Cours DEA, jacobiennes, printemps 1996.

Bas Edixhoven

November 28, 1996

1 January 8, 1996

The aim of this course is to construct the jacobian varieties associated to smooth geometrically irreducible projective curves over arbitrary fields. We will start with the definition of smooth geometrically irreducible projective curves over a field and the study of some fundamental properties of these objects. Our time is very limited (only 20 hours of lectures), so many details will not be discussed in the lectures. The lectures are therefore very incomplete, and the students taking this course are advised to fill the gaps as much as possible using the book [Har] by Hartshorne (GTM 52, Springer Verlag) and the text [Mil] by Milne in the book "Arithmetic Geometry", Springer Verlag, edited by Cornell and Silverman.

1.1 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 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.

1.3 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 $\mathrm{Spec}(\mathbb{Z}[\sqrt{2}])$.

1.4 Definition. *An A-scheme $f\colon X \to \mathrm{Spec}(A)$ is of finite type if there exists a finite covering of X by open affines $U_i = \mathrm{Spec}(A_i)$, such that every A_i is an A-algebra of finite type. An S-scheme $f\colon X \to S$ is of finite type if there exists a covering of S by affine opens S_i such that for all i the S_i-scheme $f^{-1}S_i$ is of finite type.*

1.5 Exercise. Do exercises 3.1, 3.2 et 3.3 of [Har, II].

1.6 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* $\mathrm{Hom}(*, X)$.

1.7 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) $\mathbb{G}_m\colon X \mapsto \mathcal{O}_X(X)^*$. 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.

1.8 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 is graded as follows: $\deg(b/f^m) = \deg(b) - m\deg(f)$, for $b/f^m \neq 0$). 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 [Har, 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 [Har, II.2] for another construction of $\mathbb{P}^n_A$.

1.9 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.

1.10 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}.

1.11 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:

$$0 \to \mathcal{O}_{\mathbb{P}^n_A}(\mathbb{P}^n_A) \to \prod_i \mathcal{O}_{\mathbb{P}^n_A}(U_i) \to \prod_{i,j} \mathcal{O}_{\mathbb{P}^n_A}(U_{i,j}), \tag{1.11.1}$$

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 1.8. 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. $\square$

2 January 15, 1996

2.1 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 (1.8), 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.

2.1.1 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 1.11, 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 [Har, II, Prop. 6.13], $\mathcal{L}(D_r)$ is isormorphic to $\mathcal{O}(r)$ for all r.

2.2 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 $f^*(s)_x = s_{f(x)}$.

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.

2.2.1 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 [Har, 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 $D(s_i) \cap D(s_j) = \phi^{-1}D_+(x_ix_j)$ coincide. One also sees that if $\mathcal{L}$ and the s_i come from a ϕ as above, they give us back ϕ.

2.2.2 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 $\mathcal{O}_X^{n+1}$.

2.3 Yoneda's lemma

See also [EGA 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 contravariant 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:

$$F(X) \xrightarrow{\sim} \mathrm{Hom}_{\widehat{\mathcal{C}}}(h_X, F). \tag{2.3.1}$$

2.3.2 Exercise. Construct morphisms (of bifunctors) $\alpha_{X,F}$ and $\beta_{X,F}$, inverses of each other, establishing the bijections (2.3.1).

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, the jacobians that we want to construct in this course represent "relative" Picard functors.

2.4 Fibered products, base change

See also [EGA 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.

2.4.1 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 2.3. 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:

$$\begin{array}{ccc} Z & \xrightarrow{f'} & Y \\ g' \downarrow & & g \downarrow \\ X & \xrightarrow{f} & S \end{array} \tag{2.4.2}$$

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

2.4.3 Exercise. Show that the diagram 2.4.2 is cartesian if and only if its image in $\widehat{\mathcal{C}}$ is. Consider the diagram:

$$\begin{tikzcd} A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & C \arrow[d] \\ D \arrow[r] & E \arrow[r] & F \end{tikzcd}$$

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 [Har, 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 2.4.5).

2.4.4 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 $f'\colon X' \to Y'$.*

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.

2.4.5 Exercise. Do exercises 3.9 and 3.10 of [Har, 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.

3 January 26, 1996

Our goal for today is to define the notion of smooth geometrically irreducible projective curve over an arbitrary field.

3.1 Some useful indications for some exercises in [Har]

This concerns exercises 3.1, 3.2 et 3.3 of Chapter II. It is often useful to know the following: let X be a scheme, U and V open affines in X; then every point in $U \cap V$ has an open affine neighborhood W contained in $U \cap V$ which is a principal open both in U and in V. Put $U = \mathrm{Spec}(A)$ and $V = \mathrm{Spec}(B)$. Let x be in $U \cap V$. Take f in A such that $x \in D_A(f) \subset V$. Take g in B such that $x \in D_B(g) \subset D_A(f)$. This gives us a morphism of rings $B \to A_f \to B_g$. Let h be the image of g in A_f. The universal property of localization gives us two morphisms of rings between B_g and $(A_f)_h$, which are inverses of each other, hence $D_B(g)$ is a principal open in U and in V.

In fact, for all schemes that we will encounter later in this course, the problem is easierm since in these schemes the intersection of two open affines will be affine (this results from the fact that those schemes will be separated).

Let us do exercise 3.1 of [Har, II]. So we have $f\colon X \to Y$ locally of finite type, and an open affine $V = \mathrm{Spec}(A)$ in Y. We have to show that every x in $f^{-1}V$ has an open affine neighborhood $U_x = \mathrm{Spec}(B_x)$ with B_x an A-algebra of finite type. The fact that f is locally of finite type means that every y in Y has an open affine neighborhood $V_y = \mathrm{Spec}(A_y)$ such that every x in $f^{-1}V_y$ has an open affine neighborhood $U_{x,y} = \mathrm{Spec}(B_{x,y})$ in $f^{-1}V_y$, with $B_{x,y}$ of finite type over A_y. For such y and A_y, let us note that for all a in A_y such that $y \in D(a)$, the $\mathrm{Spec}((B_{x,y})_a)$ cover $f^{-1}D(a)$, and that $(B_{x,y})_a$ is an $(A_y)_a$-algebra of finite type. We conclude that there exists a basis of open affines of Y with the required property. Now let x be in $f^{-1}U$. Let y be its image in Y. We take an affine open neighborhood $V_y = \mathrm{Spec}(A_y)$ of y and an affine open neighborhood $U_{x,y} = \mathrm{Spec}(B_{x,y})$ of x in $f^{-1}V_y$ with $B_{x,y}$ of finite type over A_y. We take a in A such that $y \in D(a) \subset V_y$. Then $\mathrm{Spec}((B_{x,y})_a)$ is an affine open neighborhood of x and $(B_{x,y})_a$ is of finite type over A, since we have $A \to A_y \to A_a = (A_y)_a \to (B_{x,y})_a$.

3.2 Projective and quasi-projective S-schemes

Let S be a scheme. Recall that for all $n \geq 0$ we have the S-scheme $\mathbb{P}^n_S$. An S-scheme X will be called projective (resp., quasi-projective) if it is isomorphic to a closed subscheme (resp., locally closed subscheme) of some $\mathbb{P}^n_S$. These definitions are those from [Har] (page 103) and are not exactly equivalent to those of [EGA] (see page 103 of [Har]). These notions generalize the notions of projective and quasi-projective varieties.

3.2.1 Example. Let A be a ring and $n \geq 0$. Put $B := A[x_0, \ldots, x_n]$. Let $I \subset B$ be an ideal. Put $I_d := I \cap B_d$. Then I is called homogeneous if $I = \oplus_d I_d$. This just means that I is generated by homogeneous elements, or, equivalently, that for $b = \sum_d b_d$ in B with $b_d \in B_d$, one has $b \in I$ if and only if for all d one has $b_d \in I_d$. Such an ideal defines a closed subscheme $V(I)$ of $\mathbb{P}^n_A$ as follows. For each f homogeneous of positive degree, the intersection of $V(I)$ with $D_+(f) = \mathrm{Spec}(B_{f,0})$ is $\mathrm{Spec}(B_{f,0}/(IB_f)_0)$; one verifies that this construction glues. For S a set of homogeneous elements of B we will write $V(S)$ for $V(BS)$. The case where S has just a single element F is already interesting; if A is a field and F is non-zero we will call $V(F)$ the hypersurface defined by F. In fact, one shows [Har, II, 5.16] that every closed subscheme of $\mathbb{P}^n_A$ is of the form $V(I)$ with I a homogeneous ideal.

3.2.2 Example. Let us show that $X := \mathbb{P}^1_{\mathbb{Z}} \times_{\mathbb{Z}} \mathbb{P}^1_{\mathbb{Z}}$ is projective, by giving an isomorphism with a closed subscheme of $\mathbb{P}^3_{\mathbb{Z}}$. We have seen in (2.2) that to give a morphism from X to $\mathbb{P}^3_{\mathbb{Z}}$, it suffices to give an invertible $\mathcal{O}_X$-module $\mathcal{L}$ and global sections s_0, s_1, s_2 and s_3 that generate it. For $\mathcal{L}$ we take $\mathrm{pr}_1^*\mathcal{O}(1) \otimes \mathrm{pr}_2^*\mathcal{O}(1)$, where pr_1 and pr_2 are the two projections. Let us write the first $\mathbb{P}^1_{\mathbb{Z}}$ as $\mathrm{Proj}(\mathbb{Z}[u_0, u_1])$ and the second one as $\mathrm{Proj}(\mathbb{Z}[v_0, v_1])$. Then for the s_i we take u_0v_0, u_0v_1, u_1v_0 and u_1v_1. Let ϕ denote the morphism from X to $\mathbb{P}^3_{\mathbb{Z}}$ given by these data. Using the functorial interpretation of $\mathbb{P}^3_{\mathbb{Z}}$ given in (2.2) it is not hard to show that ϕ induces an isomorphism between X and the closed subscheme $V(x_0x_3 - x_1x_2)$ of $\mathbb{P}^3_{\mathbb{Z}}$.

3.3 Geometrically irreducible k-schemes

Let k be a field. For every k-scheme X and every k-algebra A we put $X_A := X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(A)$. For example, for X the closed subscheme of $\mathbb{A}^n_k$ defined by equations $f_1, \ldots, f_r$ (so the f_i are in $k[x_1, \ldots, x_n]$), X_A is the closed subscheme of $\mathbb{A}^n_A$ defined by the ideal $(f_1, \ldots, f_r)$ in $A[x_1, \ldots, x_n]$. For X a closed subscheme $V(f_1, \ldots, f_r)$ of $\mathbb{P}^n_k$, X_A is the closed subscheme of $\mathbb{P}^n_A$ defined by the same equations.

Let $k \to \overline{k}$ be an algebraic closure. A k-scheme X is then said to be geometrically irreducible if $X_{\overline{k}}$ is irreducible. One shows that X/k is geometrically irreducible if and only if for every extension of fields $k \to K$ one has X_K irreducible [Har, II, exer. 3.15].

In the same way, X/k is said to be geometrically reduced (integral, regular) if $X_{\overline{k}}$ is reduced (integral, regular).

3.3.1 Example. The subscheme of $\mathbb{A}^2_{\mathbb{R}}$ defined by $x^2 - 2xy + y^2 + 1$ is irreducible and integral, but not geometrically irreducible. Let k be a field of characteristic $p > 0$ and a in k an element which is not a pth power (hence k is not perfect). Then the subscheme of $\mathbb{A}^2_k$ defined by $x^p - ay^p$ is reduced, but not geometrically reduced.

3.4 Smooth k-schemes

Let k be a field. Let X be a k-scheme which is locally of finite type. Let x be in X. Then X is called smooth at x if at every point $\overline{x}$ of $X_{\overline{k}}$ lying over x the local ring $\mathcal{O}_{X_{\overline{k}},\overline{x}}$ is regular. The k-scheme X is called smooth if it is smooth at all x; this is equivalent to $X_{\overline{k}}$ being regular.

One can show that if k is of characteristic zero, then X/k is smooth if and only if X is locally of finite type and regular.

3.4.1 Example. Let k be a field of characteristic $p > 0$ and a in $k - k^p$. Then the subscheme of $\mathbb{A}^1_k$ defined by $x^p - a$ is regular, but not smooth.

3.4.2 Definition. *Let X be a scheme, locally of finite type over a field k. For x in X, the dimension of X at x is defined to be the sup of the dimensions of the irreducible components of X containing x.*

One knows that the dimension of an irreducible k-scheme which is locally of finite type is equal to the transcendence degree of $k(\eta)$ over k, where η is the generic point of X ([Har, I, Thm. 1.8A]). The following result is very useful in practice for proving smoothness for k-schemes defined by equations.

3.4.3 Theorem. *Let k be a field. Consider a closed subscheme X of $\mathbb{A}^n_k$ given by equations $f_1, \ldots, f_r$. Let x in X be a closed point, and let d be the dimension of X at x. Then X/k is smooth at x if and only if the rank of the matrix $((\partial f_j/\partial x_i)(x))$ with coefficients in $k(x)$ is equal to $n - d$. If X/k is smooth at all its closed points, then it is smooth.*

Proof. Let $\overline{x}$ be a point of $X_{\overline{k}}$ lying over x. Then $\overline{x}$ is closed and one has $k(\overline{x}) = \overline{k}$. This induces an embedding $k(x) \to \overline{k}$. Let us also denote by x the element of $X(k(x))$ which it corresponds to, and by $\overline{x}$ the corresponding element of $X(\overline{k})$. For f in $\mathcal{O}_X(X)$ we have $f(x) = x^{\#}(f) = \overline{x}^{\#}(f) = f(\overline{x})$. So we have to show that $\mathcal{O}_{X_{\overline{k}},\overline{x}}$ is regular if and only if the rank of $((\partial f_j/\partial x_i)(\overline{x}))$ equals $n - d$. It is left to the reader to show that the dimension of $X_{\overline{k}}$ at $\overline{x}$ is equal to d. Knowing this, the proof is reduced to the case where k is algebraically closed. So in what follows we suppose that $k = \overline{k}$. We can write $x = (a_1, \ldots, a_n)$ with the a_i in k. Let $I \subset \mathcal{O}_{\mathbb{A}^n_k,x}$ be the ideal $(f_1, \ldots, f_r)$, $m \subset \mathcal{O}_{\mathbb{A}^n_k,x}$ and $\overline{m} \subset \mathcal{O}_{X,x}$ the maximal ideals.

Finally, let $\overline{I}$ be the image of I in m/m^2. Then $\overline{m} = m/I$, hence $\overline{m}^2 = (m^2 + I)/I$, hence $\overline{m}/\overline{m}^2 = m/(m^2 + I)$. So we have an exact sequence of k-vector spaces:

$$0 \to \overline{I} \to m/m^2 \to \overline{m}/\overline{m}^2 \to 0.$$

The k-vector space m/m^2 is of dimension n, because the images of $x_1 - a_1, \ldots, x_n - a_n$ form a basis. The Taylor expansions of the f_j up to order one at x show that $\overline{I}$ is generated by the $\sum_i((\partial f_j/\partial x_i)(x))(x_i - a_i)$, hence the dimension of $\overline{I}$ is the rank of the jacobian matrix. The exact sequence shows that $\mathcal{O}_{X,x}$ is regular if and only if this rank is equal to $n - d$.

