Algebraic geometry, Oslo 1970

Proceedings of the 5th Nordic Summer-School in Mathematics

Oslo, August 5-25, 1970

F. OORT, editor

Professor of Mathematics, University of Amsterdam

WOLTERS-NOORDHOFF PUBLISHING GRONINGEN

THE NETHERLANDS

INTRODUCTION TO THE THEORY OF MODULI

by

David Mumford and Kalevi Suominen [1]

5th Nordic Summer-School in Mathematics
Oslo, August 5–25, 1970

1. Endomorphisms of vector spaces

Throughout these notes, k is an algebraically closed field, varieties are reduced and irreducible k-schemes of finite type, and morphisms of varieties are k-morphisms.

A moduli problem for a class of algebraic objects consists in two parts: finding the equivalence classes of the objects under a suitable equivalence relation (usually isomorphism), and parametrizing these classes by means of a scheme (or a geometric object of more general type). In this chapter we shall be interested in the moduli of endomorphisms of vector spaces.

More precisely, let V be a vector space of dimension n over k, and let T be an endomorphism of V. The problem of classifying pairs (V, T) up to isomorphism is readily solved: there is a basis of V such that the matrix of T with respect to this basis is in the *Jordan canonical form*

$$\left(\begin{array}{ccccc|c|c} \lambda_1 & \varepsilon_{11} & 0 & \cdots & 0 & & \\ 0 & \lambda_1 & \varepsilon_{21} & \cdots & 0 & & \\ 0 & 0 & \lambda_1 & \cdots & 0 & 0 & 0 \\ & \cdots & & & & & \\ 0 & 0 & 0 & & \varepsilon_{31} & & \\ 0 & 0 & 0 & \cdots & \lambda_1 & & \\ \hline & & & & & \lambda_2 & \varepsilon_{12} \cdots 0 \\ & & & & & 0 & \lambda_2 \cdots 0 \\ & & & & & \cdots & \cdots \\ & & 0 & & & 0\ 0 & \cdots \lambda_2 \\ \hline & & 0 & & & 0 & \end{array}\right)$$

where $\varepsilon_{ij} = 0$ or 1.

[1] Assisted by M. Hazewinkel, A. Cooper, J. H. M. Steenbrink, and F. Huikeshoven.

For the second part of the moduli problem we must introduce algebraic families of pairs (V, T). Intuitively, a family of vector spaces, parametrized by a variety S, is a vector bundle over S, and an algebraic family of endomorphisms of the fibers of this vector bundle is an endomorphism of the bundle. Now, the algebraic counterpart of a bundle is a locally free sheaf of $\mathcal{O}_S$-modules. Hence we are led to the following:

DEFINITION 1. An algebraic family of endomorphisms of n-dimensional k-vector spaces on a k-variety S is a pair $(\mathcal{E}, T)$ where $\mathcal{E}$ is a locally free $\mathcal{O}_S$-module of rank n and T is an endomorphism of $\mathcal{E}$.

For each closed point s of S, we then have a vector space $\mathcal{E} \otimes k(s)$ of dimension n over $k(s) = k$ and an endomorphism $T \otimes k(s)$ of $\mathcal{E} \otimes k(s)$.

As a first attempt in the search for a moduli space it is natural to ask if there exists a family of endomorphisms in which each isomorphism class is represented exactly once. The answer is trivially yes, e.g., the base scheme may be chosen discrete if we drop temporarily the restriction that base schemes are varieties. This is obviously no satisfactory solution to the problem. Namely, if M is a k-scheme whose closed points are in $1-1$ correspondence with the classes of endomorphisms, then for each family of endomorphisms $(\mathcal{E}, T)$ over a variety S there is a map $S(k) \to M(k)$ associating with each closed point $s \in S$ the point of M which corresponds to the pair $(\mathcal{E} \otimes k(s), T \otimes k(s))$. This map should be induced by a morphism $S \to M$!

To express this condition more exactly we introduce some functorial terminology.

For each k-variety S, we denote by $\mathcal{F}(S)$ the set of families of endomorphisms on S, modulo isomorphism. If, $f: S' \to S$ is a morphism of varieties and $(\mathcal{E}, T)$ is a family of endomorphisms on S, then $(f^*\mathcal{E}, f^*T)$ is a family of endomorphisms on S'. Thus we obtain a map $f^* : \mathcal{F}(S) \to \mathcal{F}(S')$, and $\mathcal{F}$ becomes a contravariant functor from the category of k-varieties to the category of sets.

Now, the condition stated above can be made precise:

(A) There is a morphism of contravariant functors

$$\Phi : \mathcal{F} \to h_M,$$

where $h_M(S) = \mathrm{Hom}\,(S, M)$, such that

$$\Phi(\mathrm{Spec}(k)) : \mathcal{F}(\mathrm{Spec}(k)) \to M(k)$$

is bijective.

However, this condition does not suffice to define M uniquely. In fact, it may be possible to find other solutions M' by reducing the structure

sheaf: $\mathcal{O}_{M'} \subset \mathcal{O}_M$, having the underlying point set unchanged. Keeping this in mind, we write the final definition.

DEFINITION 2. A *coarse moduli space* for endomorphisms of n-dimensional k-vector spaces is a pair (M, Φ) consisting of a k-variety M and a morphism of functors $\Phi : \mathcal{F} \to h_M$ such that

$$\Phi(\mathrm{Spec}(k) : \mathcal{F}(\mathrm{Spec}(k)) \to M(k)$$

is bijective and such that for each k-variety N and each morphism of functors $\Psi : \mathcal{F} \to h_N$ there is a unique morphism $\kappa : M \to N$ which renders

$$\begin{array}{ccc} & \overset{\Phi(S)}{\nearrow} & \mathrm{Hom}(S, M) \\ \mathcal{F}(S) & & \downarrow{\scriptstyle \mathrm{Hom}(S,\kappa)} \\ & \underset{\Psi(S)}{\searrow} & \mathrm{Hom}(S, N) \end{array}$$

commutative for each k-variety S.

It is easy to see that a coarse moduli space is unique up to isomorphism, if it exists.

There is a priori no reason why the map

$$\Phi(S) : \mathcal{F}(S) \to \mathrm{Hom}(S, M)$$

should be bijective for k-varieties S other than $\mathrm{Spec}(k)$. That this be the case for all varieties S amounts to saying that the functor $\mathcal{F}$ is representable by M. Then the family $(\mathcal{E}, T)$ of endomorphisms on M which corresponds to the identity morphism of M is *universal* in the following sense: For each family of endomorphisms $(\mathcal{E}', T')$ on a variety S there is a unique morphism $f : S \to M$ such that $(f^*\mathcal{E}, f^*T)$ is isomorphic to $(\mathcal{E}', T')$.

DEFINITION 3. A *fine moduli space* for endomorphisms of n-dimensional k-vectorspaces is a pair (M, Φ) where M is a k-variety and $\Phi : \mathcal{F} \to h_M$ is an isomorphism of functors.

It is not difficult to see that a fine moduli space is also a coarse moduli space.

REMARK. Definitions 2 and 3 will also be applied to other functors. In any case, it is clear that a coarse moduli space is a fine moduli space if and only if the functor is representable.

Unfortunately, there is no fine moduli space for endomorphisms of vector spaces. Namely, if $(\mathcal{E}, T)$ is any family of endomorphisms on a variety S then for each invertible $\mathcal{O}_S$-Module L the family $(\mathcal{E} \otimes L, T \otimes 1)$ corresponds to the same morphism $S \to M$. Hence

$$\mathscr{F}(S) \to \mathrm{Hom}(S, M)$$

is not injective if there are non-trivial invertible sheaves on S.

But things are worse: *not even a coarse moduli space exists*! To see this, let us consider the variety $S = \boldsymbol{A}^1 = \mathrm{Spec}(k[t])$ with $\mathscr{E} = \mathscr{O}_S^2$ and T defined by the matrix

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$$

All the pairs $(\mathscr{E} \otimes k(s), T \otimes k(s))$ are isomorphic for closed points s of S different from 0. Hence the map $S \to M$ corresponding to the family is constant on $\boldsymbol{A}^1 - 0$. By continuity, it must be constant on S, although $(\mathscr{E} \otimes k(0), T \otimes k(0)) = (k^2, 1)$ is *not* isomorphic to $(\mathscr{E} \otimes k(s), T \otimes k(s))$ for $s \neq 0$.

