mathrm{h}^0(X, \mathcal{L}) - 2$.*

Before going into the proof of this theorem, let us say something in general about $\mathrm{h}^0(X, \mathcal{L} \otimes \mathcal{O}_X(-P))$. So consider X as above, let $\mathcal{L}$ be an invertible $\mathcal{O}_X$-module, and let P be in $X(k)$. As always, we have the short exact sequences of $\mathcal{O}_X$-modules:

$$0 \to I_P\mathcal{O}_X \to P_*k \to 0, \quad \text{and} \quad 0 \to \mathcal{L} \otimes \mathcal{O}_X(-P) \to \mathcal{L} \to P_*P^*\mathcal{L} \to 0,$$

the second one being obtained from the first one by tensoring with $\mathcal{L}$. This gives the long exact sequence:

$$0 \longrightarrow \mathrm{H}^0(X, \mathcal{L} \otimes \mathcal{O}_X(-P)) \longrightarrow \mathrm{H}^0(X, \mathcal{L}) \longrightarrow P^*\mathcal{L} \longrightarrow \cdots$$

Since $P^*\mathcal{L}$ is a k-vector space of dimension one, it follows that $\mathrm{h}^0(X, \mathcal{L} \otimes \mathcal{O}_X(-P))$ equals $\mathrm{h}^0(X, \mathcal{L}) - 1$ or $\mathrm{h}^0(X, \mathcal{L})$; the first case occurs if and only there does exist an element s in $\mathcal{L}(X)$ such that $s(P) \neq 0$. In particular, $\mathcal{L}$ is generated by global sections if and only if $\mathrm{h}^0(X, \mathcal{L} \otimes \mathcal{O}_X(-P)) = \mathrm{h}^0(X, \mathcal{L}) - 1$ for all P in $X(k)$.

Proof. By the same reasoning as we have just done, the condition that $\mathrm{h}^0(X, \mathcal{L} \otimes \mathcal{O}_X(-P-Q)) = \mathrm{h}^0(X, \mathcal{L}) - 2$ for all $P \neq Q$ just means that for every $P \neq Q$ there does exist a global section s of $\mathcal{L}$ such that $s(P) = 0$ and $s(Q) \neq 0$. In other words, this means that the s_i do separate the elements of $X(k)$, just as in the theorem of Stone-Weierstrass in analysis. The condition that for every P in $X(k)$ one has $\mathrm{h}^0(X, \mathcal{L} \otimes \mathcal{O}_X(-2P)) = \mathrm{h}^0(X, \mathcal{L}) - 2$

means that for every P there does exist a global section s of $\mathcal{L}$ that has valuation one at s. In other words, this means that the s_i do separate tangent vectors at every P.

The injectivity of ϕ is hence equivalent to the condition for all $P \neq Q$. The surjectivity of the morphisms of local rings $\phi^\#\colon \mathcal{O}_{\mathbb{P}^n_k,\phi(P)} \to \mathcal{O}_{X,P}$ is equivalent, by Nakayama's lemma, to the condition for $P = Q$. $\square$

7.2.2 Corollary. *Let X be a proper smooth geometrically irreducible curve over a field k, and let $\mathcal{L}$ be an invertible $\mathcal{O}_X$-module with* $\deg(\mathcal{L}) > 2g(X)$*. Then every k-basis of $\mathcal{L}(X)$ gives a closed immersion of X into $\mathbb{P}^N_K$, with $N = \mathrm{h}^0(X,\mathcal{L}) - 1$.*

Proof. Let $k \to \overline{k}$ be an algebraic closure of k. Then apply Serre duality to see that $\mathrm{h}^1(X_{\overline{k}}, \mathcal{L} \otimes \mathcal{O}_{X_{\overline{k}}}(-P-Q)) = 0$ for all P and Q in $X(\overline{k})$. This proves that the global sections of $\mathcal{L}$ generate $\mathcal{L}$, and that the morphism ϕ becomes a closed immersion after base change to $\overline{k}$. It is left as an exercise to deduce from this that ϕ itself is a closed immersion. $\square$

7.2.3 Remark. Over an infinite field k, one can easily show that every smooth curve in $\mathbb{P}^n_k$ with $n \geq 3$ can be embedded into $\mathbb{P}^3_k$ via a suitable projection. See [HarAG, IV, Cor. 3.6]

7.3 Weierstrass equations for elliptic curves.

7.3.1 Definition. Aan elliptic curve over a field k is a proper smooth geometrically irreducible curve E over k, of genus one, with a given element 0 in $E(k)$. (The given point is called 0 because it will be the origin for some group law.)