Suppose that X/k is smooth at all its closed points. Let $\overline{x}$ be a point of $X_{\overline{k}}$. Then take a closed point $\overline{y}$ of $X_{\overline{k}}$ in the closure of $\overline{x}$. The local ring $\mathcal{O}_{X_{\overline{k}},\overline{x}}$ is then a localization of the regular local ring $\mathcal{O}_{X_{\overline{k}},\overline{y}}$, hence regular. $\square$

4 February 2, 1996

4.1 Definition. *Let k be a field. A curve over k is a non-empty k-scheme X, locally of finite type, whose irreducible components are of dimension one.*

We can now speak of the objects that we want to study: smooth projective geometrically irreducible curves over a field. We will start by looking at some examples. The first example is the projective line: $\mathbb{P}^1_k$. Our next examples are plane curves.

4.2 Plane curves

Let $d \geq 1$ be an integer. Let $F \in k[x_0, x_1, x_2]$ be homogeneous, non-zero and of degree d. Then the closed subscheme $V(F)$ of $\mathbb{P}^2_k$ is a curve. We claim that $V(F)$ is smooth and geometrically irreducible if and only if $V(\partial F/\partial x_0, \partial F/\partial x_1, \partial F/\partial x_2, F)$ is empty, i.e., if and only if F and its partial derivatives have no common zeros. Before we prove this claim, we remark that for F homogeneous of degree d we have the identity:

$$x_0 \frac{\partial F}{\partial x_0} + x_1 \frac{\partial F}{\partial x_1} + x_2 \frac{\partial F}{\partial x_2} = dF \tag{4.2.1}$$

This identity implies that if d is invertible in k, then $V(\partial F/\partial x_0, \partial F/\partial x_1, \partial F/\partial x_2, F)$ is equal to $V(\partial F/\partial x_0, \partial F/\partial x_1, \partial F/\partial x_2)$. Let us now prove the claim. To do that, we compute the functions $x_0^{-d+1}\partial F/\partial x_1$ and $x_0^{-d+1}\partial F/\partial x_2$ on $D_+(x_0)$. Let $x := x_1/x_0$ and $y := x_2/x_0$; then we can identify $D_+(x_0)$ with $\mathbb{A}^2_k = \mathrm{Spec}(k[x, y])$ and $V(F) \cap D_+(x_0)$ with $V(f)$, with $f := F/x_0^d$. Consider a monomial $x_0^{n_0}x_1^{n_1}x_2^{n_2}$ of degree d. One verifies immediately that $x_0^{-d+1}\partial/\partial x_1$ applied to it gives $n_1x^{n_1-1}y^{n_2}$, i.e., it gives $\partial x^{n_1}y^{n_2}/\partial x$. By linearity, we get: $x_0^{-d+1}\partial F/\partial x_1 = \partial f/\partial x$. Likewise, we get $x_0^{-d+1}\partial F/\partial x_2 = \partial f/\partial y$. Let us now prove the claim.

Suppose first that $V(F)$ is smooth and geometrically irreducible. To see that F and its three partial derivatives have no common zeros we may assume that k is algebraically closed. Note that $V(F)$ is of dimension one. Let us check that F and its derivatives have no common zeros on $D_+(x_0)$. Theorem 3.4.3 and the computations that we have just done imply that F, $\partial F/\partial x_1$ and $\partial F/\partial x_2$ have no common zeros on $D_+(x_0)$. Of course, the analogous statements are true on $D_+(x_1)$ and $D_+(x_2)$.

Suppose now that F and its partial derivatives have no common zeros. Again, we may suppose that k is algebraically closed. The computations above, and Theorem 3.4.3 imply that $V(F)$ is smooth. It remains to be proved that $V(F)$ is irreducible. Suppose that $V(F)$ is not irreducible. Then F is reducible, say $F = F_1F_2$ with F_1 and F_2 both homogeneous and of degree > 0, and $V(F_1)$ and $V(F_2)$ are curves in $\mathbb{P}^2_k$. Bezout's theorem implies that $V(F_1) \cap V(F_2)$ is not empty.

Let P be a k-rational point in the intersection. Theorem 3.4.3 shows that $V(F)$ is not smooth at P. This finishes the proof of the claim.

4.2.2 Exercise. Give an example of an F in some $k[x_0, x_1, x_2]$ such that $V(F)$ is a smooth curve, and $V(\partial F/\partial x_0, \partial F/\partial x_1, \partial F/\partial x_2)$ is not empty.

Let us now look at some low degrees. One immediately sees that for $d = 1$ the curve $V(F)$ is isomorphic to $\mathbb{P}^1_k$, so that we know all about it. We move on to $d = 2$. This is already less trivial. So suppose that $C := V(F)$ is a smooth plane curve of degree two. We distinguish two cases: $C(k) = \emptyset$ and $C(k) \neq \emptyset$. In the second case, C is isomorphic to $\mathbb{P}^1_k$, as one sees by projecting from a point P in $C(k)$ onto a line L not passing through P (in fact, to make this argument rigorous one needs to show that this morphism that is defined on the complement of P extends; there is a general result for this that says that a morphism from a non-empty open part of an irreducible smooth curve to a projective k-scheme always extends to the whole curve, see [Har, I, Prop. 6.8] and [Har, II, Thm. 4.7]). Note that if k is algebraically closed, one is always in this second case. It is clear that in the first case, C is not isomorphic to $\mathbb{P}^1_k$, but that $C_{\overline{k}}$ is isomorphic to $\mathbb{P}^1_{\overline{k}}$. This first case really occurs, for example, take $x_0^2 + x_1^2 + x_2^2$ in $\mathbb{R}[x_0, x_1, x_2]$. So we see that it can happen that two k-schemes are geometrically isomorphic but not isomorphic. This is an interesting phenomenon, that can be described in terms of Galois cohomology (if k is perfect).

4.2.3 Exercise. Show that there are infinitely many smooth plane curves of degree two over $\mathbb{Q}$ that are pairwise not isomorphic. Show that for a smooth plane curve C of degree two over a field k such that $C(k)$ is empty, there is a quadratic extension K of k such that C_K is isomorphic to $\mathbb{P}^1_K$. Give an example to show that such extensions are not unique.

So every smooth plane curve of degree two becomes isomorphic to a projective line over an extension of k of degree at most two. We will now see that things are completely different in degree three.

Let C be a smooth plane curve of degree three, over some field k. We claim that C is not isomorphic to $\mathbb{P}^1_k$. One way to see this is to remark that on C there are global non-zero differential forms and on that on $\mathbb{P}^1_k$ there aren't. At this moment this method is not very convincing, because we have not yet talked about differential forms. So let us try something else. Suppose that k is not of characteristic two or three and that $C = V(F)$ with $x_0^{-3}F$ of the form $f = -y^2 + x^3 + ax + b$. (One can show (we will do this later), that every smooth plane C of degree three over such a field k is isomorphic to one given by an equation of this type, if and only if $C(k)$ is not empty.) Then C has an automorphism σ of order two: $\sigma^\#$ maps x to x and y to $-y$. One verifies easily that σ fixes exactly four elements of $C(\overline{k})$. I leave it as an exercise to the reader to show that an automorphism σ of order two of $\mathbb{P}^1_k$ with k not of characteristic two fixes exactly two elements of $\mathbb{P}^1(\overline{k})$. (First show, using Section 2.2, that $\mathrm{Aut}_k(\mathbb{P}^1_k)$ is the group $\mathrm{PGL}_2(k) := \mathrm{GL}_2(k)/k^*$.) We will see later that for k algebraically closed there is a bijection between k and the set of isomorphism classes of smooth plane curves of degree three over k. To give some idea of what a smooth plane curve C of degree d looks like, we will consider the case $k = \mathbb{C}$, and study $C(\mathbb{C})$ as a topological manifold.

4.3 Algebraic topology of complex smooth plane curves

Let $C = V(F)$ be a smooth plane curve of some degree d over $\mathbb{C}$. Instead of considering C with its Zariski topology, we will now consider $C(\mathbb{C})$ with the topology induced from the usual topology on $\mathbb{C}$. Let us first note that $\mathbb{P}^2(\mathbb{C})$ is a union of three copies of $\mathbb{C}^2$, whose mutual intersections are open in $\mathbb{C}^2$. This gives a topology on $\mathbb{P}^2(\mathbb{C})$ that induced the usual topology on each of our three copies of $\mathbb{C}^2$. It is easy to give $\mathbb{P}^2(\mathbb{C})$ the structure of a complex analytic manifold of dimension two, but for the moment we will not use that. The topology that we have just defined on $\mathbb{P}^2(\mathbb{C})$ induces a topology on $C(\mathbb{C})$. The fact that C is smooth and irreducible implies that $C(\mathbb{C})$ is a connected orientable compact topological manifold of dimension two (in fact it is even a complex analytic manifold of dimension one). By the classification of such topological manifolds, it follows that $C(\mathbb{C})$ is homeomorphic to a sphere with g handles, for some $g \geq 0$. We will compute this number, which is called the genus of $C(\mathbb{C})$.

Let P_0 be in $\mathbb{P}^2(\mathbb{C})$ but not in $C(\mathbb{C})$ and let us study the morphism $\phi\colon C \to \mathbb{P}^1_{\mathbb{C}}$ given by projecting from P_0 onto some line not containing P_0. First of all, we note that for all but finitely many points Q of $\mathbb{P}^1_{\mathbb{C}}$, $\phi^{-1}Q$ has exactly d elements. In fact, there are only finitely many points, say $P_1, \ldots, P_r$ in $C(\mathbb{C})$, such that the tangent line of C at it passes through P_0. The implicit function theorem implies that the morphism of topological spaces $\phi\colon C(\mathbb{C}) - \{P_1, \ldots, P_r\} \to \mathbb{P}^1(\mathbb{C})$ is, locally on $C(\mathbb{C}) - \{P_1, \ldots, P_r\}$, an isomorphism.

The number r depends on the point P, but we will argue that there is a non-empty Zariski open subset of $\mathbb{P}^2_{\mathbb{C}}$ on which it takes its maximal value, and we will compute that value. It is an exercise for the reader to compute that the tangent line to C at P in $C(\mathbb{C})$ is given by the equation:

$$\frac{\partial F}{\partial x_0}(P)x_0 + \frac{\partial F}{\partial x_1}(P)x_1 + \frac{\partial F}{\partial x_2}(P)x_2 = 0 \tag{4.3.1}$$

It follows that $P_0 = (p_0, p_1, p_2)$ lies on the tangent line to C at P in $C(\mathbb{C})$ if and only if

$$G_{P_0}(P) := (\partial F/\partial x_0)(P)p_0 + (\partial F/\partial x_1)(P)p_1 + (\partial F/\partial x_2)(P)p_2 = 0,$$

which is an equation of degree at most $d-1$ for P. The three partial derivatives of F are linearly independent over $\mathbb{C}$ because C is smooth (verify!), hence G_{P_0} is non-zero and of degree $d-1$. Since F is irreducible, $V(G_{P_0})$ and C have no irreducible component in common, hence by Bezout's theorem there are at most $d(d-1)$ points on C where the tangent line contains P_0. For P in $C(\mathbb{C})$, let $m(P)$ denote the intersection multiplicity at P of C and its tangent line. By the definition of tangent line one has $m(P) \geq 2$. We assume known the fact that (over a field of characteristic zero) there are only finitely many P with $m(P) > 2$ (these are called flexes; they are given by the so-called Hessian equation), if $d > 1$. Let's say that the case $d = 1$ is easy, and that we suppose $d > 1$. Let P be in $C(\mathbb{C})$ such that the tangent to C at P contains P_0. A (not so very nice but not difficult) computation shows that $V(G_{P_0})$ and C intersect transversally at P if and only if $m(P) > 2$. Hence if we take P_0 outside the union of C and the tangents to C at the finitely many P such that $m(P) > 2$, then $V(G_{P_0}) \cap C$ has exactly $d(d-1)$ elements. We suppose that we have taken P_0 like that; then $r = d(d-1)$.

The fact that the $m(P_i) = 2$ $(1 \leq i \leq r)$ implies that there are open neighborhoods $U_i \subset C(\mathbb{C})$ of P_i and $V_i \subset \mathbb{P}^1(\mathbb{C})$ of $Q_i := \phi(P_i)$ such that $\phi U_i = V_i$ and $\phi|U_i \to V_i$ is isomorphic to $D \to D$, $z \mapsto z^2$, with D the open unit disk in $\mathbb{C}$.

We will now compare the Euler characteristics of $C(\mathbb{C})$ and $\mathbb{P}^1(\mathbb{C})$ by triangulating both of them in a compatible way. We add a few points to the Q_i, say $Q_{r+1}, \ldots, Q_v$ such that we can triangulate $\mathbb{P}^1(\mathbb{C})$ such that the vertices are exactly the Q_i. Let e be the number of edges in our triangulation, and f be the number of faces. From what we know about ϕ it follows that we get a triangulation of $C(\mathbb{C})$ by taking the elements of the $\phi^{-1}Q_i$ as vertices, the closures of the inverse images of the edges minus their endpoints as edges, and the closures of the inverse images of the faces minus their vertices as faces. The numbers of vertices, edges and faces in this triangulation are $(d-1)r + d(v-r)$, de and dv. The Euler characteristic of $\mathbb{P}^1(\mathbb{C})$, which is a sphere, equals two, hence: $v - e + f = 2$. It follows that the Euler characteristic of $C(\mathbb{C})$ equals $2d - r = 2d - d(d-1) = d(3-d)$. By definition, this is equal to $2 - 2g$, hence $g = (d-1)(d-2)/2$. For example: for $d = 1$ and $d = 2$ we find what we knew, genus zero. For $d = 3$ we have genus one, a torus. For $d = 4$, a sphere with three handles. As a consequence we obtain that, at least over $\mathbb{C}$, two smooth plane curves of different degrees cannot be isomorphic, unless the degrees are one and two. Also, there are no smooth plane curves over $\mathbb{C}$ of genus two. We will see that there exist smooth projective irreducible curves over $\mathbb{C}$ of genus two by some other method.

5 February 16, 1996

Last time we looked at plane curves to get examples of smooth projective geometrically irreducible curves. We have seen that, at least over $\mathbb{C}$, the genus of a smooth plane curve of degree d equals $(d-1)(d-2)/2$. It follows that we cannot get examples of curves of genus two in that way. We will now describe a construction that gives us more examples.

5.1 Normalization

See also [Har, II, exer. 3.8]. Let X be an integral scheme and let η be its generic point. The local ring $K(X) := \mathcal{O}_{X,\eta}$ is then a field, called the function field of X. Let $U = \operatorname{Spec}(A)$ be a non-empty affine open subscheme of X. Then U contains η and $K(X)$ is the fraction field of its subring A. Let $\widetilde{A}$ be the integral closure of A in $K(X)$. We get a morphism of schemes $\widetilde{U} := \operatorname{Spec}(\widetilde{A}) \to U$. Since taking the integral closure commutes with localization, these morphisms glue and we get a morphism $\pi \colon \widetilde{X} \to X$ called the normalization of X. An integral scheme is called normal if all its local rings are integrally closed in their fraction field; the scheme $\widetilde{X}$ has this property. Also, $\widetilde{X}$ is integral and we have $K(\widetilde{X}) = K(X)$. By construction, π is an affine morphism. It has the following universal property: if $f \colon Z \to X$ is a dominant morphism with Z normal then f factors uniquely through π. Under certain conditions, e.g., if X is of finite type over a field, π is a finite morphism, i.e., every $\widetilde{A}$ is an A-module of finite type, and an isomorphism over a non-empty open subset of X. If all local rings of X are normal, for example, when they are regular, π is an isomorphism.

This construction can be generalized as follows: let $K(X) \to L$ be a finite field extension. Then instead of taking for $\widetilde{A}$ the integral closure of A in $K(X)$, we can take it in L. This gives a morphism $\pi \colon \widetilde{X} \to X$ that is called the normalization of X in L. It has a universal property similar to that of the normalization of X. If X is a scheme of finite type over a field, π is finite.