This is a typical example of the so called *jump phenomenon*, which ruins the hope of finding solutions to many moduli problems.

Similar constructions show that endomorphisms with isomorphic semi-simple parts are represented by the same point of any variety M with a morphism of functors $\mathscr{F} \to h_M$.

On the other hand, there is a variety M which separates endomorphisms with non-isomorphic semi-simple parts or, what amounts to the same, with different characteristic polynomials:

PROPOSITION 1. *There is a morphism of functors*

$$\Psi : \mathscr{F} \to h_{\boldsymbol{A}^n}$$

such that $\Psi(\mathrm{Spec}(k)) : \mathscr{F}(\mathrm{Spec}(k)) \to \boldsymbol{A}^n(k)$ *is given by*

$$(V, T) \to (a_1, \cdots, a_n),$$

where $X^n + a_1 X^{n-1} + \cdots + a_n$ *is the characteristic polynomial of* T.

PROOF. Let $(\mathscr{E}, T)$ be a family of endomorphisms on a variety S. There is an affine open covering (U_α) of S such that $\mathscr{E}|U_\alpha$ is free of rank n. If $T|U_\alpha$ is represented by an $n \times n$ matrix T with entries in $\Gamma(U_\alpha, \mathscr{O}_S)$, then

$$P_{T|U_\alpha}(X) = \det(X \cdot I - T_\alpha) \in \Gamma(U, \mathscr{O}_S)[X]$$

is a polynomial of degree n which is independent of the trivialization $\mathscr{E}|U_\alpha \xrightarrow{\sim} \mathscr{O}_{U_\alpha}^n$. But then $P_{T|U_\alpha}(X)$ and $P_{T|U_\beta}(X)$ coincide on $U_\alpha \cap U_\beta$, and so they may be joined together to define the *characteristic polynomial* of T:

$$P_T(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in \Gamma(S, \mathscr{O}_S)[X].$$

Hence we may associate with $(\mathscr{E}, T)$ canonically a morphism

$$(a_1, \cdots, a_n) : S \to A^n.$$

The rest of the proposition follows immediately.

The partly negative results we have obtained so far are intuitively in agreement with our knowledge of the Jordan canonical form of an endomorphism. Indeed, the entries outside the diagonal are constants 0 or 1. Hence the eigenvalues, or rather their symmetric polynomials, are the only true 'moduli' of endomorphisms.

To get at least a coarse moduli space we must somehow restrict the class of endomorphisms. We shall consider two canonical possibilities: endomorphisms with all $\varepsilon_{ij} = 0$ in the Jordan canonical form, i.e., semi-simple endomorphisms, and endomorphisms with all $\varepsilon_{ij} = 1$. It is not difficult to see that the latter are exactly those endomorphisms $T : V \to V$ for which there is a cyclic vector or, more precisely, a vector $v \in V$ such that $(v, Tv \cdots, T^{n-1}v)$ is a basis of V.

Let us first consider semi-simple endomorphisms. For each variety S, let $\mathscr{F}_d(S)$ denote the set of families of endomorphisms $(\mathscr{E}, T)$ on S, modulo isomorphism, such that $T \otimes k(s)$ is semi-simple for each closed point s of S. Clearly, these sets form a subfunctor $\mathscr{F}_d$ of $\mathscr{F}$.

It follows immediately from proposition 1 that $M = A^n$ satisfies the condition (A) for the functor $\mathscr{F}_d$. But we can say more:

PROPOSITION 2. *A^n is a coarse moduli space for semi-simple endomorphisms of n-dimensional vector spaces.*

PROOF. Let $M = A^n = \mathrm{Spec}(k[t_1, \cdots, t_n])$ and define an endomorphism T of $\mathscr{O}_M^n$ by the matrix

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -t_n \\ 1 & 0 & 0 & \cdots & 0 & -t_{n-1} \\ 0 & 1 & 0 & \cdots & 0 & -t_{n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 & -t_2 \\ 0 & 0 & 0 & \cdots & 1 & -t_1 \end{pmatrix}$$

Then the characteristic polynomial of T is

$$P_T(X) = X^n + t_1 X^{n-1} + \cdots + t_n$$

So, if $\Delta \in k[t_1, \cdots, t_n]$ is the discriminant of $P_T(X)$ and

$$U = D(\Delta) = \{x \in A^n | \Delta(x) \neq 0\},$$

the restriction $(\mathscr{O}_U^n, T|U)$ is a family of semi-simple endomorphisms.

Now, if N is any k-variety and $\Phi : \mathscr{F}_d \to h_N$ is a morphism of functors, $\Phi(U)$ of the class of $(\mathscr{O}_U^n, T|U)$ is a morphism $\varphi : U \to N$. Let $\Gamma \subset U \times N$

be its graph and denote by $\bar{\Gamma}$ the closure of Γ in $M \times N$. We claim that the projection $\bar{\Gamma} \to M$ is an isomorphism.

To prove this, put $S = \mathrm{Spec}(k[\lambda_1, \cdots, \lambda_n])$ and define by

$$T^1 = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$$

a family $(\mathcal{O}_S^n, T^1)$ of semi-simple endomorphisms on S. There are two morphisms $f: S \to M$ and $g: S \to N$ associated with this family. Clearly, f is given by

$$X^n + t_1 X^{n-1} + \cdots + t_n = (X - \lambda_1) \cdots (X - \lambda_n).$$

Hence each λ_i is integral over $k[t_1, \cdots, t_n]$, i.e., f is finite. Then $h = (f, g): S \to M \times N$ is finite (EGA II, 6, 1, 5 (v)) and therefore $h(S)$ is closed in $M \times N$.

On the other hand, inspecting the closed points it is not difficult to see that $\Gamma = h(V)$, where $V = f^{-1}(U) = \bigcap_{i \neq j} D(\lambda_i - \lambda_j)$. Hence $h(S) = \bar{\Gamma}$, and so $\bar{\Gamma} \to M$ is surjective with finite fibres. But then it is an isomorphism by Zariski's Main Theorem.

Now, $\bar{\Gamma}$ is the graph of a morphism $\psi: M \to N$ extending φ. If S is any variety, and $f: S \to M$, $g: S \to N$ are the morphisms corresponding to a family of semi-simple endomorphisms on S, then g and $\Psi \circ f$ coincide at all closed points of S, whence $\Psi \circ f = g$.

COROLLARY. *There is no fine moduli space for semi-simple endomorphisms of n-dimensional vectorspaces if* $n > 1$.

PROOF. Otherwise, there would exist a universal family $(\mathcal{E}, T)$ of semi-simple endomorphisms on $\boldsymbol{A}^n$. Let $R = k[[t_1, \cdots, t_n]]$ be the completion of the local ring of 0 on $\boldsymbol{A}^n$, and let $(\mathcal{E}', T')$ be the family induced by $(\mathcal{E}, T)$ on Spec (R). Since R is local, $\mathcal{E}'$ is free, and therefore $(\mathcal{E}', T')$ is isomorphic to $(\mathcal{O}^n, T'')$ where T'' is an $n \times n$ matrix with entries in the maximal ideal m of R. But then $t_n = (-1)^n \det(T'') \in m^n$, which is impossible unless $n = 1$.

REMARK. The same proof shows that in each family of endomorphisms $(\mathcal{E}, T)$ on $\boldsymbol{A}^n$ with the characteristic polynomial

$$P_T(X) = X^n + t_1 X^{n-1} + \cdots + t_n$$

the Jordan canonical form of $T \otimes k(0)$ is

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

We shall now examine the second possibility of restricting the functor $\mathscr{F}$: the families of endomorphisms with a cyclic vector. It is to be expected that A^n is a coarse module space for these. In fact, the remark above suggests that it might even be a fine moduli space.