Let now E be an elliptic curve over some field k. Applying Riemann-Roch on E gives, for $\mathcal{L}$ an invertible $\mathcal{O}_E$-module:

$$\mathrm{h}^0(E,\mathcal{L}) = \deg(\mathcal{L}), \quad \text{if} \quad \deg(\mathcal{L}) > 0.$$

We will now apply Cor. 7.2.2 with $\mathcal{L} := \mathcal{O}_E(3{\cdot}0)$. So any k-basis of $\mathrm{H}^0(E,\mathcal{O}_E(3{\cdot}0))$ gives an embedding of E into $\mathbb{P}^2_k$. The image of this closed immersion is then of the form $V(F)$, with F homogeneous of degree 3 (in fact, every one dimensional reduced closed subscheme of $\mathbb{P}^2_k$ is of the form $V(F)$ with F non-zero and homogeneous). In order to get F into what is called a generalized Weierstrass equation, we choose a special basis of $\mathrm{H}^0(E,\mathcal{O}_E(3{\cdot}0))$, by the following procedure. First of all, we choose a uniformizer π of $\mathcal{O}_{E,0}$; this uniformizer will be of relevance only up to first order, i.e., a uniformizer π' with $\pi' = \pi + \pi^2 a$ with a in $\mathcal{O}_{E,\infty}$ will lead to the same things. The space $\mathrm{H}^0(E,\mathcal{O}_E)$

consists of the constant functions; we take the basis 1 for it. Since $\mathrm{h}^0(E, \mathcal{O}_E(0)) = 1$, and $\mathrm{H}^0(E, \mathcal{O}_E(0))$ contains $\mathrm{H}^0(E, \mathcal{O}_E)$, $\mathrm{H}^0(E, \mathcal{O}_E(0)) = k$, and we get nothing new. Now $\mathrm{H}^0(E, \mathcal{O}_E(2{\cdot}0))$ has dimension two, hence contains non-constant functions. Let x be a non-constant function in $\mathrm{H}^0(E, \mathcal{O}_E(2{\cdot}0))$. Then, since $\mathrm{H}^0(E, \mathcal{O}_E(0)) = k$, x has a pole of order two at 0. After multiplying x by an element of k^*, we may assume that $(\pi^2 x)(0) = 1$, i.e., that $x = \pi^{-2} + \pi^{-1}a$ with a in $\mathcal{O}_{E,0}$. In this case, we say that x is adapted to π; note that indeed this depends only on x and on the image of π in m_0/m_0^2. For later use, we note that x is unique up to $x' = x + r$, with r in k. By the same arguments, we find a function y in $\mathrm{H}^0(E, \mathcal{O}_E(3{\cdot}0))$ with a pole of order three at 0, such that $y = \pi^{-3} + \pi^{-2}a$ with a in $\mathcal{O}_{E,0}$. Such a y is unique up to $y' = y + sx + t$ with s and t in k. Now consider the following table, giving k-bases for the spaces $\mathrm{H}^0(E, \mathcal{O}_E(n{\cdot}0))$ with $0 \leq n \leq 6$:

	$\dim_k$	k-basis
$\mathrm{H}^0(E, \mathcal{O}_E)$	1	1
$\mathrm{H}^0(E, \mathcal{O}_E(0))$	1	1
$\mathrm{H}^0(E, \mathcal{O}_E(2{\cdot}0))$	2	1, x
$\mathrm{H}^0(E, \mathcal{O}_E(3{\cdot}0))$	3	1, x, y
$\mathrm{H}^0(E, \mathcal{O}_E(4{\cdot}0))$	4	1, x, y, x^2
$\mathrm{H}^0(E, \mathcal{O}_E(5{\cdot}0))$	5	1, x, y, x^2, xy
$\mathrm{H}^0(E, \mathcal{O}_E(6{\cdot}0))$	6	1, x, y, x^2, xy, x^3
$\mathrm{H}^0(E, \mathcal{O}_E(6{\cdot}0))$	6	1, x, y, x^2, xy, y^2

Note that we have two bases of $\mathrm{H}^0(E, \mathcal{O}_E(6{\cdot}0))$. Hence, y^2 is a linear combination of 1, x, y, x^2, xy, and x^3. Since only y^2 and x^3 have a pole of order three at 0, and the others a pole of lesser order, the coefficient of x^3 in this linear combination is non-zero. Moreover, since both x and y are adapted to π, that coefficient is one. The conclusion is that, once we have chosen t, x and y, there are unique elements a_1, a_2, a_3, a_4 and a_6 in k such that:

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

(There is a reason for this numbering of the coefficients that we will explain a bit later.) The morphism $\phi\colon E \to \mathbb{P}^2_k$ given by the k-basis x, y, 1 (in this order), is a closed immersion, whose image is contained in $V(F)$, with

$$F = -Y^2Z - a_1XYZ - a_3YZ^2 + X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Since F is irreducible (this follows from the fact that the intersection with $V(Z)$ is one point, and that at that point $V(F)$ is non-singular), ϕ is an isomorphism from E to $V(F)$.

In particular, this implies that $V(F)$ is smooth. One can show that there exists a unique element Δ of degree 12 in the polynomial ring $\mathbb{Z}[A_1, A_2, A_3, A_4, A_6]$, which is graded by decreeing that A_i has degree i, such that $V(F)$ is smooth if and only if $\Delta(a_1, a_2, a_3, a_4, a_6) \neq 0$ in k.