5.1.1 Example. Let $X = \operatorname{Spec}(\mathbb{Z})$ and K a number field, i.e., a finite extension of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in K is called the ring of integers in K and is denoted O_K. One can show, using the $\mathbb{Q}$-bilinear form $K \times K \to \mathbb{Q}$, $(x, y) \mapsto \operatorname{trace}_{K/\mathbb{Q}}(xy)$, that O_K is a free $\mathbb{Z}$-module of rank $\dim_{\mathbb{Q}}(K)$. It is a hard problem to determine a $\mathbb{Z}$-basis of O_K, if K is given in the form $\mathbb{Q}[x]/(f)$; there is at present no polynomial time algorithm that can do this, not even for quadratic fields. For quadratic fields the situation is not too complicated. Let K be a quadratic extension of $\mathbb{Q}$. There exists a unique square free integer d such that $K = \mathbb{Q}(\sqrt{d})$. If $d \equiv 1(4)$ then $O_K = \mathbb{Z}[(\sqrt{d}-1)/2]$ and otherwise $O_K = \mathbb{Z}[\sqrt{d}]$. One can show this by showing that all localizations at maximal ideals of these rings are regular.

5.1.2 Proposition. *Let k be an algebraically closed field and X a (geometrically) integral curve over k. Then its normalization $\widetilde{X}$ is a smooth integral curve. If X is projective, then so is $\widetilde{X}$.*

Proof. We admit that $\pi\colon \widetilde{X} \to X$ is finite. That shows that $\widetilde{X}$ is an integral curve over k. By definition, it is smooth if and only if all its local rings are regular. The local ring at the generic point is a field, hence regular. Let x be a closed point. Since k is algebraically closed, it is a k-rational point. We know that its local ring A is integral, noetherian, of dimension one and integrally closed. Proposition 3 of [Serre, Corps Locaux, I, §2] shows that A is a discrete valuation ring, hence regular. (The proof of this proposition proceeds as follows: let $m \subset A$ be the maximal ideal, let m' be the set of elements x in the fraction field K of A such that $xA \subset m$; then mm' is either A or m; if $mm' = m$ one has $m' = A$ since A is integrally closed and one has $m' \neq A$ since A is local of dimension one; hence $mm' = A$ and it follows that m is principal.)

We admit for the moment that $\widetilde{X}$ is projective if X is. We can show that later, as a consequence of the Riemann–Roch theorem for smooth proper geometrically irreducible curves. Another way to show that $\widetilde{X}$ is a projective k-scheme is to show the more general statement that if X is a projective k-scheme and $Y \to X$ is a finite morphism, then Y is a projective k-scheme. $\square$

5.1.3 Remark. The condition that k be algebraically closed in the previous proposition cannot be dropped, as the following example shows. Let $p > 2$ be a prime number, k a field of characteristic p and a in $k - k^p$. The affine plane curve $V(-y^2 + x^p - a) \subset \mathbb{A}^2_k$ is regular and geometrically integral, but not smooth: over $\overline{k}$ it is isomorphic to $V(-y^2 + x^p)$ which is singular at the origin.

5.1.4 Proposition. *Let k be an algebraically closed field and X a (geometrically) integral curve over k. Let $K(X) \to L$ be a separable finite field extension. The normalization $\widetilde{X}$ of X in L is a smooth integral curve. If X is projective, then so is $\widetilde{X}$.*

After admitting that $\pi\colon \widetilde{X} \to X$ is finite, the proof of this proposition is the same as the one of Proposition 5.1.2, so we don't repeat it. Instead, we will look at some examples.

5.2 Hyperelliptic curves

Let k be a field of characteristic different from 2. Let L be a quadratic extension of the function field $k(x)$ of $\mathbb{P}^1_k$. We will use the following notation: $\mathbb{P}^1_k$ is constructed from the graded k-algebra $k[x_0, x_1]$, $x := x_1/x_0$ and $y := x_0/x_1$. There is a square free f in $k[x]$, unique up to multiplication by squares of non-zero elements of k, such that $L = k(x)(\sqrt{f})$. Let $\pi\colon C \to \mathbb{P}^1_k$ be the normalization of $\mathbb{P}^1_k$ in L. We want to describe C at least locally on $\mathbb{P}^1_k$ and we want to prove that C is projective. If $k = \mathbb{C}$ we want to know what $C(\mathbb{C})$ is, topologically.

If f is of degree zero, then L is of the form $k'(x)$, with k' a quadratic extension of k. It is left to the reader to show that $C = \mathbb{P}^1_{k'}$.

We suppose that f is separable and of degree $d > 0$. Note that in general the condition that f be square free does not imply that f is separable. Consider the ring $A := k[x, u]/(u^2 - f)$. We claim that it is the integral closure of $k[x]$ in L. To prove that, it is sufficient to see that A is integrally closed. Now $\mathrm{Spec}(A)$ is a smooth curve, by the jacobian criterion (f has no multiple root in $\overline{k}$). Hence A is integrally closed. This is a perfectly simple description of $C - \pi^{-1}\infty$. Let us now study what happens over the other standard affine open $\mathrm{Spec}(k[y])$.

We write $f = a_d x^d + \cdots + a_0$. We have $a_d \neq 0$. Since $x = y^{-1}$ in $k(x) = k(y)$ we also have: $f = a_d y^{-d} + \cdots + a_0 = y^{-d}(a_d + \cdots + a_0 y^d)$. For d even we put $g := a_d + \cdots + a_0 y^d$ and for d odd we put $g := a_d y + \cdots + a_0 y^{d+1}$. Then we have $L = k(y)(\sqrt{g})$. Consider the ring $B := k[y, v]/(v^2 - g)$. Just as before, we know that g has no multiple root in $\overline{k}$, hence $\mathrm{Spec}(B)$ is smooth over k and it is the normalization of $\mathrm{Spec}(k[y])$ in L.

So finally we have the following global description of C: it is covered by the two open affines $\mathrm{Spec}(A)$ and $\mathrm{Spec}(B)$, the glueing datum being the isomorphism $A_x \to B_y$ making y correspond to x^{-1} and v to $x^{-d/2}u$ (resp., $x^{(-d-1)/2}u$) if d is even (resp., odd). We conclude that C is a smooth and geometrically irreducible curve. The results on the projectivity of normalizations mentioned in the proof of Proposition 5.1.2 imply that C is projective. It would be a nice exercise to show directly, "by hand", that C is projective.

Suppose now that $k = \mathbb{C}$. Just as for plane curves, it is not so hard to find out what the genus of $C(\mathbb{C})$ is. Suppose for simplicity that d is even. Let $Q_1, \ldots, Q_d$ be the zeros of f in $\mathbb{P}^1(\mathbb{C})$. For each i, let P_i be the unique element of $\pi^{-1}Q_i$. Then the map $\pi\colon C(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ is ramified of degree two at each P_i and its restriction to $C(\mathbb{C}) - \{P_1, \ldots, P_d\}$ is a covering of $\mathbb{P}^1(\mathbb{C}) - \{Q_1, \ldots, Q_d\}$. One finds that the Euler characteristic of $C(\mathbb{C})$ is $4 - d$, hence the genus of C is $d/2 - 1$. An analogous computation shows that for d odd the genus is $(d-1)/2$.

5.3 Curves and function fields

See also [Har, I, §6]. Let k be an algebraically closed field. If C is a smooth projective irreducible curve over k, then its function field $K(C)$ is a finitely generated field extension of k, of transcendence degree one. Let $f\colon C \to D$ be a morphism of projective smooth irreducible curves over k. Since C is projective and D is separated, the image of f is closed in D (see [Har, II, exer. 4.4 and Thm. 4.9]). So either f is constant (i.e., its image is just one point), or it is surjective. In the last case f induces a morphism $K(D) \to K(C)$ of k-algebras. It follows that we have a contravariant functor $X \mapsto K(X)$ from the category of smooth projective irreducible curves over k with dominant morphisms to the category of field extensions of k.

We define a function field over k of dimension one to be a field extension K which is finitely generated and of transcendence degree one. By definition, the functor $X \mapsto K(X)$ is in fact a functor to the full subcategory of function fields over k of dimension one.

5.3.1 Theorem. *The functor $X \mapsto K(X)$ is an anti-equivalence between the category of smooth projective irreducible curves over k with dominant morphisms and the category of function fields over k of dimension one.*

A proof can be found in [Har]. In order to prove that the functor is essentially surjective, i.e., that each function field K over k of dimension one is isomorphic to the function field of some projective smooth irreducible curve over k, one can argue as follows. Take x in K such that the extension $k(x) \to K$ is finite and separable. Let C be the normalization of $\mathbb{P}^1_k$ in K. Then $K = K(C)$.

6 February 23, 1996

I recall that the principal aim of this course is to construct the jacobian varieties associated to projective smooth geometrically irreducible curves over arbitrary fields. In order to do that, we have to understand some properties of line bundles on such curves.

6.1 Line bundles and divisors on curves

See also [Har, II, §6]. Let k be a field and C a smooth projective geometrically irreducible curve over k. A line bundle on C is by definition an invertible $\mathcal{O}_C$-module. Let C_0 be the set of closed points of C. The group $\mathrm{Div}(C)$ of (Weil) divisors on C is the free $\mathbb{Z}$-module with basis C_0. Equivalently, $\mathrm{Div}(C)$ is the sub-$\mathbb{Z}$-module of $\mathbb{Z}^{C_0}$ of functions with finite support. (Note that $\oplus_{C_0}\mathbb{Z}$ is not equal to $\prod_{C_0}\mathbb{Z}$. The second is the $\mathbb{Z}$-dual of the first; it is an interesting exercise to show that the canonical map from $\oplus_{C_0}\mathbb{Z}$ to the $\mathbb{Z}$-dual of $\prod_{C_0}\mathbb{Z}$ is an isomorphism if C_0 is countable.)

The main interest in divisors comes from the connections between $\mathrm{Div}(C)$, $k(C)^*$ and $\mathrm{Pic}(C)$, the group of isomorphism classes of line bundles on C. For x in C_0 let $v_x\colon k(C)^* \to \mathbb{Z}$ be the valuation associated to x: if t_x is a uniformizer at x, i.e., a generator of the maximal ideal m_x of $\mathcal{O}_{C,x}$, then $ft_x^{-v_x(f)}$ is in $\mathcal{O}_{C,x}^*$; this does not depend on the choice of t_x. Let f be in $k(C)^*$. We claim that there are only finitely many x in C_0 such that $v_x(f) \neq 0$. To prove this, let $U = \mathrm{Spec}(A)$ be a non-empty affine open of C, let a and b be non-zero elements of A such that $f = a/b$, then all x in C_0 for which $v_x(f) \neq 0$ are in $C - U$ or in $V(a)$ or in $V(b)$, which leaves only finitely many possibilities. It follows that we can define the divisor map:

$$\mathrm{div}\colon k(C)^* \to \mathrm{Div}(C), \qquad f \mapsto \sum_{x\in C_0} v_x(f)\, x \tag{6.1.1}$$

This map is a morphism of groups. We will now first study its kernel and image. The image is called the group of principal divisors.

6.1.2 Definition. *Let $D = \sum_x n_x x$ be a divisor on C. Then the degree of D is given by:*

$$\deg(D) := \sum_x n_x \dim_k k(x)$$

The reason to include the "weights" $\dim_k k(x)$ is that after base change to $\overline{k}$ the point x gives a divisor of that degree; if $k \to k(x)$ is separable then x gives $\dim_k k(x)$ reduced points of $C_{\overline{k}}$; if $k \to k(x)$ is purely inseparable then x gives one point with multiplicity $\dim_k k(x)$ of $C_{\overline{k}}$. The map $D \mapsto \deg(D)$ is a morphism of $\mathbb{Z}$-modules from $\mathrm{Div}(C)$ to $\mathbb{Z}$. For r in $\mathbb{Z}$ we let $\mathrm{Div}^r(C)$

be the set of divisors of degree r. In order to continue, we need the notions of pullback and pushforward of divisors. Let $f\colon C \to C'$ be a dominating morphism between projective smooth geometrically irreducible curves over k. Let x be in C'_0. We can view x as a reduced closed subscheme of C'. Let $f^{-1}x$ be the inverse image in C of this closed subscheme under f. The support of $f^{-1}x$ consists of the finitely many y in C_0 with $f(y) = x$. Let t_x be a uniformizer at x. At each y in $f^{-1}x$, the closed subscheme $f^{-1}x$ is defined by the element $f^{\#}(t_x)$ of $\mathcal{O}_{C,y}$, i.e., by the $v_y(f^{\#}(t_x))$th power of m_y. We define f^*x in $\mathrm{Div}(C)$ to be $\sum_y v_y(f^{\#}(t_x))y$, where the sum runs over the y mapping to x. Since $\mathrm{Div}(C')$ is the free $\mathbb{Z}$-module with basis C'_0, we can extend this map $f^*\colon C'_0 \to \mathrm{Div}(C)$ uniquely to all of $\mathrm{Div}(C')$. We can also define a map $f_*\colon \mathrm{Div}(C) \to \mathrm{Div}(C')$ as follows: $f_*(\sum_x n_x x) = \sum_x n_x \dim_{k(f(x))}(k(x))f(x)$. Proposition 6.9 of [Har, II] says that $\deg \circ f^* = \dim_{k(C')}(k(C)) \deg$, as maps from $\mathrm{Div}(C')$ to $\mathbb{Z}$. The number $\dim_{k(C')}(k(C))$ is called the degree of f. The proof of [Har, II, Prop. 6.9] shows that $f_*\circ f^*$ is multiplication by $\deg(f)$ on $\mathrm{Div}(C')$. Let us give a sketch of the proof of [Har, II, Prop. 6.9]. By [Har, II, Prop. 6.8], f is a finite morphism. Let x be in C'_0 and let $U = \mathrm{Spec}(A)$ be an open neighborhood of x in C'. Then $f^{-1}U$ is an affine open, $\mathrm{Spec}(B)$ say, of C. Now B is finitely generated as A-module, and torsion free since it is in $k(C)$ which is itself a field extension of $k(C')$. It follows that $B \otimes_A \mathcal{O}_{C',x}$ is a free $\mathcal{O}_{C',x}$-module of rank $\deg(f)$.