However, we have seen that the existence of nontrivial invertible sheaves on a variety S prevents

$$\Psi(S) : \mathscr{F}(S) \to \mathrm{Hom}(S, A^n)$$

from being injective. To eliminate this type of redundancy we shall consider families with a 'cyclic section'. More precisely, for each variety S, let $\mathscr{F}'(S)$ denote the subset of $\mathscr{F}(S)$ represented by families of endomorphisms $(\mathscr{E}, T)$ on S such that there is a section $s \in \Gamma(S, \mathscr{E})$ for which $s, Ts, \cdots, T^{n-1}s$ span $\mathscr{E}$.

PROPOSITION 3. *The restriction of Ψ to $\mathscr{F}$*

$$\Psi' : \mathscr{F}' \to h_{A^n}$$

is an isomorphism of functors.

PROOF. Let $(\mathscr{E}, T)$ represent an element of $\mathscr{F}'(S)$ for some variety S. Then $\mathscr{E}$ is free with basis $s, Ts, \cdots, T^{n-1}s$ for some section $s \in \Gamma(S, \mathscr{E})$, and the matrix of T with respect to this basis is

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_n \\ 1 & 0 & 0 & \cdots & 0 & -a_{n-1} \\ 0 & 1 & 0 & \cdots & 0 & -a_{n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 & -a_2 \\ 0 & 0 & 0 & \cdots & 1 & -a_1 \end{pmatrix},$$

where the last column is determined by the characteristic polynomial of T.

$$P_T(X) = X^n + a_1 X^{n-1} + \cdots + a_n$$

as is seen by a direct computation of $\det(X, I - T)$, or by the Cayley-Hamilton theorem:

$$P_T(T) = T^n + a_1 T^{n-1} + \cdots + a_n = 0.$$

Hence the elements of $\mathscr{F}'(S)$ are in $1-1$ correspondence with the

n-tuples $(a_1, \cdots, a_n) \in \Gamma(S, \mathcal{O}_S)^n$, i.e., with the morphisms $S \to A^n$.

To explain the difference between the functors $\mathcal{F}_d$ and $\mathcal{F}'$, we note that $\mathcal{F}'$ is an open subfunctor of $\mathcal{F}$ in the following sense:

If $(\mathcal{E}, T)$ is a family of endomorphisms on a variety S, and if s is a closed point of S such that $T \otimes k(s)$ has a cyclic vector, there is an open neighborhood U of s such that $(\mathcal{E}|U, T|U)$ defines an element of $\mathcal{F}'(S)$.

In fact, if t is a section of $\mathcal{E}$ over some neighborhood of s such that $t(s) \in \mathcal{E} \otimes k(s)$ is a cyclic vector of $T \otimes k(s)$, then $t, Tt, \cdots, T^{n-1}t$ generate $\mathcal{E}$ in some neighborhood of S by Nakayama's lemma.

In the second half of this chapter we shall consider the problem of moduli of endomorphisms from another point of view, which ties up with more general theory. Namely, each family of endomorphisms is induced locally by the family $(\mathcal{E}, T)$ on $A^{n^2} = \mathrm{Spec}(k[t_{ij}])$ $(1 \leqq i, j \leqq n)$ in which $\mathcal{E} = \mathcal{O}^n$ and the matrix of T is (t_{ij}). In fact, if $(\mathcal{E}', T')$ is a family of endomorphisms on a variety S, and if (U_α) is an open covering of S such that each $\mathcal{E}'|U_\alpha$ is free, then $(\mathcal{E}'|U_\alpha, T|U_\alpha)$ is isomorphic to $(f_\alpha{}^*\mathcal{E}, f_\alpha{}^* T)$ with $f: U_\alpha \to A^{n^2}$ defined by the entries of the matrix of $T'|U_\alpha$ relative to some basis of $\mathcal{E}'|U_\alpha$. It follows that if M is a variety and $\Phi : \mathcal{F} \to h_M$ is a morphism of functors, Φ is uniquely determined by the morphism $\varphi : A^{n^2} \to M$ associated with $(\mathcal{E}, T)$. Hence the properties of Φ may be derived from a study of φ.

The set of closed points of A^{n^2} may be identified with the set $M(n)$ of $n \times n$ matrices with entries in k and the general linear group $GL(n)$ acts on $M(n)$ by $B \mapsto ABA^{-1}$, $A \in GL(n)$. Since the fibres of $(\mathcal{E}, T)$ over B and ABA^{-1} are isomorphic, $\varphi(B) = \varphi(ABA^{-1})$, i.e., φ is constant on each orbit $0(B)$.

On the other hand, if M is a variety and $\varphi : A^{n^2} \to M$ is a morphism which is constant on the orbits, then it follows from the discussion above that there is a morphism of functors $\Phi : \mathcal{F} \to h_M$ associating φ with the family $(\mathcal{E}, T)$ on A^{n^2}. Hence there is a natural $1-1$ correspondence between morphisms of functors $\Phi : \mathcal{F} \to h_M$ and morphisms $\varphi : A^{n^2} \to M$ constant on the orbits. It is then clear that the universal property of a coarse moduli space (M, Φ) (Definition 2) means that (M, φ) is a quotient of A^{n^2} by $GL(n)$ in the following sense:

DEFINITION 4. Let G be a group operating on a variety X. A *quotient* of X by G is a pair (Y, φ) in which Y is a variety and $\varphi : X \to Y$ is a morphism satisfying:

(i) φ is constant on the orbits of the closed points of X.

(ii) given a variety Z and a morphism $\Psi : X \to Z$ constant on the orbits, there is a unique morphism $\kappa : Y \to Z$ such that $\Psi = \kappa \circ \varphi$.

The quotient of X by G is clearly unique up to isomorphism.

The moduli problem of endomorphisms of n-dimensional vector spaces has now been reduced to finding a quotient of A^{n^2} by $GL(n)$. It may be shown to be A^n (cf. proposition 1), but even without this knowledge we can easily prove the non-existence of a coarse moduli space. Indeed, a quotient (Y, φ) is a coarse moduli space if and only if Y separates non-isomorphic endomorphisms, i.e., each fibre $\varphi^{-1}(y)$ consists of a unique orbit. But the fibres of any morphism are closed whereas the orbits need not be closed in general. In fact, if B is a triangular matrix

$$B = \begin{pmatrix} \lambda_1 & \sigma_{12} & \sigma_{12} & \cdots & \sigma_{1n} \\ 0 & \lambda_2 & \sigma_{23} & \cdots & \sigma_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & \sigma_{n-1,n} \\ 0 & 0 & 0 & \cdots & \lambda_n \end{pmatrix},$$

and $A \in GL(n)$ is

$$A = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \alpha & 0 & \cdots & 0 \\ 0 & 0 & \alpha^2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & \alpha^{n-1} \end{pmatrix}$$

then

$$ABA^{-1} = \begin{pmatrix} \lambda_1 & \sigma_{12}\alpha & \sigma_{13}\alpha^2 & \cdots & \sigma_{1n}\alpha^{n-1} \\ 0 & \lambda_2 & \sigma_{23}\alpha & \cdots & \sigma_{2n}\alpha^{n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & \sigma_{n-1,n}\alpha \\ 0 & 0 & 0 & \cdots & \lambda_n \end{pmatrix}$$

Hence, letting $\alpha \to 0$, we find that the semi-simple part B_s of B:

$$B_s = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$$

is in the closure of the orbit $0(B)$ of B.

More precisely, we have

PROPOSITION 4. *If B_1, B_2 are two $n \times n$ matrices, then $\overline{0(B_1)} \cap \overline{0(B_2)} \neq \phi$ if and only if $0((B_1)_s) = 0((B_2)_s)$. In any case $(B_i)_s \in \overline{0(B_i)}$ for $i = 1, 2$.*

PROOF. Since each orbit contains triangular matrices, we may assume B_1, B_2 triangular, so $(B_i)_s \in \overline{0(B_i)}$ as was shown above. But then $0((B_1)_s) = 0((B_2)_s)$ implies $\overline{0(B_1)} \cap \overline{0(B_2)} \neq \phi$. The inverse implication

follows e.g. from the existence of a morphism $\varphi : A^{n^2} \to A^n$ separating matrices with non-equivalent semi-simple parts (cf. proposition 1).