Let us now answer the question as to up to what F is unique, given $(E, 0)$. Of course, the point 0 does not matter, since E has a group law, so that translation over P gives an isomorphism from $(E, 0)$ to (E, P) (we will show in the next section that the group law on $E(\overline{k})$ is given by a morphism of k-schemes). So recall that we made choices for π, x, and y, and that that was all. Hence we just have to see what happens when we put:

$$\pi' = u^{-1}\pi, \quad x' = u^2x + r, \quad y' = u^3y + su^2x + t.$$

This gives an equation F' with coefficients a_i' that can be easily expressed in the a_i, u, r, s and t. This leads to a simple procedure to see whether or not two elliptic curves, given by Weierstrass equations, are isomorphic: one just has to see if there exist u, r, s and t that transform the first equation into the second. This existence is expressed by a set of polynomial equations in u, r, s and t. The reason that A_i should have degree i in the ring $\mathbb{Z}[A_1, A_2, A_3, A_4, A_6]$ is that for the transformation $\pi' = u^{-1}\pi$, $x' = u^2x$ and $y' = u^3y$, one finds $a_i' = u^ia_i$. (And do not forget that gradings have to do with actions of k^*!)

For example, let us consider the case where k has characteristic different from 2 and 3. Then we can achieve, by unique r, s and t, that a_1, a_3 and a_2 are zero, i.e., that E is given by an equation:

$$y^2 = x^3 + ax + b$$

One easily checks that this equation defines a smooth curve if and only if $4a^3 + 27b^2 \neq 0$ (do not forget that 6 is in k^*). Anyway, this equation is now unique up to the effect of $\pi' = u^{-1}\pi$, i.e., up to $a' = u^4a$, $b' = u^6b$. It is now pretty clear that the element

$$j(E) := 12^3 \frac{4a^3}{4a^3 + 27b^2}$$

is an invariant of E, i.e., depends only on the isomorphism class of E. But it is not true that $j(E) = j(E')$ implies that E is isomorphic to E'. For example, the two elliptic curves E and E' over $\mathbb{Q}$ given by the equations $y^2 = x^3 + 1$ and $y^2 = x^3 + 2$ are not isomorphic, and have the same j-invariant. But, one can show that if two elliptic curves over k have the same j-invariant, then there is a finite separable extension $k \to k'$ such that $E_{k'}$ and $E'_{k'}$ are isomorphic. In particular, over an algebraically closed field, the j-invariant does classify elliptic curves up to isomorphism.

Let me finish here by remarking that having k-schemes that are not isomorphic but that become isomorphic after a field extension has nothing to do with elliptic curves in particular. For example, a proper smooth geometrically irreducible curve X of genus zero over a field k is isomorphic to $\mathbb{P}^1_k$ if and only if $X(k)$ is not empty.

7.4 The group law on an ellliptic curve.

Let E be an elliptic curve over a field k. Recall that the Picard group $\mathrm{Pic}(E)$ is the set of isomorphism classes of invertible $\mathcal{O}_E$-modules, with the tensor product over $\mathcal{O}_E$ as group law. We have a morphism of groups:

$$\deg\colon \mathrm{Pic}(E) \longrightarrow \mathbb{Z}, \quad \mathcal{L} \mapsto \deg(\mathcal{L}).$$

for n in $\mathbb{Z}$, we let $\mathrm{Pic}^n(E)$ be the inverse image in $\mathrm{Pic}(E)$ of deg.

7.4.1 Theorem. *The map $E(k) \to \mathrm{Pic}^1(E)$, $P \mapsto \mathcal{O}_E(P)$, is a bijection. Hence the map $E(k) \to \mathrm{Pic}^0(E)$, $P \mapsto \mathcal{O}_E(P-0)$ is also a bijection. Since $\mathrm{Pic}^0(E)$ is a commutative group, this makes $E(k)$ into a commutative group. This group law is functorial for all field extensions.*

Proof. We will construct the inverse. Let $\mathcal{L}$ be an invertible $\mathcal{O}_E$-module of degree one. By Riemann-Roch, $\mathcal{L}(E)$ is a one-dimensional k-vector space. Let s be a non-zero element in $\mathcal{L}(E)$. Then $\mathrm{div}_{\mathcal{L}}(s)$ is an effective divisor of degree one on E, hence an element of $E(k)$. It is clear that P depends only on the class of $\mathcal{L}$ in $\mathrm{Pic}(E)$, and that this defines the inverse we need. The map to $\mathrm{Pic}^0(E)$ is the one to $\mathrm{Pic}^1(E)$, followed by a translation in $\mathrm{Pic}(E)$. That proves the second statement of the theorem. The last statement follows from the functoriality of the Picard group. □

Let us write this group law as $(P, Q) \mapsto P \oplus Q$, for the moment, in order to distinguish it from $P + Q$ as divisor on E. By construction, we have, for P, Q and R in $E(k)$:

$$P \oplus Q = R \quad \text{if and only if} \quad P + Q - R - 0 \quad \text{is a principal divisor.}$$

In the same way, but more symmetrically:

$$P \oplus Q \oplus R = 0 \quad \text{if and only if} \quad P + Q + R - 3{\cdot}0 \quad \text{is a principal divisor.}$$

This last identity explains that, for an elliptic curve in $\mathbb{P}^2_k$ given by a Weierstrass equation, $P \oplus Q \oplus R = 0$ if and only if P, Q and R are the three intersection points of E with a suitable line.