6.1.3 Proposition. *The kernel of* div *is the subgroup* k^* *of* $k(C)^*$*, and the image of* div *is contained in* $\mathrm{Div}^0(C)$*.*

Proof. If C is the projective line, one checks this proposition by hand. This verification is left to the reader. Intuitively, it says that a rational function on C has as many poles as zeros, and if it has no poles then it is constant. Let us first prove that $\ker(\mathrm{div}) = k^*$. Let f be in $k(C)^*$ such that $\mathrm{div}(f)$ is zero. Assume that f is not in k^*. The element f of $k(C)^*$ is transcendent over k because otherwise C would not be geometrically irreducible. By Thm. 5.3.1 we can view f as a dominating morphism to $\mathbb{P}^1_k$, namely, f gives a morphism of k-algebras $k(t) \to k(C)$ that sends t to f. By [Har, II, Prop. 6.8], this morphism f is surjective. But then there exist x in C such that $f(x)$ is the point zero in $\mathbb{P}^1_k$ and for such a point x one has $v_x(f) > 0$, which is a contradiction. Let us now prove that any principal divisor has degree zero. Let f be in $k(C)^*$ and put $D := \mathrm{div}(f)$. If f is in k^* then $D = 0$ hence $\deg(D) = 0$. We assume that f is not in k^*. Then, as we have just seen, we can view f as a surjective morphism from C to $\mathbb{P}^1_k$. Again using [Har, II, Prop. 6.8] we see that f is a finite morphism. By definition, we have: $D = f^*0 - f^*\infty = f^*(0 - \infty)$. Hence $\deg(D) = \deg(f)\deg(0 - \infty) = 0$. ☐

The next topic is the connection between divisors and line bundles. Let $D = \sum_x n_x x$ be in

$\operatorname{Div}(C)$. Then we define a presheaf $\mathcal{L}(D)$ on C by:

$$\mathcal{L}(D)(U) = \{f \in k(C) \mid \forall x \in U_0\colon v_x(f) \geq -n_x\} \tag{6.1.4}$$

One verifies immediately that $\mathcal{L}(D)$ is a sheaf and that it is an $\mathcal{O}_C$-module. We claim that it is an invertible $\mathcal{O}_C$-module. Let us prove that. Let x be in C_0. If $n_x = 0$ let U be the complement of the support of D; then $\mathcal{L}(D)|_U$ is equal to $\mathcal{O}_C|_U$. In general, let $U := \{x\} \cup (C - \operatorname{Supp}(D))$. Let t_x be a uniformizer at x. Let $U' \subset U$ be a neighborhood of x on which t_x is defined and has x as its only zero. Multiplication by $t_x^{-n_x}$ induces an isomorphism from $\mathcal{O}_C|_{U'}$ to $\mathcal{L}(D)|_{U'}$. Since $\mathcal{L}(D)$ is an invertible $\mathcal{O}_C$-module, we get a map from $\operatorname{Div}(C)$ to $\operatorname{Pic}(C)$ sending D to the isomorphism class $[\mathcal{L}(D)]$ of $\mathcal{L}(D)$.

There is also a (non-unique) way of associating divisors to line bundles. Let $\mathcal{L}$ be a line bundle. Let η be the generic point of C. By definition, $\mathcal{L}_\eta$ is a one dimensional $k(C)$-vector space. Let s be a basis of it. We will now define the divisor $\operatorname{div}(s)$ of the rational section s of $\mathcal{L}$. Let x be in C_0 and s_x a basis of the $\mathcal{O}_{C,x}$-module $\mathcal{L}_x$. The valuation of s at x is then defined to be $v_x(s) := v_x(s/s_x)$ (this does not depend on the choice of s_x), and $\operatorname{div}(s) := \sum_x v_x(s)x$. Write $D := \operatorname{div}(s)$. Then we have a morphism of $\mathcal{O}_C$-modules $\mathcal{L}(D) \to \mathcal{L}$ which on every U sends f to fs. By construction, this map is an isomorphism.

6.1.5 Proposition. *The map $D \mapsto [\mathcal{L}(D)]$ is a morphism of groups from $\operatorname{Div}(C)$ to $\operatorname{Pic}(C)$, and the following sequence is exact:*

$$0 \to k^* \to k(C)^* \to \operatorname{Div}(C) \to \operatorname{Pic}(C) \to 0$$

Proof. The fact that the map is a morphism of groups is left to the reader. Let us show that the sequence is exact at $\operatorname{Div}(C)$. Let f be in $k(C)^*$. Then multiplication by f^{-1} induces an ismorphism from $\mathcal{O}_C$ to $\mathcal{L}(\operatorname{div}(f))$. This shows that $[\mathcal{L}(D)]$ is zero if D is a principal divisor. It remains to show the converse. So let D be a divisor such that $[\mathcal{L}(D)] = 0$. Let $\phi\colon \mathcal{O}_C \to \mathcal{L}(D)$ be an isomorphism. Let $f := \phi(1)$. Since 1 is a basis of $\mathcal{O}_C$, f is a basis of $\mathcal{L}(D)$. Hence for any open $U \subset C$ and g in $k(C)^*$ we have $gf \in \mathcal{L}(D)(U)$ if and only if $g \in \mathcal{O}(U)$. The first condition is equivalent to: $\operatorname{div}(g)|_U + \operatorname{div}(f)|_U \geq -D|_U$ (the ordering is the partial ordering in which $\sum_x n_x x \geq \sum_x m_x x$ iff $n_x \geq m_x$ for all x). The second condition is equivalent to: $\operatorname{div}(g)|_U \geq 0$. It follows that $\operatorname{div}(f) = -D$. Hence D is a principal divisor. We have now shown exactness at $\operatorname{Div}(C)$. It remains to show exactness at $\operatorname{Pic}(C)$. But we have already seen that every line bundle is isomorphic to one of the form $\mathcal{L}(D)$. □

Let us finish this section on divisors and line bundles with a motivation for the study of them. It is reasonable to want to understand the set of rational functions on a curve with poles and zeros of some prescribed kind, for example, the f in $k(C)^*$ with $\operatorname{div}(f) \geq -D$ for a given divisor D. If one adds the function 0 to this set one obtains a k-vector space $L(D)$. By the definition of $\mathcal{L}(D)$, this space $L(D)$ is the set of its global sections. One can then get information on the dimensions $l(D)$ of the spaces $L(D)$ by applying the machinery of sheaves and cohomology. The problem of determining $l(D)$ as a function of certain invariants of D as for example $\deg(D)$ is the Riemann–Roch problem. The answer to this problem will be given after we have treated the necessary theory concerning differential forms.

6.2 Differential forms

See also [Har, II, §8]. Before introducing differential calculus on schemes, let us recall the definition of the tangent bundle and such on C^∞-manifolds. The tangent bundle of $\mathbb{R}^n$ is by definition just the product $\mathbb{R}^n \times \mathbb{R}^n$. For X an n-dimensional manifold one defines its tangent bundle TX by glueing the tangent bundles of charts of X. Up to canonical isomorphism, the TX one obtains does not depend on the choice of the charts. There are more intrisic ways of defining TX. The tangent space $TX(x)$ of X at x is the set of equivalence classes of parametrized curves through x, where two of them are equivalent if they give the same tangent vector in some chart (and hence in all charts). A still more intrinsic way to define $TX(x)$ is to make its elements v act on germs of C^∞-fuctions at x by taking derivative at x in the direction v. This identifies $TX(x)$ with the $\mathbb{R}$-vector space of $\mathbb{R}$-derivations $\operatorname{Der}_{\mathbb{R}}(\mathcal{O}_{X,x}, \mathbb{R})$, where $\mathcal{O}_X$ denotes the sheaf on X of C^∞-functions. One easily sees that $\operatorname{Der}_{\mathbb{R}}(\mathcal{O}_{X,x}, \mathbb{R})$ is canonically isomorphic to the dual of m_x/m_x^2, where m_x is the maximal ideal in $\mathcal{O}_{X,x}$. It is a general principle that instead of working with vector bundles one can work with their sheaves of C^∞-sections: to a vector bundle $p\colon E \to X$ one associates the sheaf C_E^∞ that sends U to the $\mathcal{O}_X(U)$-module of C^∞-sections of $p\colon p^{-1}U \to U$. This gives a locally free $\mathcal{O}_X$ module C_E^∞. It is not very complicated to reconstruct $p\colon E \to X$ from C_E^∞. A section of C_{TX}^∞ over U is, by the usual definition in differential topology, a vector field on U. The interpretation of the tangent space as a space of derivations shows that $C_{TX}^\infty(U) = \operatorname{Der}_{\mathbb{R}}(\mathcal{O}_X(U), \mathcal{O}_X(U))$. This motivates the following constructions.

Let $A \to B$ be a morphism of rings. For M a B-module we let $\operatorname{Der}_A(B, M)$ be the B-module of A-derivations of B to M, i.e., $\operatorname{Der}_A(B, M)$ is the set of A-linear maps D from B to M satisfying Leibniz's rule: $D(fg) = fD(g) + gD(f)$. One verifies that this is indeed a B-module if one defines $(bD)(f) = bD(f)$. For D in $\operatorname{Der}_A(B, M)$ one has: $D(1) = D(1^2) = D(1)+D(1)$, hence $D(1) = 0$, and it follows that $D(a) = 0$ for all a in A.

6.2.1 Proposition. *Let $A \to B$ be a morphism of rings. There exists an A-derivation $d\colon B \to \Omega^1_{B/A}$ such that for every A-derivation $D\colon B \to M$ there is a unique B-linear map $f : \Omega^1_{B/A} \to M$*

such that $D = f\circ d$. In other words, d is the universal derivation.

Proof. One constructs d as follows. Take the free B-module with basis $\{d(b)\,|\,b\in B\}$ (here the $d(b)$ are supposed to be distinct). Then $\Omega^1_{B/A}$ is the quotient of this free B-module by the submodule generated by the relations $d(ab) = ad(b)$, $d(b_1+b_2) = d(b_1)+d(b_2)$ and $d(b_1b_2) = b_1d(b_2)+b_2d(b_1)$ for all a in A and b, b_1 and b_2 in B. $\square$

6.2.2 Example. Let $B := A[x_1,\ldots,x_n]$, the polynomial ring in n variables. We claim that $\Omega^1_{B/A}$ is the free B-module with basis $dx_1,\ldots,dx_n$. To prove this, it is enough to note that the two B-modules represent the same functor. So one just has to show that for a B-module M the map $\mathrm{Der}_A(B,M)\to M^n$ that sends D to $(D(x_1),\ldots,D(x_n))$ is an isomorphism. This is left to the reader.

6.2.3 Example. Let $A\to B$ be a morphism of rings, let $I\subset B$ be an ideal and put $C := B/I$. Let $\pi\colon B\to C$ be the canonical projection. Let M be a C-module. We have an exact sequence:

$$0\to \mathrm{Der}_A(C,M)\to \mathrm{Der}_A(B,M)\to \mathrm{Hom}_C(I/I^2,M)$$

in which D in $\mathrm{Der}_A(C,M)$ is mapped to $D\circ\pi$ and D in $\mathrm{Der}_A(B,M)$ is mapped to $D|_I$. Interpreting this in terms of the universal derivations, we get the exact sequence:

$$I/I^2\to C\otimes_B\Omega^1_{B/A}\to\Omega^1_{C/A}\to 0$$

Note that this gives an explicit presentation of $\Omega^1_{C/A}$ if $B = A[x_1,\ldots,x_n]$ and $I = (f_1,\ldots,f_r)$.

7 February 23, 1996

7.1 Differential forms, continued

We begin by listing some more properties of the module of differentials $\Omega^1_{B/A}$.

7.1.1 Proposition. *1. Let $A \to B \to C$ be morphisms of rings. We have a natural morphism of C-modules: $C \otimes_B \Omega^1_{B/A} \to \Omega^1_{C/A}$. These morphisms will induce pullback morphisms of differential forms on schemes.*

2. Let $A \to B$ be a morphism of rings. Let $S \subset B$ be a multiplicative system; then the natural map $S^{-1}\Omega^1_{B/A} \to \Omega^1_{S^{-1}B/A}$ is an isomorphism.

3. Let $A \to B$ and $A \to A'$ be morphisms of rings. Put $B' := A' \otimes_A B$. The natural morphism $B' \otimes_B \Omega^1_{B/A} \to \Omega^1_{B'/A'}$ is an isomorphism.

4. Let $A \to B \to C$ be morphisms of rings. The sequence

$$C \otimes_B \Omega^1_{B/A} \to \Omega^1_{C/A} \to \Omega^1_{C/B} \to 0$$

is exact.

The proofs are quite straightforward and can be found in [Har, II, §8]. We will now define differential forms on schemes. Let $f\colon X \to Y$ be a morphism of schemes. For each pair of affine opens $\operatorname{Spec}(B)$ in X and $\operatorname{Spec}(A)$ in Y such that $f(\operatorname{Spec}(B)) \subset \operatorname{Spec}(A)$ we have the B-module $\Omega^1_{B/A}$. The fact that $\Omega^1_{B/A}$ is compatible with localisation on $\operatorname{Spec}(B)$ implies that the quasi-coherent $\mathcal{O}_{\operatorname{Spec}(B)}$-modules $\widetilde{\Omega^1_{B/A}}$ glue together in a natural way. Hence we obtain a quasi-coherent $\mathcal{O}_X$-module that we denote $\Omega^1_{X/Y}$. It comes with an $\mathcal{O}_Y$-derivation $d\colon \mathcal{O}_X \to \Omega^1_{X/Y}$, which is the universal $\mathcal{O}_Y$-derivation on $\mathcal{O}_X$.

7.1.2 Proposition. *Let k be a field, X a k-scheme and P in $X(k)$. Then $P^*\Omega^1_{X/k}$ is canonically isomorphic to m_P/m_P^2, where m_P is the maximal ideal in $\mathcal{O}_{X,m_P}$.*

Proof. We can suppose that X is affine, say $\operatorname{Spec}(A)$; then P corresponds to a maximal ideal m of A such that $A/m = k$. The exact sequence $0 \to m \to A \to k$ is canonically split since A is a k-algebra. Hence we have $A = m \oplus k$, where the projection of A to m sends f to $f - f(P)$. One verifies immediately that $D\colon A \to m/m^2$, $f \mapsto [f - f(P)]$, is a k-derivation. This gives us an A-linear map $\alpha\colon \Omega^1_{A/k} \to m/m^2$. Since A acts on m/m^2 via k, we get a k-linear map $\overline{\alpha}\colon k \otimes_A \Omega^1_{A/k} \to m/m^2$. On the other hand, consider the composition $m \to A \to \Omega^1_{A/k} \to k \otimes_A \Omega^1_{A/k}$. Since it lands in a k-vector space, it factors through a k-linear map $\beta\colon m/m^2 \to k \otimes_A \Omega^1_{A/k}$. One verifies that $\overline{\alpha}$ and β are inverses. □

7.1.3 Proposition. *Let k be a field and X a k-scheme which is locally of finite type. Let x be closed in X and let d be the dimension of X at x. Then X is smooth at x if and only if $\Omega^1_{X,x}$ is a free $\mathcal{O}_{X,x}$-module of rank d.*

Proof. We may suppose that $X = \mathrm{Spec}(A)$, with $A = k[x_1, \dots, x_n]/(f_1, \dots, f_r)$, and that k is algebrically closed. It follows from Example 6.2.3 that $\Omega^1_{A/k}$ has the presentation:

$$A^r \to A^n \to \Omega^1_{A/k} \to 0,$$

where the map from A^r to A^n is given by the matrix $(\partial f_j/\partial x_i)$, and where the ith element e_i of the standard basis of A^n is mapped to dx_i. We know that the rank of the matrix $(\partial f_j/\partial x_i)(x)$ is at most $n - d$, with equality if and only if X is smooth at x (Thm. 3.4.3). It follows that X is smooth at x iff $\dim_k(x^*\Omega^1_{X/k}) = d$ iff $(\Omega^1_{X/k})_x$ is free of rank d as $\mathcal{O}_{X,x}$-module. Here we have used the following lemma. □

7.1.4 Lemma. *Let X be a locally noetherian scheme and $\mathcal{M}$ a coherent $\mathcal{O}_X$-module. Then the function $r\colon X \to \mathbb{Z}$, $x \mapsto \dim_{k(x)} x^*\mathcal{M}$ is upper semicontinuous, i.e., for any n in $\mathbb{Z}$, the set $\{x \in X \mid r(x) \geq n\}$ is closed. Moreover, if X is reduced and r is constant, then $\mathcal{M}$ is locally free or rank r.*

Proof. Do exercise 5.8 of [Har, II]. □

7.1.5 Corollary. *Let C be a curve over a field k. Then C is smooth if and only if $\Omega^1_{C/k}$ is locally free of rank one as $\mathcal{O}_C$-module.*

Let C be a projective smooth geometrically irreducible curve over a field k. Then $\Omega^1_{C/k}$ is an invertible $\mathcal{O}_C$-module. Any divisor D such that $\mathcal{L}(D)$ is isomorphic to $\Omega^1_{C/k}$ is called a canonical divisor on C. Of course, such D are unique up to linear equivalence. Let us look at some examples.