It is not hard to see that each fibre of the canonical morphism $\varphi : A^{n^2} \to A^n$ contains a unique closed orbit (semi-simple matrices) and a unique relatively open orbit (matrices with a cyclic vector), which coincide if all the eigenvalues are different. Furthermore, the union of the relatively open orbits is open in A^{n^2} whereas the union of the closed orbits is neither open nor closed (if $n > 1$). These facts are reflected in the moduli problem as shown by propositions 2 and 3.

We shall now consider the quotient of a variety by a group in general with applications to moduli problems in mind. We have seen that the closedness of orbits is one desirable property. For technical reasons it is convenient to impose the following conditions on a good orbit space:

DEFINITION 5. Let G be a group operating on a variety X. A *geometric quotient* of X by G is a pair (Y, φ) consisting of a variety Y and a morphism $\varphi : X \to Y$ satisfying:

(i) for each closed point $y \in Y$, $\varphi^{-1}(y)$ is an orbit, i.e., a closed invariant subset such that G acts transitively on its closed points.

(ii) for each invariant open subset $U \subset X$ there is an open subset $V \subset Y$ such that $U = \varphi^{-1}(V)$.

(iii) for each open set $V \subset Y$, $\varphi^* : \Gamma(V, \mathcal{O}_Y) \to \Gamma(\varphi^{-1}(V), \mathcal{O}_X)$ is an isomorphism of $\Gamma(V, \mathcal{O}_Y)$ onto the ring $\Gamma(\varphi^{-1}(V), \mathcal{O}_X)^G$ of invariant functions on $\varphi^{-1}(V)$.

REMARK. The condition (ii) is weaker than the corresponding condition iii) of definition o.6 in (GIT, p.4).

The first thing to prove is

PROPOSITION 5. *A geometric quotient of a variety by a group is a quotient. In particular, it is unique up to isomorphism.*

PROOF. Let $\Psi : X \to Z$ be a morphism which is constant on the orbits of closed points. If (W_i) is an affine open covering of Z, each $\Psi^{-1}(W_i)$ is an invariant open subset of X, hence by condition (ii) of definition 5 there is an open set $V_i \subset Y$ such that $\varphi^{-1}(V_i) = \Psi^{-1}(W_i)$. Since φ is surjective by (i), (V_i) is a covering of Y.

Now, any morphism $\kappa : Y \to Z$ such that $\Psi = \kappa \circ \varphi$ must satisfy $\kappa(V_i) \subset W_i$. Hence $\kappa | V_i$ is defined by a homomorphism $h_i : \Gamma(W_i, \mathcal{O}_Z) \to \Gamma(V_i, \mathcal{O}_Y)$ such that $\varphi^* \circ h_i = \Psi^* : \Gamma(W_i, \mathcal{O}_Z) \to \Gamma(\Psi^{-1}(W_i), \mathcal{O}_X)$. Since φ^* is injective by (iii) of definition 5, h_i is uniquely determined. Hence at most one κ exists.

But Ψ^* maps $\Gamma(W_i, \mathcal{O}_Z)$ into the ring of invariant functions

$$\Gamma(\Psi^{-1}(W_i), \mathcal{O}_X)^G = \varphi^*\Gamma(V_i, \mathcal{O}_Y).$$

Therefore such an h_i exists and defines a morphism $\kappa_i : V_i \to W_i$. By uniqueness $\kappa_i = \kappa_j$ on $V_i \cap V_j$; hence $\kappa : Y \to Z$ may be constructed.

In the rest of this chapter we shall assume that G is an algebraic group (LAG, 1.1), acting algebraically on a variety X; in other words, the action is defined by a morphism of varieties $\sigma : G \times X \to X$ (LAG, 1.7). In this case, the orbits are locally closed subvarieties (LAG, 1.8).

If $G = \mathrm{Spec}(S)$ is affine, and $R = \Gamma(X, \mathcal{O}_X)$, then σ defines a k-algebra homomorphism

$$\sigma^* : R \to S \otimes R = \Gamma(G \times X, \mathcal{O}_{G\times X}).$$

More generally, an action of G on a k-vector space V is given by a linear map

$$\hat{\sigma} : V \to S \otimes V$$

such that

$$\begin{array}{ccc} V & \xrightarrow{\hat{\sigma}} & S \otimes V \\ {\scriptstyle\hat{\sigma}}\downarrow & & \downarrow{\scriptstyle 1\otimes\hat{\sigma}} \\ S \otimes V & \xrightarrow[\hat{\mu}\otimes 1]{} & S \otimes S \otimes V \end{array}$$

commutes ($\hat{\mu} : S \to S \otimes S$ is induced by the morphism $\mu : G \times G \to G$ defining the group structure) and

$$V \xrightarrow{\hat{\sigma}} S \otimes V \xrightarrow{\varepsilon\otimes 1} k \otimes V \cong V$$

is the identity ($\varepsilon : S \to k$ is given by $\varepsilon(f) = f(1)$).

Indeed, if V is finite-dimensional, with basis $e_1, \cdots, e_n$, and $\hat{\sigma}(e_i) = \sum_j a_{ij} \otimes e_j$ $(1 \leqq i \leqq n)$, then the elements $a_{ij} \in S$ define a group homomorphism $G \to GL(n)$.

In general, a closed point g of G operates on V (on the right) by

$$x \to xg = \sum_i a_i(g) \cdot x_i$$

if $\hat{\sigma}(x) = \sum a_i \otimes x_i$. It follows immediately that each vector $x \in V$ is contained in a finite-dimensional invariant subspace ($\sum kx_i$ if the x_i are linearly independent and $a_i \neq 0$). Clearly, x is invariant if and only if $\hat{\sigma}(x) = 1 \otimes x$, and a subspace $W \subset V$ is invariant if and only if $\hat{\sigma}(W) \subset S \otimes W$.

DEFINITION 6. An affine group G is *reductive* if each action of G on a finite-dimensional vector space V is completely reductive, i.e., if $W \subset V$ is an invariant subspace, then there is an invariant subspace $W' \subset V$ such that $V = W \oplus W'$.

If the characteristic of k is 0, it may be shown that semi-simple groups are reductive (IT, 4.37).

A basic property of reductive groups is the following:

LEMMA. *If G is a reductive group acting on a vector space V, then the subspace V^G of invariant elements of V has a unique invariant complement V_G in V.*

PROOF. By Zorn's lemma there is a maximal invariant subspace $V_G \subset V$ such that $(V_G)^G = V_G \cap V^G = 0$. If $V' \subset V$ is any invariant subspace and $x \in V'$, there is a finite-dimensional invariant subspace $W \subset V'$ containing x. By complete reductivity, there is an invariant subspace $W' \subset W$ such that $W = (W \cap V_G) \oplus W'$. If $(V')^G = 0$ then $(W')^G = 0$ and therefore $(V_G \oplus W')^G = 0$. By the maximality of V_G we have $W' = 0$. Hence $V' \subset V_G$, which proves the uniqueness of V_G.

Finally, to show that $V^G \oplus V_G = V$, let $x \in V$ and let $W \subset V$ be a finite-dimensional invariant subspace containing x. Then there is an invariant subspace $W' \subset W$ such that $W = (W \cap V^G) \oplus W'$. But then $(W')^G = 0$, so $W' \subset V_G$, and therefore $x \in W \subset V^G \oplus V_G$.

The result of this lemma may be conveniently formalized by means of the *Reynolds operator* $E : V \to V$. It is the projection of V onto V^G with kernel V_G.

PROPOSITION 6. *Let G be a reductive group acting on vector spaces V and V' with Reynolds operators E and E', respectively. Then each G-linear map $u : V \to V'$ commutes with E and E':*

$$E' \circ u = u \circ E.$$

PROOF. Since $u(V^G) \subset (V')^G$, it is enough to show that $u(V_G) \subset (V')_G$. If $x \in V_G$, there is a finitedimensional invariant subspace $W \subset V_G$ containing x, and $W = (W \cap \ker(u)) \oplus W'$ for some invariant subspace $W' \subset W$. But u maps W' isomorphically onto $u(W) \subset V'$. Hence $(u(W))^G = u((W')^G) = 0$, and therefore $u(x) \in u(W) \subset V'_G$.