8 March 12, 1999

8.1 Elliptic curves are group schemes.

Last time, we have seen, using the theorem of Riemann-Roch, that for E an elliptic curve over a field k, we have a bijection from $E(k)$ to $\mathrm{Pic}^0(E)$, sending P to $\mathcal{O}_E(P-0)$. This bijection induces a group structre on $E(k)$. We want to show now that this group structure comes from a structure of group scheme on E/k, i.e., from a morphism $E \times_k E \to E$ satisfying certain properties. To achieve this, there are at least two strategies. The first one is to show by hand that the group law on $E(k)$ is given, locally on $E \times_k E$, by regular functions. The second one consists of generalizing the bijection $E(k) \to \mathrm{Pic}^0(E)$ from fields to arbitrary schemes, i.e., to construct an isomorphism of functors from E to a suitably defined functor that has a group structure. The first strategy is certainly possible, but the second one is more satisfactory, and gives a good idea of what jacobian varieties are for curves of higher genus. So we will follow the second strategy, even if it is somewhat technical.

So for E an elliptic curve over a field k, we are led to consider $E(S)$, for arbitrary k-schemes S. Moreover, we will have to consider an element P in $E(S)$ as an S-valued point of E_S, where E_S denotes the S-scheme obtained from E/k via the base change $S \to \mathrm{Spec}(k)$. This means that we will have to prove things for elliptic curves over arbitrary schemes, such as E_S/S. Since we have to do this anyway, we should introduce the notion of elliptic curve over a scheme.

8.1.1 Definition. Let S be a scheme. An elliptic curve over S is an S-scheme E that is proper, smooth, equipped with a given element 0 in $E(S)$, whose fibres are elliptic curves: for every s in S, the $k(s)$-scheme E_s obtained from E/S is an elliptic curve over $k(s)$.

8.1.2 Example. Let A_0 be the polynomial ring $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$. Over A_0, we have the closed subscheme E of $\mathbb{P}^2_{A_0}$ given by the equation:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^2.$$

This equation has a discriminant Δ in A_0 that we won't define here. It is a polynomial in the a_i of degree 12, where each a_i has degree i, and it has the property that $V(\Delta)$ is the closed subscheme of $\mathrm{Spec}(A_0)$ over which E is not smooth. Let $A := A_0[1/\Delta]$, and denote by E the A-scheme obtained from E/A_0 via the base change $A_0 \to A$. Let 0 in $E(A)$ be the point $(0:1:0)$. Then $(E/A, 0)$ is an elliptic curve over A.

8.1.3 Theorem. *Let E'/S be an elliptic curve over a scheme. Then, locally on S, E' can be given by a Weierstrass equation. More precisely, S can be covered by open subschemes U such that E'_U/U can be obtained from E/A via a suitable morphism $U \to \mathrm{Spec}(A)$:*

$$\begin{array}{ccccc} E' & \longleftarrow & E'_U & \longrightarrow & E \\ \downarrow & & \downarrow & \square & \downarrow \\ S & \longleftarrow & U & \longrightarrow & S \end{array}$$

Proof. We just give a sketch, because we lack at least two techniques for doing this proof in detail. One uses Riemann-Roch for the fibres of E/S together with the theorem [HarAG, III, Thm. 12.11] that describes the behaviour of cohomology with respect to base change. That shows, if $p\colon E \to S$ denotes the structural morphism of the S-scheme E, that the $\mathrm{R}^1 p_*\mathcal{O}_E(n{\cdot}0)$ (n in $\mathbb{Z}$) are locally free of the rank given by Riemann-Roch if S were $\mathrm{Spec}(k)$ with k a field. Moreover, it then follows that $p_*\mathcal{O}_E = \mathcal{O}_S$, and that the $p_*\mathcal{O}_E(n{\cdot}0)$ (n in $\mathbb{Z}$) are locally free of the rank given by Riemann-Roch if S were $\mathrm{Spec}(k)$ with k a field. Once one has these results, one can generalize the proof we gave over a field. For details see chapter 2 of [KaMaAM].

Actually, in order to apply [HarAG, III, Thm. 12.11], one needs that S be locally noetherian. Hence one has to reduce first to the case where S is locally noetherian. But since E/S is proper and smooth, it is of finite presentation, which implies that, locally on S, it is obtained by base change from some E'/S' with $S' = \mathrm{Spec}(R)$ with R a finitely generated $\mathbb{Z}$-algebra (see [GrDiEGA, IV, Thm. 8.11.?]). Intuitively, this is pretty clear, since E/S is locally given by finitely many equations, in finitely many variables. $\square$