7.1.6 Example. Consider $C := \mathbb{P}^1_k$. Then $C = U_0 \cup U_1$ with $U_0 = \mathrm{Spec}(k[x])$, $U_1 = \mathrm{Spec}(k[y])$ and $xy = 1$. Let ω be a global section of $\Omega^1_{C/k}$. The restriction of ω to U_0 is of the form $(\sum_{i=0}^n a_i x^i)dx$. On $U_1 \cap U_0$, in terms of y, this is equal to $-(\sum_{i=0}^n a_i y^{-i})y^{-2}dy$. One sees that this has a pole at ∞ as soon as $\omega \neq 0$. Hence: $\Gamma(\mathbb{P}^1_k, \Omega^1_{\mathbb{P}^1_k/k}) = 0$.

7.1.7 Example. Let C be the smooth projective hyperelliptic curve over a field k of characteristic $\neq 2$ given by the affine equation $u^2 = f$, with f in $k[x]$ separable and of degree > 0. Suppose that the degree d of f is odd. Then one can show that the elements ω_i, $0 \leq i \leq (d-3)/2$, given by $\omega_i = x^i u^{-1} dx$ form a basis of the k-vector space $\Gamma(C, \Omega^1_{C/k})$. Hence $\dim_k(\Gamma(C, \Omega^1_{C/k})) =$

$(d-1)/2$. We have seen in §5.2 that for $k = \mathbb{C}$, $C(\mathbb{C})$ has genus $(d-1)/2$. This is not a coincidence: for C over $\mathbb{C}$ one has $g(C(\mathbb{C})) = \dim_{\mathbb{C}}(\Gamma(C, \Omega^1_{C/\mathbb{C}}))$. This allows us to define the genus of C to be $\dim_k(\Gamma(C, \Omega^1_{C/k}))$ in general. But, of course, we will have to show that these dimensions are finite.

7.1.8 Definition. *Let C be a smooth projective geometrically irreducible curve over a field k. Let $\mathcal{L}$ be a line bundle on C. Let D be in $\mathrm{Div}(C)$ such that $\mathcal{L}(D)$ is isomorphic to $\mathcal{L}$. We define the degree of $\mathcal{L}$ to be the degree of D. This is independent of the choice of D because the difference with another choice is a principal divisor, and hence of degree zero. It is immediate that two line bundles that are isomorphic have the same degree. It follows that we have a morphism $\deg\colon \mathrm{Pic}(C) \to \mathbb{Z}$ that sends $[\mathcal{L}]$ to $\deg(\mathcal{L})$.*

This gives us a second numerical invariant of C: the degree of $\Omega^1_{C/k}$. It is not hard to compute that for $\mathbb{P}^1_k$ this degree is -2, and that for a hyperelliptic curve $y^2 = f$ with f of odd degree d it is $d-3$. In general it is $2g(C) - 2$.

8 March 8, 1996

8.1 The theorem of Riemann–Roch

Let C be a smooth projective geometrically irreducible curve over a field k. We have seen that $\Omega^1_{C/k}$ is an invertible $\mathcal{O}_C$-module. We define the genus $g(C)$ of C to be the dimension of the k-vector space $\Gamma(C, \Omega^1_{C/k})$. Let us admit for the moment that for $\mathcal{L}$ an invertible $\mathcal{O}_C$-module the k-vector space $\Gamma(C, \mathcal{L})$ is of finite dimension. We will prove a bit further that in fact $\dim_k(\Gamma(C, \mathcal{L}))$ is at most $\max(0, \deg(\mathcal{L}) + 1)$; in particular, it is zero if $\deg(\mathcal{L}) < 0$. Let K be any divisor on C such that $\mathcal{L}(K)$ is isomorphic to $\Omega^1_{C/k}$ (i.e., K is the divisor of some non-zero element of $\Omega^1_{C/k,\eta}$, where η is the generic point of C; such divisors are called canonical divisors). Recall that for any divisor D on C we have defined an invertible $\mathcal{O}_C$-module $\mathcal{L}(D)$ and that $l(D)$ is the dimension of the space of global sections $L(D)$ of $\mathcal{L}(D)$. The following theorem, called the theorem of Riemann–Roch, gives a relation between $l(D)$ and $l(K - D)$.

8.1.1 Theorem. *For any divisor D on C we have*

$$l(D) - l(K - D) = \deg(D) + 1 - g(C)$$

We do not have time to give a proof of this theorem. Proofs can be found in [Har] and in [Serre, Groupes algébriques et corps de classes, II]. These proofs use cohomology of sheaves; the second proof less than the first. I hope to say a few things about the proof at the end of today's lecture. A very useful consequence of Thm. 8.1.1 is that for D of degree greater than the degree of K one has $l(K - D) = 0$, hence $l(D) = \deg(D) + 1 - g(C)$. Putting $D := 0$ in Thm. 8.1.1 and using that $\Gamma(C, \mathcal{O}_C) = k$ gives $l(K) = g(C)$, which is in fact the definition of $g(C)$. Putting $D := K$ in Thm. 8.1.1 gives $\deg(K) = 2g(C) - 2$, a result that we already verified by hand for plane curves and hyperelliptic curves. Of course, Thm. 8.1.1 has a version in terms of invertible $\mathcal{O}_C$-modules instead of divisors: it says that for any invertible $\mathcal{O}_C$-module $\mathcal{L}$ one has:

$$\dim_k(\Gamma(C, \mathcal{L})) - \dim_k(\Gamma(C, \Omega^1_{C/k} \otimes \mathcal{L}^{-1})) = \deg(\mathcal{L}) + 1 - g(C) \tag{8.1.2}$$

The following consequence of Thm. 8.1.1 will be most important for us in the construction of the jacobian of C.

8.1.3 Corollary. *Let $\mathcal{L}$ be an invertible $\mathcal{O}_C$-module of degree at least $g(C)$ on C. Then there is an effective divisor D such that $\mathcal{L} \cong \mathcal{L}(D)$.*

Proof. Let $\mathcal{L}$ be as in the statement. Then the right hand side of (8.1.2) is > 0, hence, since dimensions are ≥ 0, we have $\dim_k(\Gamma(C, \mathcal{L})) > 0$. Let s be a non-zero element of $\Gamma(C, \mathcal{L})$. Then the divisor $\mathrm{div}(s)$ of s is effective and $\mathcal{L}$ is isomorphic to $\mathcal{L}(\mathrm{div}(s))$. $\square$

Theorem 8.1.1 has many applications; see [Har, IV]. For example, one can show that a curve C of genus zero with $C(k) \neq \emptyset$ is isomorphic to $\mathbb{P}^1_k$. One can show that a curve C of genus one with a rational point P can be embedded in $\mathbb{P}^2_k$ such that it is given by an equation of the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, and that $C(k)$ has a natural group structure. One can show that the complement of a closed point P on C is affine. One can show that C can be embedded in $\mathbb{P}^3$ (for this one doesn't need Riemann–Roch). One can show that there exists a dominant morphism of C to $\mathbb{P}^1_k$ of degree at most $g(C) + 1$. Again, we have no time to look at this. Let us also note that there are applications to the theory of error correcting codes (take k a finite field).

8.2 Hurwitz's formula

Let $\pi\colon C \to C'$ be a dominant morphism between smooth projective geometrically irreducible curves. We know that π is a finite morphism, and that for $\mathrm{Spec}(B)$ an open affine of C', $\pi^{-1}\mathrm{Spec}(B)$ is of the form $\mathrm{Spec}(C)$ with C a B-algebra which is locally free of rank $\deg(\pi)$ as B-module. The exact sequences of Proposition 7.1.1(4), with A replaced by k, glue to an exact sequence of sheaves on C:

$$\pi^*\Omega^1_{C'/k} \to \Omega^1_{C/k} \to \Omega^1_{C/C'} \to 0 \tag{8.2.1}$$

The two sheaves on the left in this exact sequence are both invertible $\mathcal{O}_C$-modules. It follows that $\pi^*\Omega^1_{C'/k} \to \Omega^1_{C/k}$ is either injective or zero. By looking at $\Omega^1_{C/C',\eta}$ one sees that $\pi^*\Omega^1_{C'/k} \to \Omega^1_{C/k}$ is zero if and only if the field extension $k(C') \to k(C)$ is inseparable. Let us suppose that this field extension is separable (in which case we say that π is separable). Then we have an exact sequence:

$$0 \to \pi^*\Omega^1_{C'/k} \to \Omega^1_{C/k} \to \Omega^1_{C/C'} \to 0 \tag{8.2.2}$$

and $\Omega^1_{C/C',\eta} = 0$. Since $\Omega^1_{C/C'}$ is a coherent $\mathcal{O}_C$-module, it has support in a finite number of closed points of C. These points are exactly those at which the geometric fibre of π is not reduced, and are called the ramification points. Let x be a point such that $\Omega^1_{C/C',x} \neq 0$. Since $\Omega^1_{C/k,x}$ is a free $\mathcal{O}_{X,x}$-module of rank one, $\Omega^1_{C/C',x}$ is isomorphic to $\mathcal{O}_{X,x}/m_x^{r_x}$ for a unique $r_x > 0$. The divisor $R := \sum_x r_x x$ is called the ramification divisor. One verifies easily that the injection $\pi^*\Omega^1_{C'/k} \to \Omega^1_{C/k}$ identifies $\pi^*\Omega^1_{C'/k}$ with the subsheaf $\Omega^1_{C/k} \otimes \mathcal{L}(-R)$ of $\Omega^1_{C/k}$. It follows that we have the following formula, relating the degrees of $\Omega^1_{C'/k}$, $\Omega^1_{C/k}$ and R:

$$\deg(\Omega^1_{C/k}) = \deg(\pi^*\Omega^1_{C'/k}) + \deg(R) = \deg(\pi)\deg(\Omega^1_{C'/k}) + \deg(R) \tag{8.2.3}$$

Of course, this formula expresses the genus of C in terms of the genus of C' and the degree of R. It generalises the results that we obtained by hand, for plane curves and hyperelliptic curves over $\mathbb{C}$ (if we admit that the topological genus, i.e., the genus of $C(\mathbb{C})$, equals $g(C)$). In certain cases there is a simple formula for the r_x. Suppose that k is algebraically closed and let x in C be a ramification point of π. Let e_x be the multiplicity of x in the divisor π^*y, where $y = \pi(x)$. Then we claim that $r_x \geq e_x - 1$, with equality if and only if e_x is invertible in k. The proof is as follows. Let t_x and t_y be uniformizers at x and y, respectively. Then $\pi^\#(t_y) = t_x^{e_x}u$, with u in $\mathcal{O}_{C,x}^*$. Note that dt_y is a $\mathcal{O}_{C',y}$-basis of $\Omega^1_{C'/k,y}$, and that dt_x is a $\mathcal{O}_{C,x}$-basis of $\Omega^1_{C/k,x}$. We have:

$$\pi^*(dt_y) = d(\pi^\# t_y) = d(t_x^{e_x}u) = t_x^{e_x-1}(e_x u + t_x u')dt_x, \tag{8.2.4}$$

where $u' = du/dt_x$. This shows clearly what we claimed. For example, if k is algebraically closed of characteristic zero one has $R = \sum_x (e_x - 1)x$, where the sum ranges over all closed x in C.

8.3 On the proof of the Riemann-Roch theorem

Let as usual C be a smooth projective geometrically irreducible curve of over a field k. We suppose that k is algebraically closed. One basic tool to prove properties of the $l(D)$ is the following.

8.3.1 Proposition. *Let D be a divisor on C and P a closed point on C. Then we have an exact sequence of sheaves on C:*

$$0 \to \mathcal{L}(D) \to \mathcal{L}(D+P) \to P_*k \to 0,$$

where the map $\mathcal{L}(D) \to \mathcal{L}(D+P)$ is the inclusion, and where $P\colon \mathrm{Spec}(k) \to C$ is the element of $C(k)$ corresponding to P.

Proof. Let us first define a morphism $\mathcal{L}(D+P) \to P_*k$. Let t be a uniformizer at P and let n be the multiplicity of P in $D+P$. Then t^{-n} is a $\mathcal{O}_{C,P}$-basis of $\mathcal{L}(D+P)_P$. Let U be an open neighborhood of P and f in $\mathcal{L}(D+P)(U)$. Then we send f to $(t^n f)(P)$ (note that $t^n f$ is regular at P). The exactness of the sequence follows directly from the definitions. $\square$

Since taking global sections is left exact, Prop. 8.3.1 gives exact sequences:

$$0 \to L(D) \to L(D+P) \to k \tag{8.3.2}$$

8.3.3 Proposition. *For all divisors D one has $l(D) \leq \deg(D) + 1$.*

Proof. We know that this is true if $\deg(D) \leq 0$, and that for D of degree zero $l(D) = 1$ iff D is principal. So the proof is by induction on $\deg(D)$; (8.3.2) gives the induction step. $\square$

Let us now discuss a very little bit the proof of the Riemann–Roch theorem. By the definition of $g(C)$, it is true for $D = 0$. The proof is by induction on $\sum_x |n_x|$, if $D = \sum_x n_x x$. For D a divisor on C and P a closed point one constructs an exact sequence of k-vector spaces:

$$0 \to L(D) \to L(D+P) \to k \to L(K-D)^\vee \to L(K-(D+P))^\vee \to 0 \tag{8.3.4}$$

where, for V a k-vector space, $V^\vee$ denotes its dual. It is clear that this provides the induction step. The exact sequences (8.3.4) are constructed as long exact cohomology sequences

(8.3.5)

$$0 \to \mathrm{H}^0(C, \mathcal{L}(D)) \to \mathrm{H}^0(C, \mathcal{L}(D+P)) \to \mathrm{H}^0(C, P_*k) \to \mathrm{H}^1(C, \mathcal{L}(D)) \to \mathrm{H}^1(C, \mathcal{L}(D+P)) \to 0$$

coming from the exact sequence of sheaves of Prop. 8.3.1. Serre's duality theorem gives isomorphisms

$$\mathrm{H}^1(C, \mathcal{L}) \to \mathrm{H}^0(C, \Omega^1_{C/k} \otimes \mathcal{L}^{-1})^\vee \tag{8.3.6}$$

Probably more about cohomology later.

8.4 Effective divisors of degree $g(C)$

Let again C be a smooth projective geometrically irreducible curve over an algebraically closed field k. Let g be the genus of C. We have seen that every invertible $\mathcal{O}_C$-module is isomorphic to some $\mathcal{L}(D)$, with D an effective divisor of degree g. In other words, the map

$$C(k)^g \to \mathrm{Pic}^g(C), \qquad (P_1, \ldots, P_g) \mapsto \mathcal{L}(P_1 + \cdots + P_g) \tag{8.4.1}$$

is surjective. The aim of this section is to show that there exist $(P_1, \ldots, P_g)$ in $C(k)^g$ such that the fibre of (8.4.1) over the image of $(P_1, \ldots, P_g)$ consists exactly of the permutations of $(P_1, \ldots, P_g)$. We will deduce later that this is then true for all $(P_1, \ldots, P_g)$ in a non-empty open subset of $C(k)^g$.