COROLLARY. *If a reductive group G acts on a k-algebra R by algebra automorphisms (i.e. $x \mapsto x \circ g$ is an algebra automorphism of R for each closed point $g \in G$), then the Reynolds operator E on R satisfies the Reynolds identity*

$$E(x \circ y) = x \circ E(y)$$

for $x \in R^G$, $y \in R$.

In fact, if $x \in R^G$, $y \to x \circ y$ is a G-linear map of R. Hence it commutes with E.

REMARK. If $G = \mathrm{Spec}(S)$, the assumption of the corollary means that the action $\hat{\sigma} : R \to S \otimes R$ is an algebra homomorphism.

We can now prove the main result of this chapter.

THEOREM 1. *Let G be a reductive group acting on an affine variety X with closed orbits. Then the geometric quotient (Y, φ) of X by G exists and Y is an affine variety.*

PROOF. Let $R = \Gamma(X, \mathcal{O}_X)$. Then G acts on R. Let $Y = \mathrm{Spec}(R^G)$ and define $\varphi : X \to Y$ by the inclusion $R^G \to R$. We claim that Y is an affine variety, i.e., R^G is a k-algebra of finite type.

LEMMA 1. *If S is an R^G-algebra, then S is the ring of invariants in $R \otimes_{(R^G)} S$.*

PROOF. Let E and E' be the Reynolds operators on R and $R \otimes_{(R^G)} S$ respectively. By proposition 6, $E'(a \otimes 1) = E(a) \otimes 1$ for $a \in R$. Since R is isomorphic as R^G-module to $R^G \oplus \ker E$, it follows that

$$S \cong R^G \otimes_{(R^G)} S \subset (R \otimes_{(R^G)} S)^G.$$

Conversely, if

$$f = \sum a_i \otimes b_i \in (R \otimes_{(R^G)} S)^G,$$

then

$$\begin{aligned} f &= E'(\textstyle\sum a_i \otimes b_i) = E'(\sum (a_i \otimes 1)(1 \otimes b_i)) \\ &= \textstyle\sum E'(a_i \otimes 1) \circ (1 \otimes b_i) \text{ (by Reynolds identity)} \\ &= \textstyle\sum E(a_i) \otimes b_i \in R^G \otimes_{(R^G)} S. \end{aligned}$$

If I is an ideal of R^G, then $R/IR \simeq R \otimes_{(R^G)} (R^G/I)$. Hence by lemma 1 $(R/IR)^G = R^G/I$, and therefore $IR \cap R^G = I$. This means that $I \mapsto IR$ is an order preserving injection of the set of ideals in R^G into the set of ideals in R. Since R is noetherian, R^G is also noetherian.

If $R = \sum_{n \geqq 0} R_n$ is a graded k-algebra with $R_0 = k$ and the action of G preserves the gradation, $R^G = \sum_{n \geqq 0} R_n^G$ is also a graded algebra. Since it is noetherian, the ideal $R_+^G = \sum_{n \geqq 0} R_n^G$ is generated by a finite number of homogeneous elements $f_i \in R_{n_i}^G$ $(1 \leqq i \leqq r)$. By induction on n it is then easily shown that each vector space R_n^G is generated by monomials of $f_1, \cdots, f_r$. Hence R^G is finitely generated as a k-algebra.

Finally, in the general case, let $V \subset R$ be a finite-dimensional invariant subspace containing a set of generators. Then the action of G on V extends to a gradation preserving action on the symmetric algebra $R' = S(V)$, and the canonical algebra homomorphism $u : R' \to R$ is G-linear and surjective. If E and E' are the Reynolds operators on R and R', then we have

$$R^G = E(R) = E(u(R')) = u(E'(R')) = u((R')^G)$$

by proposition 6. Hence R^G is finitely generated as a quotient of a finitely generated k-algebra $(R')^G$. This proves that Y is a variety.

LEMMA 2. *If (I_i) is a family of invariant ideals in R then*

$$(\sum_i I_i) \cap R^G = \sum_i (I_i \cap R^G).$$

PROOF. If $f \in (\sum I_i) \cap R^G$, then f is a finite sum $\sum f_i$ with $f_i \in I_i$. It follows that

$$f = Ef = \sum Ef_i \in \sum_i (I_i \cap R^G)$$

since the Reynolds operator of I_i is the restriction of the Reynolds operator E on R by proposition 6.

Writing Z_i for the closed subset of X defined by I_i we obtain the following geometric statement:

If (Z_i) is a family of closed invariant subsets of X, then

$$(*) \qquad \overline{\varphi(\cap_i Z_i)} = \cap_i \overline{\varphi(Z_i)}.$$

Now, if Z is a closed invariant subset of X and $Z' = \varphi^{-1}(y)$ where y is a closed point of Y, then

$$\overline{\varphi(Z \cap Z')} = \overline{\varphi(Z)} \cap \{y\}.$$

Hence $y \in \overline{\varphi(Z)}$ implies $Z \cap Z' \neq \phi$, i.e., $y \in \varphi(Z)$. Therefore $\varphi(Z)$ is closed, and $(*)$ becomes

$$(**) \qquad \varphi(\cap_i Z_i) = \cap_i \varphi(Z_i)$$

In particular, $\varphi(X)$ is closed in Y. But φ is dominant, hence $\varphi(X) = Y$.

We now claim that the conditions (i), (ii) and (iii) of definition 5 are satisfied by (Y, φ).

(i) If y is a closed point of Y, then $\varphi^{-1}(y)$ contains at least one orbit since φ is surjective. If $Z_1, Z_2 \subset \varphi^{-1}(y)$ are two orbits, then

$$\varphi(Z_1 \cap Z_2) = \varphi(Z_1) \cap \varphi(Z_2) = \{y\},$$

since Z_1 and Z_2 are closed by assumption. Therefore $Z_1 \cap Z_2 \neq \phi$, i.e., $Z_1 = Z_2$.

(ii) If U is an invariant open subset of X, $Z = X \setminus U$ is closed and invariant. Therefore $\varphi(Z)$ is closed in Y. If V is its open complement, then $\varphi^{-1}(V) \subset U$. On the other hand, the orbit of any closed point of U is a closed invariant subset Z' of X such that $Z \cap Z' = \phi$. Therefore $\varphi(Z') \cap \varphi(Z) = \phi$ and Z' is contained in $\varphi^{-1}(V)$.

(iii) If $V = D(f)$ is an affine open subset of Y, $\Gamma(V, \mathcal{O}_Y) = R_f^G$ is the ring of invariants in $\Gamma(\varphi^{-1} V, \mathcal{O}_X) = R_f = R \otimes_{R^G} R_f^G$ by lemma 1. The same is true for any open subset V of Y by the basic properties of sheaves.

This concludes the proof of the theorem.

REMARK. If the orbits of closed points of X are not assumed closed, the following is still true:

(1) If x and x' are closed points of X then $\varphi(x) = \varphi(x')$ if and only if $\overline{0(x)} \cap \overline{0(x')} \neq \phi$.

(2) For each closed point y of Y, $\varphi^{-1}(y)$ contains a unique closed orbit.

(3) There is an invariant open set $X_S \subset X$ such that a closed point x of X is in X_S if and only if the orbit $0(x)$ is closed and the stabilizer $S(x)$ is of minimal dimension. Then $Y_S = \varphi(X_S)$ is open in Y and $(Y_S, \varphi|X_S)$ is a geometric quotient of X_S by G.

In fact, (1) may be proved as (i) above. To verify (2) note that a minimal closed invariant subset of $\varphi^{-1}(y)$ is an orbit (LMG, 1.8); uniqueness follows from (1). For a proof of (3), consider the invariant open set X^{reg} which consists of the points whose stabilizers has minimal dimension (GIT, 0.9). Then $\varphi(X \setminus X^{\text{reg}})$ is closed in Y and its complement is Y_S, $X_S = \varphi^{-1}(Y_S)$. The rest of the proof is as in theorem 1.