We will now define, for E/S an elliptic curve, the relative Picard functor that is supposed to be represented by E/S. Naively, a first guess would be the functor that associates, to every S-scheme T, the group $\mathrm{Pic}(E_T)$. But this functor cannot be representable, since it is not a sheaf for the Zariski topology if S is not empty: take T an S-scheme such that $\mathrm{Pic}(T)$ is not zero, take $\mathcal{L}$ a non-trivial $\mathcal{O}_T$-module, then $p_T^*\mathcal{L}$ is an element in $\mathrm{Pic}(E_T)$ that becomes zero locally on T, but is non-zero. To overcome this problem, one simply defines the relative Picard functor associated to E/S by:

$$\mathrm{Pic}_{E/S}\colon (T \to S) \mapsto \mathrm{Pic}(E_T)/p_T^*\mathrm{Pic}(T).$$

Let us note that since 0_T is a section of p_T, $p_T^*\mathrm{Pic}(T)$ is in fact a direct factor of $\mathrm{Pic}(E_T)$. For every i in $\mathbb{Z}$, we have a subfunctor $\mathrm{Pic}^i E/S$ of $\mathrm{Pic}_{E/S}$ given, for every S-scheme T, by the elements of $\mathrm{Pic}(E_T)$ that have degree i on all fibres of E_T/T. We have morphisms of functors:

$$E \to \mathrm{Pic}^1_{E/S}, \quad P \in E(T) \mapsto \left[I_{P_T}^\vee\right], \quad \text{and} \quad E \to \mathrm{Pic}^0_{E/S}, \quad P \mapsto \left[I_{P_T}^\vee \otimes_{\mathcal{O}_{E_T}} I_{0_T}\right].$$

8.1.4 Theorem. *These morphisms of functors are isomorphisms. We view E/S as a group scheme via the isomorphism with $\mathrm{Pic}^0_{E/S}$. Explicitly, for P, Q and R in $E(T)$ one has $P+Q+R=0$ if and only if there is an invertible $\mathcal{O}_T$-module $\mathcal{L}$ such that $I_{P_T}\otimes I_{Q_T}\otimes I_{R_T}$ is isomorphic, as $\mathcal{O}_{E_T}$-module, to $I_{0_T}^{\otimes 3}\otimes p_T^*\mathcal{L}$.*

Proof. See [KaMaAM], Chapter 2. Let us just note that this proof does not require more technique than the previous one. □

8.2 Rigidity and some consequences.

For the moment, we will mean, for E and E' elliptic curves over S, by morphism of elliptic curves from E to E' a morphism f of S-schemes such that $f(0)=0'$. Note that this last condition can always be realized by composing f by a (unique) translation. We will see in a moment that in fact such a morphism respects the group structures, hence is automatically a morphism of S-group schemes.

8.2.1 Theorem. *Let $f\colon E\to E'$ be a morphism of elliptic curves over a scheme S. Suppose that for some s in S we have $f_s=0$, i.e., f induces the constant morphism 0 from E_s to E'_s. Then $f=0$ in a neighborhood of s.*

Proof. We start by replacing S by an open affine neighborhood of s in S. Let $U\subset E'$ be an affine open neighborhood of $0'(s)$ in E'. Then $f^{-1}U$ is open in E and contains E_s, since $f_s=0$. Let Y be $E-f^{-1}U$. Then Y is closed in E, and, $p\colon E\to S$ being proper, fY is closed in S. Hence $S':=S-fY$ is open in S, and contains s. Now we replace S by an affine open $\mathrm{Spec}(A)$ of S' containing s, and U by the affine $\mathrm{Spec}(B)=U\cap p'^{-1}\mathrm{Spec}(A)$. Then $f\colon E\to E'$ factors through $\mathrm{Spec}(B)\to E'$. Now we use that for any A-scheme X and any A-algebra B we have:

$$\mathrm{Hom}_{A\text{-Sch}}(X,\mathrm{Spec}(B))=\mathrm{Hom}_{A\text{-Alg}}(B,\mathcal{O}_X(X)).$$

Now recall that we have $p_*\mathcal{O}_E=\mathcal{O}_S$, hence $\mathcal{O}_E(E)=A$. This means that f factors through p, i.e., is of the form $P\circ p$ for some P in $E'(S)$. But since $f(0)=0'$, we have $P=0'$, and $f=0$. □

8.2.2 Corollary. *For $f\colon E\to E'$ a morphism of elliptic curves over some scheme S, S is the disjoint union $\coprod_d S_d$, indexed by $d\geq 0$, of open (and hence closed) subschemes such that $f=0$ on S_0 and f finite locally free of rank d on S_d for $d>0$. The degree of f is defined to be the locally constant function on S that takes value d on S_d.*

Proof. We have seen the existence of the open subscheme S_0. It is not hard to show that $f = 0$ defines a closed subset of S. Hence S_0 is open and closed, and we can replace S by $S - S_0$. Then f is non-constant on each fibre, hence finite and surjective and hence flat on each fibre. Then f is finite because proper and quasi-finite. It is flat because of the fibre by fibre criterion of flatness. For details, see [KaMaAM], Chapter 2. $\square$

8.2.3 Corollary. *The group law on E/S given by the isomorphism with $\mathrm{Pic}^0_{E/S}$ is the unique group law on E/S for which 0 is the origin.*

Every morphism of elliptic curves $f\colon E \to E'$ (i.e., a morphism of S-schemes with $f(0) = 0'$) is a morphism of S-group schemes.