Let us first study the problem of determining in some way the effective divisors D' that are linearly equivalent to a given divisor D, i.e., such that $D' - D$ is a principal divisor. Now $D' - D$ is a principal divisor if and only if there exists f in $k(C)^*$ such that $\mathrm{div}(f) = D - D'$. Such an f is in fact a section of $\mathcal{L}(D)$, whose divisor (not as a rational function but as a section of $\mathcal{L}(D)$) equals D'. The converse holds too: let f be a non-zero section of $\mathcal{L}(D)$ and let D' be the divisor of f as a section of $\mathcal{L}(D)$; then $D - D'$ is the principal divisor $\mathrm{div}(f)$. Hence we have established a bijection:

$$\mathbb{P}(\Gamma(C, \mathcal{L}(D))) \to \{\text{effective divisors } D' \text{ with } D' \equiv D\} \tag{8.4.2}$$

where for V a k-vector space $\mathbb{P}(V) := (V - \{0\})/k^*$, and where $\equiv$ denotes linear equivalence. This reduces our problem to showing that there is a non-empty subset U in $C(k)^g$ such that for all $(P_1, \ldots, P_g)$ in U we have $l(D) = 1$, or, equivalently, $l(K - D) = 0$.

8.4.3 Lemma. *Let D be a divisor on C. For all closed points P in C for which there exists an s in $L(D)$ which does not vanish at P (as a section of $\mathcal{L}$) one has $l(D - P) = l(D) - 1$. In particular, if $l(D) \neq 0$ then for all but finitely many points P one has $l(D - P) = l(D) - 1$.*

Let us now construct $(P_1, \ldots, P_g)$ as desired. If $g = 0$ there is nothing to prove, so suppose that $g > 0$. Lemma 8.4.3 says that for all but finitely many P_1 we have $l(K - P_1) = g - 1$. Take such a P_1. Repeated application of Lemma 8.4.3 gives $P_2, \ldots, P_g$.

9 March 15, 1996

9.1 Quotients by actions of finite groups: construction

This topic is almost completely absent in [Har]. Good references are [Serre, Groupes algébriques et corps de classes, III, §12] and [Mumford, Abelian varieties, II, §7 and III, §12]. Let G be a finite group, acting on a ring A. Let $A^G := \{a \in A \mid \forall g \in G : g(a) = a\}$ be the subring of G-invariants of A. Let $X := \operatorname{Spec}(A)$ and $Y := \operatorname{Spec}(A^G)$. Then G acts from the right on X and the morphism $\pi \colon X \to Y$ is invariant under G in the following sense: $\pi \circ r(g) = \pi$ for all g in G, where $r(g)$ is the automorphism of X induced by g. From the construction of π and the anti-equivalence between rings and affine schemes it is clear that $\pi \colon X \to Y$ is the quotient for the action of G in the category of affine schemes: every G-invariant morphism $f \colon X \to Z$ with Z affine factors uniquely through π. The following proposition says that the situation is in fact much better: π is the quotient in the category of locally ringed spaces. To make sense of this, we have to define the notion of quotient of a locally ringed space X by an action, say from the right, of a finite group G. So let $Y := X/G$ as sets, and let $\pi \colon X \to Y$ be the quotient map. We give Y the induced topology: $U \subset Y$ is open if and only if $\pi^{-1}U$ is open in X. For $U \subset Y$ open G acts on the ring $\mathcal{O}_X(\pi^{-1}U)$ since $\pi^{-1}U$ is G-stable; we define $\mathcal{O}_Y(U) := \mathcal{O}_X(\pi^{-1}U)^G$. Then π is the quotient for the G-action in the category of ringed spaces. We leave it as an exercise for the reader to verify that $(Y, \mathcal{O}_Y)$ is actually a locally ringed space and that for $f \colon X \to Z$ a G-invariant morphism of locally ringed spaces the morphism from $Y \to Z$ given by the universal property is actually a morphism of locally ringed spaces. Here are some hints. Let y be in Y, and x in X with $\pi x = y$. For $U \subset Y$ open and containing y we have $\mathcal{O}_X(\pi^{-1}U) \to k(x)$, with $k(x)$ the residue field at x. For f in $\mathcal{O}_Y(U)$ with $f(x) \neq 0$ in $k(x)$, f is invertible on the open G-invariant subset $D(f)$ of $\pi^{-1}U$.

9.1.1 Proposition. *Let $X = \operatorname{Spec}(A)$ be an affine scheme with an action by a finite group G. Then the morphism $\pi \colon X \to Y := \operatorname{Spec}(A^G)$ is a quotient in the category of locally ringed spaces.*

Proof. Let us first note that every a in A is a root of the polynomial $\prod_{\sigma \in G}(X - \sigma(a))$ which is monic and has coefficients in $B := A^G$. So π is integral and hence closed. We want to show that π is set-theoretically the quotient map. The fibres of π are G-stable since π is G-invariant, so it remains to show that each fibre of π consists of exactly one G-orbit. Before we do that, let us show that for b in B we have $B_b = (A_b)^G$, in the sense that the natural morphism $B_b \to (A_b)^G$ is an isomorphism. Localization is exact, hence the injection $B \to A$ induces an injection $B_b \to A_b$, which in fact factors through $(A_b)^G$. Let a/b^n be in $(A_b)^G$. There exists

$m \geq 0$ such that for all σ in G we have $b^m(\sigma(a) - a) = 0$. It follows that $a/b^n = ab^m/b^{n+m}$ is in B_b. Let now y be in Y, and let X_y be the set-theoretical fibre of π over y. Because π is closed and dominant, π is surjective. Hence X_y consists of at least one G-orbit. Suppose that X_y consists of more than one G-orbit. Let x_1G and x_2G be two distinct orbits in X_y. The fact that $B_b = (A_b)^G$ for all b in B implies that $B_y = (A \otimes_B B_y)^G$. It follows that $A \otimes_B k(y)$ is integral over $k(y)$, hence that every prime ideal of $A \otimes_B k(y)$ is maximal. This implies that every point in X_y is a maximal ideal of $A \otimes_B B_y$. The Chinese Remainder Theorem says that the morphism $A \otimes_B B_y \to \prod_{x \in x_1 \cdot G} k(x) \times \prod_{x \in x_2 \cdot G} k(x)$ is surjective. Let f be in $A \otimes_B B_y$ having image 1 in the $k(x)$ with $x \in x_1 \cdot G$ and 0 in the $k(x)$ with $x \in x_2 \cdot G$. Then $\prod_\sigma \sigma(f)$ has the same property and is G-invariant hence in B_y which is impossible. Hence X_y consists of exactly one G-orbit, and we have proved that, set-theoretically, π is the quotient map. Since π is closed, Y has the quotient topology.

It remains to show that the morphism of sheaves $\mathcal{O}_Y \to (\pi_* \mathcal{O}_X)^G$ on Y is an isomorphism. Since both are sheaves, it suffices to verify that on all $D(b)$ with b in B they have the same sections. But that we have already done, since it amounts to $B_b = (A_b)^G$. $\square$

9.1.2 Corollary. *Let X be a scheme with an action by a finite group G. Suppose that every G-orbit in X is contained in an affine open subset of X. Then the quotient X/G in the category of locally ringed spaces is actually a scheme.*

Proof. Let us first prove that for every x in X there exists a G-stable affine open subset U of X containing xG. In the case where X is separated over an affine scheme, finite intersections of affine opens are affine, hence if U is an affine open containing xG, then $\cap_\sigma U\sigma$ is a G-stable open affine containing xG. In general one reduces to this case. Let $U_0 = \mathrm{Spec}(A)$ be an affine open in X containing xG. Let $U_1 := \cap_\sigma U_0\sigma$: this is a G-stable open subset of X, not necessarily affine. Let $I \subset A$ be an ideal such that $U_0 - U_1 = V(I)$, and let $p_1, \ldots, p_n$ be the prime ideals in A corresponding to the elements of xG. A standard argument shows that there exists an element a in A such that a is in I, but not in the union of the p_i. Then $U_2 := D(a) \subset U_1$ is an affine open subset containing xG. Since U_0 is separated, $U_3 := \cap_\sigma U_2\sigma$ has all the desired properties.

Let $\pi \colon X \to Y := X/G$ be the quotient in the category of locally ringed spaces. Let y be in Y. Let $U = \mathrm{Spec}(A)$ be a G-stable affine open subset in X containing $\pi^{-1}y$. Then πU is an open subset of Y, and Prop. 9.1.1 implies that $\pi U = \mathrm{Spec}(A^G)$. Hence Y is a scheme. $\square$

9.1.3 Remark. If X is quasi-projective over a scheme S and G acts by automorphisms of X as an S-scheme, then every orbit of G is contained in an affine open subset of X.

9.1.4 Example. Let $X := \mathrm{Spec}(L)$ with L a field. Let G be a finite subgroup of the automorphism group of L. Let $K := L^G$. Then $\pi \colon X \to Y := \mathrm{Spec}(K)$ is the quotient by G. One knows in this case that $K \to L$ is a separable Galois extension of degree $|G|$, with Galois group G. Note that the geometric fibre of π, i.e., $\mathrm{Spec}(L \otimes_K \overline{K}) \to \mathrm{Spec}(\overline{K})$, is the disjoint union of copies of $\mathrm{Spec}(\overline{K})$, indexed by G, and that G acts freely and transitively on the set $X(\overline{K})$. So despite of the fact that X consist of just one point, the G-action on it is free in a certain sense.

9.1.5 Example. Let $X := \mathbb{A}^2_k = \mathrm{Spec}(k[x,y])$ with k of characteristic different from 2. Let σ be the k-automorphism of X given by $\sigma^\# \colon x \mapsto -x$, $y \mapsto -y$. Then $k[x,y]^G$ has a k-basis consisting of the monomials $x^a y^b$ with $a+b$ even. We want to describe $k[x,y]^G$ by generators and relations. Clearly x^2, xy and y^2 generate $k[x,y]^G$. Let $\phi \colon k[u,v,w] \to k[x,y]^G$ be the morphism of k-algebras sending u to x^2, v to xy and w to y^2. Obviously, $uw - v^2$ is in the kernel of ϕ. We claim that $\ker(\phi) = (uw - v^2)$. So let f be in $\ker(\phi)$. We want to show that the image $\bar{f}$ of f in $k[u,v,w]/(uw-v^2)$ is zero. Replacing v^2 by uw in f as many times as possible, we see that $\bar{f}$ can be written as $g + hv$, with g and h in $k[u,w]$. Since $\phi(f) = 0$ we have $0 = g(x^2,y^2) + xyh(x^2,y^2)$ in $k[x,y]$. This clearly implies that g and h are zero, hence $\bar{f}$ too. It follows that the quotient $Y := \mathrm{Spec}(k[x,y]^G)$ is isomorphic to $V(uw - v^2)$ in $\mathbb{A}^3_k$. Note that Y is singular at the origin. So apparently it can happen that a quotient of a smooth k-scheme is not smooth. We will see in the next section that this cannot happen if G acts freely.

9.1.6 Example. Let X be an integral scheme which is normal, with an action by a finite group G satisfying the conditions of Cor. 9.1.2. Then one easily shows that the quotient Y is integral and normal too. It follows that for X a smooth projective irreducible curve over an algebraically closed field Y is the smooth projective irreducible curve corresponding to $k(X)^G$. It also follows that for $X = \mathrm{Spec}(O_L)$ with L a number field, i.e., a finite extension of $\mathbb{Q}$, $Y = \mathrm{Spec}(O_K)$ where $K = L^G$.

9.1.7 Example. Let R be a ring, $n \geq 0$ and $A := R[x_1, \ldots, x_n]$. Let $G := \mathrm{S}_n$ be the group of permutations of $\{1, 2, \ldots, n\}$. We let G act on A by R-algebra automorphisms permuting the x_i: $\sigma \colon x_i \mapsto x_{\sigma(i)}$. Then $B := A^G$ is the sub-A-algebra generated by the elementary symmetric polynomials $p_1, \ldots, p_n$. Since the p_i are algebraically independent, it follows that $\mathrm{Spec}(B)$, which is $\mathbb{A}^n_R/G$ is isomorphic to $\mathbb{A}^n_R$, with the quotient map given by the p_i.

9.2 Quotients by actions of finite groups: properties

9.2.1 Proposition. *Let R be a noetherian ring, X an R-scheme of finite type, G a finite group acting on X as R-scheme such that the action satisfies the hypothesis of Cor. 9.1.2. Then the* *quotient $Y := X/G$ is of finite type over R and $\pi\colon X \to Y$ is finite.*

Proof. It suffices to prove this for X affine, say $X = \mathrm{Spec}(A)$. Let $x_1, \ldots, x_n$ be R-generators of A. Let C be the sub-R-algebra of $B := A^G$ that is generated by the (finitely many) coefficients of the polynomials $\prod_\sigma (X - \sigma(x_i))$. Then C is of finite type over R, hence noetherian. By construction, A is finite over C, hence B too. It follows that A is finite over B and that B is of finite type over R. $\square$

9.2.2 Proposition. *Let R be a ring and X an R-scheme with an action by a finite group G satisfying the hypothesis of Cor. 9.1.2. Let $\pi\colon X \to Y := X/G$ be the quotient. Let R' be an R-algebra, let $X' := X \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R')$ etc. Then we have a natural morphism $X'/G \to (X/G)'$. If R' is flat over R this morphism is an isomorphism.*

Proof. Reduce to $X = \mathrm{Spec}(A)$ affine. Then the question is whether $A^G \otimes_R R' \to (A \otimes_R R')^G$ is an isomorphism or not. We have an exact sequence of R-modules:

$$0 \to A^G \to A \to \prod_\sigma A, \tag{9.2.3}$$

where the map $A \to \prod_\sigma A$ sends a to $\sigma \mapsto \sigma(a) - a$. Since $R \to R'$ is flat, this sequence remains exact after tensoring with R', proving what we need. $\square$

9.2.4 Theorem. *Let R be a noetherian ring, X an R-scheme of finite type with an action by a finite group G, satisfying the hypothesis of Cor. 9.1.2. Let $\pi\colon X \to Y$ be the quotient. Let y be in Y. Then the diagram*

$$\begin{array}{ccc} X & \longleftarrow & \coprod_{x \mapsto y} \mathrm{Spec}(\widehat{\mathcal{O}_{X,x}}) \\ \downarrow & & \downarrow \\ Y & \longleftarrow & \mathrm{Spec}(\widehat{\mathcal{O}_{Y,y}}) \end{array} \tag{9.2.5}$$

is Cartesian, and the second vertical arrow is also a quotient for the action by G. Let x be in $\pi^{-1}y$ and let G_x be the stabilizer in G of x. Then $\widehat{\mathcal{O}_{Y,y}} = \widehat{\mathcal{O}_{X,x}}^{G_x}$. If G acts freely on X in the sense that it acts freely on the sets $X(S)$ for all R-schemes S, then π is finite étale (see Remark 9.2.7): for every x in X the complete local ring $\widehat{\mathcal{O}_{X,x}}$ is an $\widehat{\mathcal{O}_{Y,\pi(x)}}$-algebra of the form $\widehat{\mathcal{O}_{Y,\pi(x)}}[t]/(f)$, with f monic and $(f, f') = \widehat{\mathcal{O}_{Y,\pi(x)}}[t]$.