Finally, we note that a slight generalization of the proof given above shows that (Y, φ) is a quotient of X by G even if the orbits are not closed (GIT, theorem 1.1).

2. n ordered points on a line

The moduli problem has led us to consider quotients of schemes by groups. The affine case was studied in chapter 1. In this chapter we shall examine the quotient of a projective variety by means of an elementary example.

The projective group $PGL(2) = GL(2)/\boldsymbol{G}_m$ (over k) acts canonically on the projective line $\boldsymbol{P}^1 = P^1_k$, hence on the product $(\boldsymbol{P}^1)^n$ for each integer n. To construct a quotient of $(\boldsymbol{P}^1)^n$ under this action, we might proceed as follows: find invariant affine open sets $U_i \subset (\boldsymbol{P}^1)^n$, find quotients V_i of the U_i by $PGL(2)$ using results of chapter 1, and join the V_i together along the quotients of the $U_i \cap U_j$. In this case, however, there is a more direct method. We assume $n \geqq 3$.

Closed points of $(\boldsymbol{P}^1)^n$ are n-tuples $(x_1, \cdots, x_n)$ of closed points of $\boldsymbol{P}^1$. Let U_{123} be the invariant open subset of $(\boldsymbol{P}^1)^n$ whose closed points are those with x_1, x_2, x_3 distinct. Then the orbit of any closed point $(x_1, \cdots, x_n)$ of U_{123} contains a unique closed point of the form $(0, 1, \infty, y_1, \cdots, y_{n-3})$. It follows that the action $\sigma : PGL(2) \times (\boldsymbol{P}^1)^n \to (\boldsymbol{P}^1)^n$ induces an isomorphism

$$PGL(2) \times (\boldsymbol{P}^1)^{n-3} \xrightarrow{\sim} U_{123}$$

mapping a closed point $(g, y_1, \cdots, y_{n-3}) \in PGL(2) \times (\boldsymbol{P}^1)^{n-3}$ onto $\sigma(g, 0, 1, \infty, y_1, \cdots, y_{n-3})$.

If $PGL(2)$ acts on itself by left translations and trivially on $(\boldsymbol{P}^1)^{n-3}$, then the isomorphism is $PGL(2)$-linear, i.e., U_{123} is a trivial principal $PGL(2)$-bundle over $(\boldsymbol{P}^1)^{n-3}$.

For each triple (i, j, k) with $1 \leqq i, j, k \leqq n$ distinct, let U_{ijk} denote the invariant open set of $(\boldsymbol{P}^1)^n$ whose closed points are those with x_1, x_j, x_k distinct. Then we find as above that U_{ijk} is a trivial $PGL(2)$-bundle over a scheme P_{ijk} isomorphic to $(\boldsymbol{P}^1)^{n-3}$.

Given two triples (i, j, k) and (i', j', k') the intersection

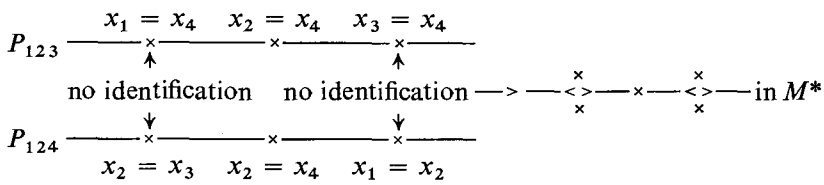
$$U' = U_{ijk} \cap U_{i'j'k'}$$

is an invariant open set. Hence its image U_1 in P_{ijk} is canonically isomorphic to its image U_2 in $P_{i'j'k'}$. Indeed, a morphism $U_1 \to U_2$ can be defined by composing the projection $U' \to U_2$ with a section $U_1 \to U'$. Joining the P_{ijk} together by these natural isomorphisms we obtain a scheme M^*.

The union $U^* = \bigcup_{1 \geqq i > j > k \geqq n} U_{ijk}$ is an invariant open subset of $(\boldsymbol{P}^1)^n$, with closed points $(x_1, \cdots, x_n)$ such that at least three of the x_i are distinct. It is clear that there is a natural morphism $\tau : U^* \to M^*$ making U^* a principal fibre bundle over M^* with structure group $PGL(2)$.

Thus it seems that M^* is a reasonable (partial) solution of the quotient problem for $(\boldsymbol{P}^1)^n$. In fact it is easy to see that (M^*, τ) is a geometric quotient of U^*. But the trouble is that M^* is *not separated* if $n > 3$, hence it cannot be quasi-projective.

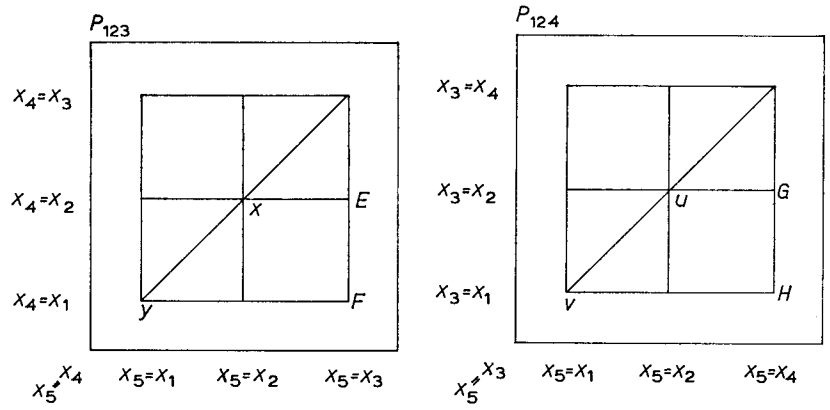
EXAMPLE A: $n = 4$. Let us identify P_{123} with $\boldsymbol{P}^1$ so that $\tau(0, 1, \infty, y)$ corresponds to y. If P_{134} is identified with $\boldsymbol{P}^1$ by $\tau(0, y', \infty, 1) \leftrightarrow y'$, then the image of the diagonal map $P_{123} \cap P_{134} \to P_{123} \times P_{134} \xrightarrow{\sim} (\boldsymbol{P}^1)^2$ is given by $yy' = 1$, $y \neq 0$, $y' \neq 0$. Since it is not closed M^* is not separated. In fact, if y specializes to 0, then y' specializes to ∞, but the points with $x_1 = x_4$ in U_{123} are different from the points with $x_2 = x_3$ in P_{134}. Hence we get the following picture:



It is interesting to not e that permuting (x_1, x_2) with (x_3, x_4) leaves $P_{123} \cup P_{134}$ invariant interchanging the components of the double points.

Adding P_{124} and P_{234} brings forth another doubled point, that corresponding to points of U^* with either $x_2 = x_4$ or $x_1 = x_3$.

EXAMPLE B. $n = 5$. Let us consider P_{123} and P_{124}, both isomorphic to $\boldsymbol{P}^1 \times \boldsymbol{P}^1$:



The intersection of P_{123} and P_{124} on M^* defines an isomorphism of the open subsets $P_{123} \setminus (E \cup F)$ and $P_{124} \setminus (G \cup H)$. Let $U \subset P_{123} \times P_{124}$ be the graph of this isomorphism. The complement of U in its closure P consists of two pairs of intersecting lines

$$E \times \{v\} \cup \{x\} \times H \text{ and } F \times \{u\} \cup \{y\} \times G$$

Hence $P_{123} \cup P_{124}$ is not separated as a subscheme of M^*. However: $P_{123} \setminus \{x, y\}$ and $P_{124} \setminus \{u, v\}$ are mapped isomorphically onto open subsets of P. Therefore, after omitting x, y, u, v there remains a separated subscheme which is isomorphic to $P \setminus \{(x, v), (y, u)\}$.

In the general case, to obtain a separated quotient, we must leave out part of U^*. This is quite trivial if no restriction is imposed. But if the quotient should be complete, we must be careful not to omit too many points.

PROBLEM. Does there exist an open subset $U \subset U^*$ invariant under the action of $PGL(2)$ and under permutations of the coordinates such that $\tau(U)$ is separated and complete?