Proof. Let us prove the second assertion; the first one is proved in the same way. So let $f\colon E \to E'$ be a morphism of S-schemes with $f(0) = 0'$. We have to show that $f(P + Q) = f(P) + f(Q)$ for all T and P and Q in $E(T)$. Base change to T reduces this problem to the case $T = S$. Now consider the morphism $F\colon E \times_S E \to E' \times_S E$ that sends, for every T/S, P' and Q' in $E(T)$ to $(f(P' + Q') - f(P') - f(Q'), Q')$. Now view $E \times_S E$ and $E' \times_S E$ as elliptic curves over E via their projections to the second coordinate. Then F is a morphism of elliptic curves over E, with the property that at $0(S)$ in E it is zero (i.e., $F(P', 0_T) = 0'_T$ for all P'). Hence $F = 0$ on an open and closed subset of E that contains $0(S)$. But, as all fibres of E/S are connected, that open and closed subset is E itself. $\square$

From now on we will mean by morphism of elliptic curves a morphism of group schemes.

8.3 Dual morphisms.

Let $f\colon E \to E'$ be a morphism of elliptic curves over a scheme S. Then we get a morphism $f^t\colon E' \to E$, called the dual or transpose of f, as follows:

$$\begin{array}{ccc} E & \xleftarrow{f^t} & E' \\ \sim\downarrow & & \downarrow\sim \\ \mathrm{Pic}^0_{E/S} & \xleftarrow{f^*} & \mathrm{Pic}^0_{E'/S} \end{array}$$

where $f^*\colon \mathrm{Pic}^0_{E'/S} \to \mathrm{Pic}^0 E/S$ is the morphism that sends, for every T/S, $[\mathcal{L}]$ to $[f^*\mathcal{L}]$. Let us note that f^* commutes with the tensor product, hence is compatible with the group laws (even without assuming that f is a morphism of group schemes). It is obvious that for $g\colon E' \to E''$ a morphism of elliptic curves, one has $(g\circ f)^t = f^t\circ g^t$, because $(g\circ f)^* = f^*\circ g^*$.

For n in $\mathbb{Z}$, and E/S an elliptic curve, we will denote by $[n] = [n]_E\colon E \to E$ the morphism that is multiplication by n for the group law on E.

8.3.1 Theorem. *Let $f\colon E \to E'$ be a morphism of elliptic curves. Then $f \circ f^t = [\deg(f)]_{E'}$.*

Proof. By rigidity, it suffices to prove this over a field, and hence over an algebraically closed field (note that if S is the spectrum of an artinian local ring, then this application of rigidity is pretty strong). So let now $S = \mathrm{Spec}(k)$, with k algebraically closed. Via the bijection $E(k) \to \mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\equiv$, the map $f \circ f^t$ corresponds to the map on degree zero divisors that sends D to f_*f^*D, where f_* is defined on divisors by linearity: $f_*(\sum a_iP_i) = \sum a_if(P_i)$. But for every Q in $E'(k)$ we have:

$$f_*f^*Q = f_*\left(\sum_{f(P)=Q} e_PP\right) = \left(\sum_{f(P)=Q} e_P\right)Q = \deg(f)Q,$$

which shows that $f_*f^*D = \deg(f)D$ for every D in $\mathrm{Div}(E')$. □

8.3.2 Corollary. *Let $f\colon E \to E'$ be a morphism of elliptic curves. Then $f^t \circ f = [\deg(f)]_E$, and $f^{tt} = f$.*

Proof. We have:

$$f \circ f^t \circ f = [\deg(f)]_{E'} \circ f = f \circ [\deg(f)]_E,$$

hence:

$$0 = f \circ (f^t \circ f - [\deg(f)]_E).$$

By rigidity, it suffices to prove the required identity over a field. Hence we have either $f = 0$ or f finite. In the first case, the indentity is obviously true. In the second case, $f^t \circ f - [\deg(f)]_E$ has image in the finite closed subscheme $\ker(f)$ defined by the cartesian diagram:

$$\begin{array}{ccc} \ker(f) & \longrightarrow & S \\ \downarrow & & \downarrow{\scriptstyle 0} \\ E & \xrightarrow{f} & E' \end{array}$$

But then, as $\mathcal{O}_E(E)$ consists just of the constant functions, $f^t \circ f - [\deg(f)]_E = 0$. □

8.3.3 Theorem. *Let f and g be morphisms of elliptic curves from E to E' over some scheme S. Then $(f+g)^t = f^t + g^t$ in $\mathrm{Hom}_S(e', E)$.*

Proof. Rigidity reduces the problem to $S = \mathrm{Spec}(k)$ with k a field. We may suppose that k is algebraically closed. Then it remains to show that for all $\mathcal{L}$ in $\mathrm{Pic}^0(E')$ we have:

$$(f+g)^*\mathcal{L} = f^*\mathcal{L} \otimes g^*\mathcal{L}.$$

Now consider the following diagram:

$$\begin{array}{ccccc} & & E' & & \\ & & \mathrm{pr}_1\uparrow & & \\ E & \xrightarrow{(f,g)} & E' \times_k E' & \xrightarrow{+} & E' \\ & & \mathrm{pr}_2\downarrow & & \\ & & E' & & \end{array}$$

It follows that the theorem is a consequence of (and in fact equivalent to) the next one. □

8.3.4 Theorem. *(Theorem of the square.) Let E be an elliptic curve over a field. Then, for any invertible $\mathcal{O}_E$-module $\mathcal{L}$ of degree zero, we have:*

$$+^*\mathcal{L} \cong \mathrm{pr}_1^*\mathcal{L} \otimes \mathrm{pr}_2^*\mathcal{L}$$

as $\mathcal{O}_{E\times_k E}$-modules.