Proof. We replace Y by $\mathrm{Spec}(\mathcal{O}_{Y,y})$ and X by $X \times_Y \mathrm{Spec}(\mathcal{O}_{Y,y})$. Then $Y = \mathrm{Spec}(B)$ with B local, and $X = \mathrm{Spec}(A)$ for some A. We apply Prop. 9.2.2 with $R := B$ and $R' := \widehat{B}$. It follows that $(A \otimes_B \widehat{B})^G = \widehat{B}$. Let m_B be the maximal ideal of B. Since A is a finitely generated

B-module, we have $A \otimes_B \widehat{B} = \varprojlim A \otimes_B B/m_B^n$. The prime ideals of $A \otimes_B B/m_B^n$ are precisely the x in $\pi^{-1}y$ (for $n \geq 1$), and they are maximal ideals. It follows that $A \otimes_B B/m_B^n$ is the product of its localizations at these x. Hence $A \otimes_B \widehat{B} = \prod_{x \mapsto y} \widehat{\mathcal{O}_{X,x}}$. Since we won't use the fact that π is finite etale if G acts freely, we won't prove it either. $\square$

9.2.6 Remark. Let X be a scheme with an action by a finite group such that every orbit is contained in an open affine subset of X. One would like to understand the functor that X/G represents, i.e., the sets $(X/G)(S)$ with S any scheme. Of course, the map $X(S) \to (X/G)(S)$ factors through $X(S)/G$, but the maps $X(S)/G \to (X/G)(S)$ need not be injective nor surjective. For example, let $G := \mathbb{Z}/2\mathbb{Z}$, $X := \mathrm{Spec}(\mathbb{Q}(i))$ with the action of G given by $\sigma\colon i \mapsto -i$; then $X/G = \mathrm{Spec}(\mathbb{Q})$ and $X(\mathbb{Q})/G \to (X/G)(\mathbb{Q})$ is not surjective. To show that it need not be injective, take $X := \mathrm{Spec}(\mathbb{Q}[\varepsilon])$ with $\varepsilon^2 = 0$, take $G := \mathbb{Z}/2\mathbb{Z}$ that acts via $\sigma\colon \varepsilon \mapsto -\varepsilon$; then $X/G = \mathrm{Spec}(\mathbb{Q})$; take $S := X$. There is a positive statement, however: for k an algebraically closed field the map $X(k)/G \to (X/G)(k)$ is bijective (left as an exercise to the reader; note that if X is a k-scheme of finite type it follows from the facts that X/G is topologically the quotient and that $X(k)$ is the same as the set of closed points).

9.2.7 Remark. Let S be a scheme and X an S-scheme. Then X is finite etale over S if it is finite locally free and has geometrically reduced fibers. For example, if $S = \mathrm{Spec}(k)$ with k a field, then the finite etale S-schemes are the spectra of finite products of finite separable extensions of k. For $S = \mathrm{Spec}(A)$ affine the finite etale S-schemes are the $\mathrm{Spec}(B)$ with B an A-algebra which is locally free of finite rank as an A-module and has the property that for every morphism $A \to k$ with k a field, $B \otimes_A k$ is reduced. For locally noetherian S, $f\colon X \to S$ is finite etale if and only if f is finite and for every closed x in X the complete local ring $\widehat{\mathcal{O}_{X,x}}$ is an $\widehat{\mathcal{O}_{Y,f(x)}}$-algebra of the form $\widehat{\mathcal{O}_{Y,f(x)}}[t]/(g)$ with g monic and $(g, g') = \widehat{\mathcal{O}_{Y,f(x)}}[t]$. If S is locally of finite type over an algebraically closed field k, then $f\colon X \to S$ is finite etale if and only if f is finite and for all x in $X(k)$ the induced morphism of complete local rings $\widehat{\mathcal{O}_{Y,f(x)}} \to \widehat{\mathcal{O}_{X,x}}$ is an isomorphism. A good reference for etale and finite etale morphisms is [SGA 1] (Springer Lecture Notes in Mathematics 224). See also Lemmas 10.1.2 and 10.1.3.

9.3 Symmetric products of curves

Let k be a field and C a smooth projective geometrically irreducible curve over k. Let $n \geq 1$ and let C^n denote the n-fold fibered product of C over k. The group S_n acts on C^n and since C^n is projective, every orbit is contained in an affine open subset of C^n. The quotient $C^{(n)} := C^n/\mathrm{S}_n$ is called the nth symmetric product of C.

9.3.1 Proposition. *The k-scheme $C^{(n)}$ is smooth projective and of dimension n.*

Proof. Let us first show that $C^{(n)}$ is of finite type and smooth of dimension n. It is of finite type because of Prop. 9.2.1. To say that it is smooth is to say that $C^{(n)}_{\overline{k}}$ is regular. By Prop. 9.2.2 we have $C^{(n)}_{\overline{k}} = (C_{\overline{k}})^{(n)}$. Hence we may assume that k is algebraically closed and we have to show that $C^{(n)}$ is regular at all closed points. Let us look a bit closer at $C^{(n)}(k)$. According to Rem. 9.2.6, $C^{(n)}(k) = C(k)^n/\mathrm{S}_n$, i.e., it is the set of unordered $n$tuples of elements of $C(k)$. Equivalently, $C^{(n)}(k)$ is the set of effective divisors of degree n on C. Let $y = m_1P_1 + \cdots + m_rP_r$ be in $C^{(n)}(k)$, with the P_i distinct and the $m_i \geq 1$. Its local ring is regular if and only if its completion is, and we can compute this completion using Thm. 9.2.4. For each i, let t_i be a uniformizer at P_i; then $\widehat{\mathcal{O}_{X,P_i}} = k[[t_i]]$, the formal power series ring. Let $x = (P_1, \ldots, P_1, \ldots, P_r, \ldots, P_r)$ in $C(k)^n$, with m_1 times P_1, m_2 times P_2, etc. Let $X := C^n$ and $Y := C^{(n)}$. Then

$$\widehat{\mathcal{O}_{X,x}} = k[[t_{1,1}, \ldots, t_{1,m_1}, \ldots, t_{r,1}, \ldots . t_{r,m_r}]].$$

The stabilizer $\mathrm{S}_{n,x}$ of x is the subgroup $\mathrm{S}_{m_1} \times \cdots \times \mathrm{S}_{m_r}$ of S_n. One easily proves that

$$\widehat{\mathcal{O}_{Y,y}} = k[[p_{1,1}, \ldots, p_{1,m_1}, \ldots, p_{r,1}, \ldots . p_{r,m_r}]],$$

where $p_{i,1}, \ldots, p_{i,m_i}$ are the elementary symmetric polynomials in the variables $t_{i,1}, \ldots, t_{i,m_i}$. (Use that over arbitrary rings, like $k[[p_{1,1}, \ldots, p_{1,m_1}, \ldots, p_{r-1,1}, \ldots . p_{r-1,m_{r-1}}]]$, one knows that every symmetric polynomial is a polynomial in the elementary symmetric polynomials in a unique way.) This clearly shows that $\mathcal{O}_{Y,y}$ is regular.

It remains to show that $C^{(n)}$ is projective. The next example shows that $(\mathbb{P}^1_k)^{(n)}$ is isomorphic to $\mathbb{P}^n$. Let $f\colon C \to \mathbb{P}^1_k$ be dominant. Then f is finite. It follows that the induced morphism $C^{(n)} \to (\mathbb{P}^1_k)^{(n)}$ is finite. Hence $C^{(n)}$ is finite over $\mathbb{P}^n_k$, and $C^{(n)}$ is projective. $\square$

9.3.2 Example. Let k be any field. We want to show that $(\mathbb{P}^1_k)^{(n)}$ is isomorphic to $\mathbb{P}^n_k$. So first we construct a morphism $f\colon (\mathbb{P}^1_k)^n \to \mathbb{P}^n_k$ and then we show that it is the quotient for the action of S_n. Let A be any k-algebra. Let $P_1, \ldots, P_n$ be in $\mathbb{P}^1_k(A)$. Locally on A (or, more correctly, on $\mathrm{Spec}(A)$) we can write $P_i = (a_i, b_i)$ with a_i and b_i in A such that $Aa_i + Ab_i = A$. Consider the polynomial $(b_1x - a_1y) \cdots (b_nx - a_ny)$ in $A[x, y]$. Its coefficients give an element $f(P)$ in $\mathbb{P}^n_k(A)$. One verifies that this in fact defines a morphism f as desired. Let us now show that f is a quotient for the action of S_n. It is clear that f is S_n-invariant, hence we get a morphism $g\colon (\mathbb{P}^1_k)^{(n)} \to \mathbb{P}^n_k$. Both source and target are integral and projective and smooth over k. The morphism g is finite because f is. Now look at the function fields. One computes easily that $k((\mathbb{P}^1_k)^n)$ has degree $n!$ over $k(\mathbb{P}^n_k)$ and over $k((\mathbb{P}^1_k)^{(n)})$. It follows that the latter two fields are the same. Since both $\mathbb{P}^n_k$ and $(\mathbb{P}^1_k)^{(n)}$ are normal, they are in fact the same.

The most important part of this section is to understand $C^{(n)}$ as a functor. In fact, Milne's text contains some mistakes: his Propositions 3.10 and 3.11 are not true; one would have to suppose that the scheme T (in the notation of Milne) is reduced. One can prove that his Theorem 3.13 is true (but the proof given by Milne is incomplete). To keep things as simple as possible, we will use a somewhat weaker version of that theorem.

9.3.3 Definition. *Let T be any k-scheme. An effective relative Cartier divisor D on C_T of degree n is a closed subscheme D of C_T which is finite and locally free of rank n over T and whose sheaf of ideals $\mathcal{I}_D$ is locally generated by one element which is not a zero-divisor.*

9.3.4 Remark. Let P be a T-valued point of C. Then $P(T) \subset C_T$ is an effective relative Cartier divisor P of degree one on C_T (we view P as a section of $C_T \to T$). One can add two effective relative Cartier divisors D_1 and D_2 on C_T: the sum $D_1 + D_2$ has ideal sheaf $\mathcal{I}_{D_1}\mathcal{I}_{D_2}$. The degree of D_1+D_2 is the sum of the degrees of D_1 and D_2. If one has $D_1+D_2 = D_1+D_3$, then $D_2 = D_3$ (this follows directly from the fact that a local generator of the sheaf of ideals is not a zero-divisor. The set of effective relative Cartier divisors of degree n on C_T will be denoted $\mathrm{Div}_C^n(T)$. This set varies functorially in T: a morphism $T' \to T$ induces a map $\mathrm{Div}_C^n(T) \to \mathrm{Div}_C^n(T')$: D is mapped to $D_{T'}$ which is in fact in $\mathrm{Div}_C^n(T')$ (here one uses that D is flat over T). We have a morphism of functors $p\colon C^n \to \mathrm{Div}_C^n$ defined as follows: for T a k-scheme map $(P_1, \ldots, P_n)$ in $C^n(T)$ to the element $P_1 + \cdots + P_n$ of $\mathrm{Div}_C^n(T)$.

Milne's Theorem 3.13 says the following.

9.3.5 Theorem. *There exists a unique morphism of functors $C^{(n)} \to \mathrm{Div}_C^n$ compatible with $\pi\colon C^n \to C^{(n)}$ and $p\colon C^n \to \mathrm{Div}_C^n$. This morphism is an isomorphism.*

The weaker version that we will use concerns two subobjects. Let $\Delta \subset C^n$ be the union of the "diagonals" $\Delta_{i,j}$ with $i < j$: for $i < j$ let $\mathrm{pr}_{i,j}\colon C^n \to C^2$ be the projection on the ith and jth factors; then $\Delta_{i,j} := \mathrm{pr}_{i,j}^{-1}\Delta$ where this Δ is the diagonal in $C \times_k C$. By construction, $\Delta \subset C^n$ is S_n-stable. We denote its image in $C^{(n)}$ still by Δ. Then $(C^n - \Delta)/\mathrm{S}_n = C^{(n)} - \Delta$. The subobject of Div_C^n that we consider is the following. For T a k-scheme we define $\mathrm{Div}_C^{\mathrm{et},n}(T)$ to be the subset of those D of $\mathrm{Div}_C^n(T)$ whose geometric fibres over T are reduced (i.e., the D that are etale over T). This $\mathrm{Div}_C^{\mathrm{et},n}$ is a subfunctor of Div_C^n. It is clear from the construction that the morphism $p\colon C^n \to \mathrm{Div}_C^n$ induces a morphism $p\colon (C^n - \Delta) \to \mathrm{Div}_C^{\mathrm{et},n}$.

9.3.6 Theorem. *There exists a unique morphism of functors $C^{(n)} - \Delta \to \mathrm{Div}_C^{\mathrm{et},n}$ compatible with $\pi\colon (C^n - \Delta) \to (C^{(n)} - \Delta)$ and $p\colon (C^n - \Delta) \to \mathrm{Div}_C^{\mathrm{et},n}$. This morphism is an isomorphism.*

10 March 18, 1996

10.1 Symmetric products of curves, continued

Our task is to prove Thm. 9.3.6. We will first show that there exists a unique morphism of functors $\overline{p}\colon C^{(n)}-\Delta \to \mathrm{Div}_C^{\mathrm{et},n}$ which is compatible with π and p. Then we will show that $\overline{p}$ is an isomorphism. Recall that, by Yoneda's lemma, $\mathrm{Hom}(C^{(n)}-\Delta, \mathrm{Div}_C^{\mathrm{et},n}) = \mathrm{Div}_C^{\mathrm{et},n}(C^{(n)}-\Delta)$. Let D' be the element of $\mathrm{Div}_C^{\mathrm{et},n}(C^n-\Delta)$ that corresponds to the morphism p. We have to show that there is a unique element D of $\mathrm{Div}_C^{\mathrm{et},n}(C^{(n)}-\Delta)$ such that $D' = \pi^* D$. This D has to be a closed subscheme of $C_{C^{(n)}-\Delta}$ with certain properties. We have a good candidate for D: the quotient D'/S_n.

10.1.1 Proposition. *Let D be the quotient of D' by the action of S_n. Then D is a closed subscheme of $C_{C^{(n)}-\Delta}$, one has $\pi^{-1}D = D'$ and D is an effective relative etale Cartier divisor of degree n. Moreover, D is the unique closed subscheme of $C_{C^{(n)}-\Delta}$ such that $\pi^{-1}D = D'$.*

Proof. Let us write $X := C^n - \Delta$ and $Y := C^{(n)} - \Delta$. Let i' denote the closed immersion of D' into C_X. By construction we get a morphism $i\colon D \to C_Y$. Since D' is finite over Y, D is finite over Y. One verifies that it suffices to prove the theorem after base change to $\overline{k}$. So now we suppose that k is algebraically closed. Let us show that i is a closed immersion. We know that i is closed. We have to see that i is injective and that for each d in $D(k)$ the morphism $i^{\#}\colon \mathcal{O}_{C_Y,i(d)} \to \mathcal{O}_{D,d}$ is surjective. Let y in $Y(k)$ be the image of d, and choose x in $X(k)$ with image y. Then $x = (P_1,\ldots,P_n)$ with the P_i in $C(k)$ all distinct. We choose uniformizers t_i at the P_i. Then $\widehat{\mathcal{O}_{X,x}} = k[[t_1,\ldots,t_n]] = \widehat{\mathcal{O}_{Y,y}}$, as we have seen in the proof of Prop. 9.3.1. That same proof, applied to C_X and to D' also shows that i, after base change from Y to $\mathrm{Spec}(\widehat{\mathcal{O}_{Y,y}})$, coincides with the base change of i' from X to $\mathrm{Spec}(\widehat{\mathcal{O}_{X,x}})$. Using this, it is standard that i is injective and that $i^{\#}$ surjective at d. Hence i is a closed immersion. It also follows that D is an effective relative etale Cartier divisor of degree n, and that $\pi^{-1}D = D'$. Suppose that E is a closed subscheme of C_Y such that $\pi^{-1}E = D$. Then for all y in $Y(k)$ the base changes to $\mathrm{Spec}(\widehat{\mathcal{O}_{Y,y}})$ of D and E must coincide. It follows that $E = D$. $\square$

In order to show that $\overline{p}\colon C^{(n)}-\Delta \to \mathrm{Div}_C^{\mathrm{et},n}$ is an isomorphism we will construct an inverse of it. To do that, we need some lemmas on finite etale morphisms.