Considering first the case $n = 4$, we see by example A that no such U exists. There are open subsets invariant under $PGL(2)$ such that the quotient is separated and complete, but no such set is invariant under permutations of the coordinates, since the components of the doubled points are interchanged by permutations. In fact, I conjecture that there is no solution for even integers n.

On the other hand, if n is odd, there is always a remarkable solution. Indeed, if $n = 5$, it is not hard to see that the quotient is separated and complete after the omission of the points with some three coordinates coinciding (such as x, y, u, v in example B). In general, if $n = 2e+1$, we define U as the open set whose closed points are such that no point of $\boldsymbol{P}^1$ occurs $e+1$ times among the coordinates.

To prove that $\tau(U)$ is separated and complete, we recall the valuative criterion:

PROPOSITION 1. *Let X be an algebraic k-scheme. If X is separated (resp. complete), then the canonical map*

$$\mathrm{Hom}_k(\mathrm{Spec}(A), X) \to \mathrm{Hom}_k(\mathrm{Spec}(K), X)$$

is injective (resp. bijective) for each k-algebra A which is a valuation ring with fraction field K.

Conversely, if the map

$$\mathrm{Hom}_k(\mathrm{Spec}k[[t]], X) \to \mathrm{Hom}_k(\mathrm{Spec}(k((t))), X)$$

is injective (resp. bijective), then X is separated (resp. complete).

PROPOSITION 2. *$M = \tau(U)$ is separated and complete.*

PROOF. To show that M is separated, let $R = k[[t]]$, $K = k((t))$, and consider two morphisms $\mathrm{Spec}(R) \to M$ with the same restriction to $\mathrm{Spec}(K)$. We claim that the two morphisms are equal. Using local sections of τ it is possible to lift these morphisms to R-valued points of U. By a suitable choice of a point $\infty \in \boldsymbol{P}^1$, we may assume that they factor through $(\boldsymbol{A}^1)^n \subset (\boldsymbol{P}^1)^n$, hence are of the form $x = (x_1(t), \cdots, x_n(t))$ and $y = (y_1(t), \cdots, y_n(t))$ with $x_i(t),\ y_i(t) \in R$ $(1 \leqq i \leqq n)$. Regarded as K-valued points, x and y have the same image in M. Hence there is a K-valued point σ of $PGL(2)$ such that $y_K = \sigma \cdot x_K$. In other words, there are elements $a(t), b(t), c(t), d(t)$ of $k((t))$ such that

$$y_i(t) = \frac{a(t)x_i(t)+b(t)}{c(t)x_i(t)+d(t)} \qquad (1 \leqq i \leqq n).$$

Clearly, we may assume that $a(t), b(t), c(t), d(t)$ are in $k[[t]]$ with constant terms $a(0), b(0), c(0), d(0)$ not all equal to 0.

Now, if $a(0) \cdot d(0) - b(0) \cdot c(0) \neq 0$, then

$$\Delta(t) = a(t)d(t) - b(t)c(t)$$

is invertible in R, and therefore σ is actually an R-valued point of $PGL(2)$. But then $\tau(x) = \tau(y)$ on $\mathrm{Spec}(R)$ as was claimed.

On the other hand, if $\Delta(0) = 0$, but $c(0) \neq 0$ or $d(0) \neq 0$, then for each i we have either

$$x_i(0) = -\frac{d(0)}{c(0)} \text{ or } y_i(0) = \frac{a(0)}{c(0)} = \frac{b(0)}{d(0)}$$

One of these conditions holds for at least $e+1 = (n+1)/2$ integers i. But this is impossible, since $(x_1(0), \cdots, x_n(0))$ and $(y_1(0), \cdots, y_n(0))$ are k-valued points of U.

Finally, if $c(0) = d(0) = 0$, then $a(0) \neq 0$, and

$$x_i(0) = -\frac{b(0)}{a(0)}$$

for each i contradicting the assumption.

To prove the completeness of M, we show that each morphism $\mathrm{Spec}(K) \to M$ may be extended to $\mathrm{Spec}(R)$, where $R = k[[t]]$ and $K = k((t))$ as above.

Any K-valued point of M may be lifted to a K-valued point of U: $(x_1(t), \cdots, x_n(t))$ with $x_i(t) \in K \cup \{\infty\}$ $(1 \leqq i \leqq n)$. Hence it will suffice to show that there is a K-valued point σ of $PGL(2)$ such that $(\sigma x_1(t), \cdots, \sigma x_n(t))$ is an R-valued point of U. In any case, each $x_i(t)$ defines a unique morphism $\mathrm{Spec}(R) \to \boldsymbol{P}^1$ since $\boldsymbol{P}^1$ is separated and complete (proposition 1). The restriction of this morphism to the closed point of $\mathrm{Spec}(R)$ is given by $x_i(0) \in k \cup \{\infty\}$. If $(x_1(0), \cdots, x_n(0))$ is a k-valued point of U, $(x_1(t), \cdots, x_n(t))$ is an R-valued point of U and there is nothing to prove.

In general, we proceed by induction on the least integer p such that no $e+1$ of the morphisms $\mathrm{Spec}(R/R \cdot t^{p+1}) \to \boldsymbol{P}^1$ defined by the $x_i(t)$ $(1 \leqq i \leqq n)$ are equal. We may assume that none of the $x_i(0)$ are infinite by a suitable choice of coordinates on $\boldsymbol{P}^1$. Writing $x_i(t) = \sum_{j=0}^{\infty} a_{ji} t^j$, we see that the condition means that no $e+1$ of the polynomials

$$\sum_{j=0}^{p} a_{ji} t^j$$

are equal. Incidentally, this shows that p is finite.

If $p = 0$, then no $e+1$ of the points $x_i(0)$ coincide, and $(x_1(t), \cdots, x_n(t))$ is an R-valued point of U as was seen above.

In case $p > 0$, there is a unique polynomial $\sum_{j=0}^{p-1} a_{ji} t^j$ occurring more than e times. We may assume for convenience that these polynomials have indices $1 \leqq i \leqq r$ with $e+1 \leqq r \leqq n$. Let σ be the K-valued point of $PGL(2)$ defined by

$$\sigma = \begin{pmatrix} 1 & -a \\ 0 & t \end{pmatrix}$$

or

$$x(t) \mapsto \sigma x(t) = \frac{x(t)-a}{t}$$

where $a \in k$ is the common value of the constants $x_i(0) = a_{0i}$ $(1 \leqq i \leqq r)$. Then it is easy to verify that $(\sigma x_1(t), \cdots, \sigma x_n(t))$ satisfies the induction assumption with p replaced by $p-1$. This completes the proof.

This result is interesting as such, but we can prove more:

THEOREM 1. *M is projective.*

PROOF. The general method of constructing ample invertible sheaves on a quotient of a scheme X is to search for ample invertible sheaves on X such that the action of the group extends to the sheaf and to apply the theory of descent. In our case, however, there is a more elementary way of producing invertible sheaves on M.

For each pair (i,j) of integers $1 \leqq i,j \leqq n$ with $i \neq j$, let D_{ij} denote the closed subset of U defined by $x_i = x_j$. Since D_{ij} is invariant under the action of $PGL(2)$, $\Delta_{ij} = \tau(D_{ij})$ is closed in M and $D_{ij} = \tau^{-1}(\Delta_{ij})$. This is easily proved by using local sections of τ. Furthermore, Δ_{ij} is irreducible of codimension one, i.e., a prime divisor on M.

Let $L_{ij} = \mathcal{O}_M(\Delta_{ij})$ be the invertible sub-$\mathcal{O}_M$-Module of the sheaf of rational functions on M whose sections are regular everwhere except for at most a simple pole at Δ_{ij}. In other words, if $f \in \Gamma(V, \mathcal{O}_M)$ is a local equation of Δ_{ij}, then the sections of L_{ij} over V are the multiples of f^{-1}. We denote by $\delta_{ij} \in \Gamma(M, L_{ij})$ the canonical section 1. To find relations among the L_{ij} we embed $\mathrm{Pic}(M)$ into $\mathrm{Pic}(U)$, which is isomorphic to $\mathrm{Pic}((\boldsymbol{P}^1)^n)$, since $(\boldsymbol{P}^1)^n \setminus U$ is of codimension $i = (n-1)/2 \geqq 2$ for $n \geqq 5$ (the case $n = 3$ is trivial).