Proof. Let P be the element in $E(k)$ such that $\mathcal{L}$ is isomorphic to $\mathcal{O}_E(P-0)$. Then $+^*\mathcal{L}$ is isomorphic to $\mathcal{O}_{E\times_k E}(+^*P - +^*0)$, and $\mathrm{pr}_1^*\mathcal{L}\otimes \mathrm{pr}_2^*\mathcal{L}$ is isomorphic to $\mathcal{O}_{E\times_k E}(\mathrm{pr}_1^*P - \mathrm{pr}_1^*0 + \mathrm{pr}_2^*P - \mathrm{pr}_2^*0)$. Viewing $E\times_k E$ as an elliptic curve over E, via pr_1, shows that:

$$+^*P - +^*0 \equiv \mathrm{pr}_2^*P - \mathrm{pr}_2^*0 + \mathrm{pr}_1^*D,$$

for some D in $\mathrm{Div}(E)$. Restricting this to $E\times\{Q\}$ for any Q shows that $D \equiv P - 0$. □

Now it is harvest time!

8.3.5 Corollary. *Let E/S be an elliptic curve, with S not empty. Then the ring $\mathrm{End}_S(E)$ is torsion free as $\mathbb{Z}$-module, and is an integral domain in the sense that $1 \neq 0$ and $ab = 0$ implies $a = 0$ or $b = 0$ (the ring is not necessarily commutative). For every n in $\mathbb{Z}$ we have $\deg([n]_E) = n^2$.*

Proof. We have $1 \neq 0$ in $\mathrm{End}_S(E)$ because S is not empty. For $ab = 0$ implying $a = 0$ or $b = 0$ we may, by rigidity, assume that $S = \mathrm{Spec}(k)$ with k a field. But then this follows from the fact that a non-zero endomorphism of E is surjective and has finite kernel. For the torsion freeness of $\mathrm{End}_S(E)$ as $\mathbb{Z}$-module, we may also assume that $S = \mathrm{Spec}(k)$. By what we just proved, it suffices to show that for each prime p, $[p]_E \neq 0$. For this, it suffices to show that the closed subscheme $\ker([2])$ of E is non-zero and different from E, which one can verify by hand using a Weierstrass model (in fact, $E[2]$ is a finite group scheme over k of rank 4). For the final statement, we may assume that $n \geq 0$, and we write:

$$[\deg([n])] = [n] \circ [n]^t = [1 + \cdots + 1] \circ [1 + \cdots + 1]^t = [n] \circ [n] = [n^2].$$

Since $\mathbb{Z} \to \mathrm{End}_S(E)$ is injective, this implies $\deg([n]) = n^2$. □

From now on we will denote $[n]$ simply by n.

8.3.6 Corollary. *Let E be an elliptic curve over a field. Then $\mathrm{End}_k(E)$ is an integral domain (not necessarily comutative) with an involution $f \mapsto f^t$. For every f in $\mathrm{End}_k(E)$ one has $\mathrm{tr}(f) := f + f^t$ in $\mathbb{Z}$, and this integer is called the trace of f. For every f in $\mathrm{End}_k(E)$ we have:*

$$0 = (f - f)(f - f^t) = f^2 - \mathrm{tr}(f)f + \deg(f),$$

which means that every f satisfies a monic degree two polynomial with coefficients in $\mathbb{Z}$. Moreover, this degree two polynomial satisfies:

$$\mathrm{tr}(f)^2 - 4\deg(f) \leq 0,$$

which is equivalent to its two roots in $\mathbb{C}$ being complex conjugates.

Proof. We have already seen that $\mathrm{End}_k(E)$ is an integral domain, and that $f \mapsto f^t$ is an involution. To show that $f + f^t$ is in $\mathbb{Z}$, write:

$$\deg(1 + f) = (1 + f)(1 + f)^t = (1 + f)(1 + f^t) = 1 + f + f^t + ff^t = 1 + \mathrm{tr}(f) + \deg(f).$$

This shows that $\mathrm{tr}(f) = \deg(1 + f) - \deg(f)$ is an integer. Now note that

$$0 \leq \deg(n + mf) = (n + mf)(n + mf)^t = n^2 + nm\mathrm{tr}(f) + m^2\deg(f)$$

for all n and m in $\mathbb{Z}$. This implies that the discriminant of this quadratic form, which happens to be $\mathrm{tr}(f)^2 - 4\deg(f)$, is ≤ 0. □

The not necessarily commutative integral domains R with a positive involution as above can be classified. The various possibilities are: $R = \mathbb{Z}$, R a subring of finite index in the ring of integers of an imaginary quadratic field with the unique non-trivial involution, and a subring of a quaternion algebra over $\mathbb{Q}$ that is free of rank four as $\mathbb{Z}$-module, with an involution that is unique up to conjugation. In the last case, the quaternion algebra is definite, in the sense that $\mathbb{R} \otimes R$ is isomorphic, as $\mathbb{R}$-algebra, to Hamilton's quaternion algebra. In the first two cases, all these possibilities do arise, in fact over each algebraically closed field. In the last case, the field has to have positive characteristic, call it p, and then the quaternion algebra has discriminant p, i.e., it is split at all primes $l \neq p$.