10.1.2 Lemma. *Let $f\colon X \to Y$ be a finite etale morphism with a section $P\colon Y \to X$. Then P is an open and closed immersion, and the Y-scheme X is the disjoint union of the image of P and its complement, both of which are finite etale over Y.*

Proof. One reduces to Y affine, say $Y = \mathrm{Spec}(A)$. Then X is affine too, say $X = \mathrm{Spec}(B)$. We may suppose that B is free of some rank n as A-module. Let $I \subset B$ be the kernel of $P^\#$ and let $J \subset B$ be the annihilator of I. We have $B = A \oplus I$ as A-modules. The etaleness of X over Y at P implies that (and is in fact equivalent too) $I^2 = I$. Nakayama's lemma implies that I locally generated by one element as a B-module (note that I is finitely generated as A-module since it is a quotient of B; hence I is finitely generated as B-module). It follows that I is a locally free B/J-module of rank one. We may suppose that I is generated by an element x. Then $x^2 = ux$ with $\overline{u}$ a unit B/J. Let v be in B such that $\overline{v} = \overline{u}^{-1}$ in B/J, and put $e := vx$. We then have $e^2 = v^2x^2 = v^2ux = v(vux) = vx = e$. This idempotent gives the decomposition we need. $\square$

10.1.3 Lemma. *Let S be a scheme, and X a finite etale S-scheme of some rank n. Then the contravariant functor $F\colon (\mathrm{Sch}/S) \to (\mathrm{Sets})$ sending $T \to S$ to the set of isomorphisms of T-schemes $\phi\colon \coprod_{i=1}^n T \to X_T$ is representable by a finite etale S-scheme S' of rank $n!$. The obvious action of S_n on S' is free and has quotient $S' \to S$.*

Proof. Let us first consider the functor $H\colon (\mathrm{Sch}/S) \to (\mathrm{Sets})$ that sends $T \to S$ to the set of T-morphisms $\phi\colon \coprod_{i=1}^n T \to X_T$. This functor is obviously represented by the n-fold fibered product X^n of X over S. The functor F is a subfunctor of H, so we want to show that it is represented by some subscheme of X^n. Let us consider an S-scheme T and an element ϕ of $H(T)$. Then ϕ is given by an n-tuple $P := (P_1, \ldots, P_n)$ of elements of $X(T)$. We view the P_i as elements of $X_T(T)$. Then ϕ is an isomorphism if and only if the n sections P_i are disjoint, i.e., iff for all $i < j$ the closed subscheme of T defined by $P_i = P_j$ is empty (note that in that case the disjoint union of n copies of T is a closed subscheme of X_T; a degree consideration shows that this closed subscheme is equal to X_T). It follows that ϕ is an isomorphism if and only if the morphism $(P_1, \ldots, P_n)$ from T to X^n factors through the open subscheme $S' := X^n - \Delta$, where Δ is the union over all $i < j$ of the (i,j)th diagonal, just as defined in Section 9.3. This means that F is represented by S'. An iterated application of Lemma 10.1.2 shows that S' is finite etale over S, its degree is equal to $n!$. The action by S_n is free in the sense that S_n acts freely on all sets $S'(T)$. It remains to show that the quotient is S. This is clear in the case where X is isomorphic to $\coprod_{i=1}^n S$. But this condition is verified after the base change $S' \to S$. Hence $S'_{S'} \to S'$ is the quotient for the action by S_n on $S'_{S'}$ obtained by base change. Hence we have $(S'/\mathrm{S}_n)_{S'} = S'$ (use Prop. 9.2.2). Since $S' \to S$ is faithfully flat (i.e., it is flat and surjective) we have $S'/\mathrm{S}_n = S$. $\square$

We can now construct the inverse of $\overline{p}$. Let S be a k-scheme, and let E be in $\mathrm{Div}_C^{\mathrm{et},n}(S)$. Let S' be the S-scheme given by Lemma 10.1.3. Then $E_{S'}$ can be written as $P_1 + \cdots + P_n$, with the P_i disjoint. These P_i define a morphism $\phi'\colon S' \to C^n - \Delta$, such that $\phi'^{-1}D' = E_{S'}$, where

D' is as in Prop. 10.1.1. Taking quotients by S_n gives a morphism $\phi\colon S \to C^{(n)} - \Delta$ such that $\phi^{-1}D = E$. This construction defines a morphism from $\mathrm{Div}_C^{\mathrm{et},n}$ to $C^{(n)} - \Delta$, of which on verifies that it in inverse to $\overline{p}$. This finishes the proof of Theorem 9.3.6.

10.2 Effective divisors of degree g, continuation of 8.4

Let C be a smooth projective geometrically irreducible curve over an algebraically closed field k. In 8.4 we showed that for "most" $(P_1, \ldots, P_g)$ in $C^g(k)$ one has $l(P_1 + \cdots + P_g) = 1$. We want to show that this condition in fact defines a Zariski open subset U of C^g.

10.2.1 Proposition. *The subset of $(P_1, \ldots, P_g)$ in $(C^g - \Delta)(k)$ such that $l(P_1 + \cdots + P_g) = 1$ is Zariski open and not empty.*

Proof. We define a line bundle $\mathcal{L}$ on C^g by:

$$\mathcal{L} := \bigotimes_{i=1}^{g} \mathrm{pr}_i^* \Omega^1_{C/k}.$$

We choose a basis $\omega_1, \ldots, \omega_g$ of $V := \Gamma(C, \Omega^1_{C/k})$. An element P of $C(k)$ defines a morphism of k-vector spaces $P^*\colon V \to P^*\Omega^1_{C/k}$ that we consider as a kind of functional on V since $P^*\Omega^1_{C/k}$ is of dimension one. Just as in 8.4 one sees that an element $(P_1, \ldots, P_g)$ of $(C^g - \Delta)(k)$ has $l(P_1 + \cdots + P_g) = 1$ if and only if the functionals $P_1^*, \ldots, P_g^*$ are linearly independent (say if one chooses bases of the $P_i^*\Omega^1_{C/k}$). This condition is equivalent to saying that the determinant $\det(P_i^*\omega_j)$, which is an element of the one dimensional k-vector space $\otimes_{i=1}^g P_i^*\Omega^1_{C/k}$, is non-zero. We can do this construction globally on C^g: consider the section $s := \det(\mathrm{pr}_i^*\omega_j)$ of $\mathcal{L}$ on C^g. Then $D(s) \cap (C^g - \Delta)$ is the set of $(P_1, \ldots, P_g)$ with $l(P_1 + \cdots + P_g) = 1$. Hence the result. $\square$

10.2.2 Remark. It is clear that our section s of $\mathcal{L}$ vanishes on Δ. Hence s can be considered as a section s' of $\mathcal{L} \otimes \mathcal{L}(-\Delta)$. It is not hard to see that in fact $D(s') \subset C^g$ is the open subset such that $(P_1, \ldots, P_g)$ has $l(P_1 + \cdots + P_g) = 1$ iff $(P_1, \ldots, P_g)$ is in it. We will not use this, but it is clear that it gives some interesting information on the morphism of C^g to the degree g part of the Picard functor.

10.3 Definition of the relative Picard functor

Let C be a smooth projective geometrically irreducible curve over a field k. Let g be its genus. The jacobian variety J that we want to construct should represent the degree zero part of what we will call the relative Picard functor of C over k. One would be tempted to try to show that the functor $(\mathrm{Sch}/k) \to (\mathrm{Sets})$ that sends S to $\mathrm{Pic}(C_S)$ is representable, and say that J is the subscheme that represents the subfunctor that sends S to the subset $\mathrm{Pic}^0(C_S)$ of $\mathrm{Pic}(C_S)$ consisting of isomorphism classes of invertible $\mathcal{O}_{C_S}$-modules that have degree zero on all fibres X_s. But the functor $S \mapsto \mathrm{Pic}(C_S)$ is not representable. For example, suppose that we have P in $C(k)$. Then for each S we have a section P^* of $\mathrm{Pic}(S) \to \mathrm{Pic}(C_S)$. This shows that $\mathrm{Pic}(S) \to \mathrm{Pic}(C_S)$ is injective. But then $\mathrm{Pic}(C_S)$ does not behave at all as a sheaf: let $\mathcal{L}$ be an invertible $\mathcal{O}_S$-module, then $p^*\mathcal{L}$ is locally trivial on S, but it is easy to get examples where it is non-trivial globally (e.g., take $S := \mathbb{P}^1_k$). So it is not $S \mapsto \mathrm{Pic}^0(C_S)$ that will be represented by J, but a kind of sheafification of it. In general, this sheafification is hard to describe, but if $C(k)$ is not empty it has an easy description. So we will assume from now on that we have an element P_0 in $C(k)$. For each S we have $P_0^*\colon \mathrm{Pic}(C_S) \to \mathrm{Pic}(S)$. It is a section of $\mathrm{Pic}(S) \to \mathrm{Pic}(C_S)$, hence it induces an isomorphism between $\mathrm{Pic}(C_S)$ and $\mathrm{Pic}(S) \oplus \mathrm{Pic}(C_S)/\mathrm{Pic}(S)$. The relative Picard functor $\mathrm{Pic}_{C/k}$ is defined by: $\mathrm{Pic}_{C/k}(S) := \mathrm{Pic}(C_S)/\mathrm{Pic}(S)$.

Let S be a k-scheme and $\mathcal{L}$ an invertible $\mathcal{O}_{C_S}$-module. Then the function $\deg_{\mathcal{L}}\colon S \to \mathbb{Z}$, $s \mapsto \deg(\mathcal{L}_s)$ is locally constant on S (this is proved using the fact that the Euler characteristic of $\mathcal{L}$ is locally constant; see the proof of [Har, III, Thm. 9.9). It follows that S is the disjoint union of its open and closed subschemes S_i, $i \in \mathbb{Z}$, on which $\mathcal{L}$ has degree i. If $\mathcal{L}$ is isomorphic to $p^*\mathcal{M}$ for some invertible $\mathcal{O}_S$-module $\mathcal{M}$, then $\mathcal{L}$ has degree zero on all fibres. For i in $\mathbb{Z}$ we define $\mathrm{Pic}^i_{C/k}$ to be the functor $S \mapsto \mathrm{Pic}^i(C_S)/\mathrm{Pic}(S)$. It follows that $\mathrm{Pic}_{C/k}$ is representable if and only if $\mathrm{Pic}^0_{C/k}$ is, and that in that case, $\mathrm{Pic}_{C/k}$ is a disjoint union indexed by $\mathbb{Z}$ of copies of $\mathrm{Pic}^0_{C/k}$ (use the $- \otimes \mathcal{L}(iP_0)$).

10.4 Representability of $\mathrm{Pic}^0_{C/k}$

We recall the situation: C is a smooth projective geometrically irreducible curve over a field k, such that $C(k)$ is not empty.

10.4.1 Theorem. *The functor $\mathrm{Pic}^0_{C/k}$ is representable. The k-scheme that represents it (unique up to unique isomorphism) is called the jacobian variety J of C.*

Proof. Because of lack of time, we will only give a proof in the case where k is algebraically closed. So from now on we assume that $k = \overline{k}$. As always, let g be the genus of C. Let U be the open subscheme of $C^g - \Delta$ given by Prop. 10.2.1: $U(k)$ is the set of $(P_1, \ldots, P_g)$ such that $l(P_1 + \cdots + P_g) = 1$. By definition, $U \subset C^g$ is stable under the action of S_g; let V be its quotient, this is an open subscheme of $C^{(g)} - \Delta$. As explained in 8.4, this V should be the open subscheme on which the morphism $\phi\colon C^{(g)} \to \mathrm{Pic}^g_{C/k}$ is an open immersion, but since we do not know yet that $\mathrm{Pic}^g_{C/k}$ is a scheme, it is not directly clear what this means (we will see in a moment what it means). Anyway, we will try to construct a scheme J representing $\mathrm{Pic}^0_{C/k}$ by glueing copies of V. For each x in $\mathrm{Pic}^g(C)$ we define $\phi_x\colon V \to \mathrm{Pic}^0_{C/k}$ to be $t_{-x}\circ\phi$, where $t_{-x}\colon \mathrm{Pic}^g_{C/k} \to \mathrm{Pic}^0_{C/k}$ is the translation by $-x$. Let V_x be a copy of V. We will think of the $\phi_x\colon V_x \to \mathrm{Pic}^0_{C/k}$ as charts. The next step in the proof is to find certain subfunctors $\mathrm{Pic}^0_{C/k,x}$ of $\mathrm{Pic}^0_{C/k}$ such that ϕ_x induces an isomorphism between V_x and $\mathrm{Pic}^0_{C/k,x}$. Let $\mathcal{L}_x$ be an invertible $\mathcal{O}_C$-module in the isomorphism class x. Let D be in $V_x(k)$. Then $\phi_x(D)$ is the isomorphism class of an invertible $\mathcal{O}_C$-module $\mathcal{L}$ such that there exists a unique divisor E of degree g on C such that $\mathcal{L}\otimes\mathcal{L}_x \cong \mathcal{L}(E)$, and that moreover this divisor E is etale (in fact, it is D). To define $\mathrm{Pic}^0_{C/k,x}$, we need to have a version of this over arbitrary k-schemes. So let S be a k-scheme and $\mathcal{L}$ be an invertible $\mathcal{O}_{C_S}$-module which has degree zero on all C_s. Let $q\colon C_S \to C$ be the projection. Let $S'_x \subset S$ be the set of s such that $\Gamma(C_{k(s)}, i_s^*(\mathcal{L}\otimes q^*\mathcal{L}_x))$ has dimension one over $k(s)$, where $i_s\colon C_{k(s)} \to C_S$ is the morphism obtained from the base change $\mathrm{Spec}(k(s)) \to S$. It follows from [Har, III, Thm 12.11] that S'_x is an open subset of S, that $p_*(\mathcal{L}\otimes q^*\mathcal{L}_x)$ is locally free of rank one on S'_x and that the morphisms $(p_*(\mathcal{L}\otimes q^*\mathcal{L}_x))_s \to \Gamma(C_{k(s)}, i_s^*(\mathcal{L}\otimes q^*\mathcal{L}_x))$ are surjective for s in S'_x. This gives us an effective relative Cartier divisor D_x on $C_{S'_x}$. Let S_x be the biggest open subset of S'_x over which D_x is etale. It follows from Thm. 9.3.6 that there is a unique morphism $S_x \to V_x$ such that D_x is the pullback of the universal divisor over V_x. Let $\mathrm{Pic}^0_{C/k,x}$ be the subfunctor of $\mathrm{Pic}^0_{C/k}$ such that for all k-schemes S, $\mathrm{Pic}^0_{C/k,x}(S)$ consists of those $\mathcal{L}$ for which $S_x = S$. It follows that ϕ_x induces an isomorphism from V_x to $\mathrm{Pic}^0_{C/k,x}$.

We can now get glueing data for the V_x. Let x and y be in $\mathrm{Pic}^g(C)$. Then we have open subsets $V_{x,y} \subset V_x$ and $V_{y,x} \subset V_y$. By construction, ϕ_x and ϕ_y induce an isomorphism between them. These isomorphisms satisfy the transitivity condition necessary to glue the V_x. Let J be the k-scheme obtained by glueing the V_x. It is then reasonably straightforward to show that the ϕ_x glue to an isomorphism $J \to \mathrm{Pic}^0_{C/k}$. $\square$