8.4 Elliptic curves over finite fields.

Let us now consider an elliptic curve E over a finite field $k := \mathbb{F}_q$. Then we have a particular element in $\mathrm{End}_k(E)$: the frobenius endomorphism $F \colon E \to E$ given on each open affine $\mathrm{Spec}(A)$ by $F^{\#} \colon x \mapsto x^q$ (note that this induces the identity on k, as it should). This morphism F is purely inseparable, and has derivative zero everywhere. Therefore, $1 - F$ has derivative the identity map, hence nowhere zero. Hence $\ker(1-F)$ is the finite reduced closed subscheme of E consisting of the k-rational points of E. Note that $\deg(F) = q$, since $k(E)$ is algebraic over $k(x)$. The following theorem due to Hasse (I think) has now, after 10 weeks of labor, an obvious proof.

8.4.1 Theorem. *The number of $\mathbb{F}_q$-rational points on E is given by:*

$$\#E(\mathbb{F}_q) = \deg(1 - F) = (1 - F)(1 - F)^t = 1 - \mathrm{tr}(F) + q.$$

In this expression, $|\mathrm{tr}(F)| \leq 2\sqrt{q}$. Moreover, if we let α and β denote the two roots in $\mathbb{C}$ of the polynomial $X^2 - \mathrm{tr}(F)X + q$, then for every $n \geq 1$, we have:

$$\#E(\mathbb{F}_{q^n}) = 1 - \alpha^n - \beta^n + q^n.$$

References

[CoSiAG] G. Cornell and J.H. Silverman. *Arithmetic Geometry.* Springer-Verlag.

[CoSiSt] G. Cornell, J.H. Silverman and G. Stevens (editors). *Modular Forms and Fermat's Last Theorem.* Springer-Verlag, 1997.

[EdEvDA] B. Edixhoven and J.-H. Evertse. *Diophantine approximation on abelian varieties.* Lecture Notes in Mathematics 1566, Springer-Verlag.

[GeMaHA] S.I. Gelfand and Yu.I. Manin. *Homological Algebra.* Algebra V. Encyclopaedia of Mathematical Sciences, Volume 38, A.I. Kostrikin and I.R. Shafarevich (Eds.).

[GrDiEGA] A. Grothendieck and J.A. Dieudonné. *Éléments de Géométrie Algébrique, Ch. I, II, III, IV.* Publications Mathématiques de l'I.H.E.S. 4, 8, 11, 17, 20, 24, 28, 32. Ch. I: Grundlehren der mathematische Wissenschaften in Einzeldarstellungen 166, Springer-Verlag.

[GrAH] A. Grothendieck. *Sur quelques points d'algèbre homologique.* Tôhoku Math. J. Vol. 9, (1957), 119–221.

[HarAG] R. Hartshorne. *Algebraic geometry.* GTM 52, Springer-Verlag.

[HarRD] R. Hartshorne. *Residues and duality.* Lecture Notes in Mathematics 20, Springer-Verlag.

[IlCD] L. Illusie *Catégories drives et dualit: travaux de J.-L. Verdier.* Enseign. Math. (2) 36 (1990), no. 3-4, 369–391.

[JaA2] N. Jacobson. *Basic algebra II.* W.H. Freeman and company.

[KaMaAM] N. Katz and B. Mazur. *Arithmetic moduli of elliptic curves.* Annals of athematics studies, Study 108, Princeton University Press.

[LaA] S. Lang. *Algebra.* Addison-Wesley. 2nd and 3rd editions.

[Li] Lipman. Asterique. ....

[MacCWM] S. Mac Lane. *Categories for the working mathematician.* GTM 5, Springer-Verlag.

[MasSH] W.S. Massey. *Singular homology theory.* GTM 70, Springer-Verlag.

[MumAV] D. Mumford. *Abelian varieties.* Tata Institute for fundamental resarch, Oxford University Press.

[SeGA] J-P. Serre. *Groupes algébriques et corps de classes.* Hermann, Paris (1959).

[SiAE] J.H. Silverman. *The arithmetic of elliptic curves.* GTM 106, Springer-Verlag.

[SiAT] J.H. Silverman. *Advanced topics in the arithmetic of elliptic curves.* GTM 151, Springer-Verlag.

[SiTaRP] J.H. Silverman and J. Tate. *Rational points on elliptic curves.* UTM, Springer-Verlag.