LEMMA 1. *$\tau^* : \mathrm{Pic}(M) \to \mathrm{Pic}(U)$ is injective.*

PROOF. Let D be a divisor on M such that $\tau^{-1}(D)$ is linearly equivalent to 0, i.e., $\tau^{-1}(D) = \mathrm{div}(f)$ for some rational function f on U, or, what amounts to the same, on $(\boldsymbol{P}^1)^n$. Then for each closed point σ of $PGL(2)$, $\mathrm{div}(\sigma(f)) = \mathrm{div}(f)$. This implies that $\sigma(f) = \chi(\sigma) \cdot f$ for some constant $\chi(\sigma) \in k^*$, since $(\boldsymbol{P}^1)^n$ is complete. But then χ is a character of $PGL(2)$. [In fact, the action of $PGL(2)$ on the generic fibre $Z = \tau^{-1}(y)$ of τ induces a homomorphism

$$\begin{aligned} \hat{\sigma} : \Gamma(Z, \mathcal{O}_Z) &\to \Gamma(PGL(2) \times Z, \mathcal{O}_{PGL(2)\times Z}) \\ &= \Gamma(PGL(2), \mathcal{O}_{PGL(1)}) \otimes_k \Gamma(Z, \mathcal{O}_Z). \end{aligned}$$

If $\hat{\sigma}(f) = \sum \chi_i \otimes f_i$ where $f_i \in \Gamma(Z, \mathcal{O}_Z)$ $(1 \leqq i \leqq r)$ are linearly independent with $f_1 = f$ and $\chi_i \in \Gamma(PGL(2)\ \mathcal{O}_{PGL(2)})$ $(1 \leqq i \leqq r)$, then it is readily seen that $\chi_i = 0$ for $i > 1$ and $\chi_1 = \chi$ is an invertible section of $\mathcal{O}_{PGL(2)}$ defining a group homomorphism $PGL(2) \to \boldsymbol{G}_m]$.

But $PGL(2)$ has no non-trivial characters, since it coincides with its commutator subgroup (LAG, 10.8(2)). Therefore $\chi = 1$ and f is invariant under $PGL(2)$. Again, using local sections of τ, it is shown that $f = g \circ \tau$ for some rational function g on M and $D = \operatorname{div}(g)$.

There remains to study the structure of $\operatorname{Pic}((\boldsymbol{P}^1)^n)$ and the image of $\operatorname{Pic}(M)$ in $\operatorname{Pic}((\boldsymbol{P}^1)^n)$. It is clear that $\tau^*(L_{ij}) = \mathcal{O}_U(D_{ij})$. On the other hand, considering the rational function

$$\frac{x_0 y_1 - x_1 y_0}{x_0 y_0}$$

on $\boldsymbol{P}^1 \times \boldsymbol{P}^1$ with bihomogeneous coordinates $(x_0, x_1; y_0, y_1)$, we find that the diagonal D of $\boldsymbol{P}^1 \times \boldsymbol{P}^1$ is linearly equivalent to the divisor $\boldsymbol{P}^1 \times \{0\} + \{0\} \times P^1$, or, in terms of invertible sheaves,

$$\mathcal{O}(D) \simeq p_1^*(\mathcal{O}(1)) \otimes p_2^*(\mathcal{O}(1))$$

where $p_1, p_2 : \boldsymbol{P}^1 \times \boldsymbol{P}^1 \to \boldsymbol{P}^1$ are the projections.

Hence $L_{ij} = L_{ji}$ corresponds to $p_i^*(\mathcal{O}(1)) \otimes p_j^*(\mathcal{O}(1))$ on $(\boldsymbol{P}^1)^n$. It follows that

$$L_{ij} \otimes L_{kl} \simeq L_{ik} \otimes L_{jl}$$

for each quadruple (i, j, k, l) with $i \neq j$, $k \neq l$, $i \neq k$, $j \neq l$. In fact, $\Delta_{ij} + \Delta_{kl} - \Delta_{ik} - \Delta_{jl}$ is the divisor of the rational function on M defined by the invariant crossratio of the four coordinates (x_i, x_j, x_k, x_l) of a point of U.

It may be shown that $p_1^*(\mathcal{O}(1)), \cdots, p_n^*(\mathcal{O}(1))$ are free generators of $\operatorname{Pic}((\boldsymbol{P}^1)^n)$ and the image of $\operatorname{Pic}(M)$ is a subgroup of index 2. But this is not necessary for our purposes.

For any i between 1 and n, $p_i^*(\mathcal{O}(2))$ is in the image of $\operatorname{Pic}(M)$, namely, it corresponds to

$$L_{ii} = L_{ik} \otimes L_{il} \otimes L_{kl}^{-1}$$

for some k, l with i, k, l distinct. By lemma 1, L_{ii} is independent of k and l. *We claim that* $L = L_{11} \otimes \cdots \otimes L_{nn}$ *is ample.*

The proof is based on the following observation:

$$L \simeq L_{i_1 j_1} \otimes \cdots \otimes L_{i_n j_n}$$

if each integer between 1 and n occurs exactly twice in

$$(i_1, \cdots, i_n, j_1, \cdots, j_n),$$

and further, if $i_k \neq j_k$ for $1 \leqq k \leqq n$, then there is a section

$$\delta_{i_1 j_1} \otimes \cdots \otimes \delta_{i_n j_n} \in \Gamma(M, L_{i_1 j_1} \otimes \cdots \otimes L_{i_n j_n})$$

having $\Delta_{i_1 j_1} \cup \cdots \cup \Delta_{i_n j_n}$ as its set of zeros.

LEMMA 2. *For each closed point $(x_1, \cdots, x_n)$ of U there is a sequence $(i_1, \cdots, i_n, j_1, \cdots, j_n)$ where each integer between 1 and n occurs exactly twice such that $x_{i_k} \neq x_{j_k}$ for $1 \leqq k \leqq n$ and $(i_1, i_2, i_3) = (j_3, j_1, j_2)$.*

PROOF. By induction on $l = (n-1)/2$. The case $l = 1$ is trivial. If $l > 1$, we choose i_n and j_n such that x_{i_n} and x_{j_n} are two distinct points occurring with maximal multiplicity in $(x_1, \cdots, x_n)$. Since there are at most two points with multiplicity l, each of the remaining points occurs at most $l-1$ times. If one of the points x_{i_n}, x_{j_n} occurs with multiplicity one, then either all of the points x_i are distinct or exactly one of them has multiplicity greater than one (but less than $l+1$). In either case at least three distinct points remain after omitting x_{i_n} and x_{j_n}. Hence, taking $i_{n-1} = i_n, j_{n-1} = j_n$, we are reduced to the case $l-1$.

Let $(i_1, \cdots, i_n, j_1, \cdots, j_n)$ be as in lemma 2 and denote by $M_{i_1 \cdots i_n, j_1 \cdots j_n}$ the open subset of M where $\delta_{i_1 j_1} \otimes \cdots \otimes \delta_{i_n j_n}$ does not vanish, i.e.,

$$M_{i_1 \cdots i_n j_1 \cdots j_n} = M \setminus (\Delta_{i_1 j_1} \cup \cdots \cup \Delta_{i_n j_n}).$$

These sets form an open covering of M by Lemma 2. Hence *it suffices to show that they are affine* (EGA II, 4.5.2, last statement).

Now $\tau^{-1}(M_{i_1 \cdots i_n j_1 \cdots j_n})$ is contained in $U_{i_1 i_2 i_3}$.

Therefore $M_{i_1 \cdots i_n j_1 \cdots j_n}$ is a subset of $P_{i_1 i_2 i_3}$, which is isomorphic to $(\boldsymbol{P}^1)^{n-3}$. Furthermore, the complement of $M_{i_1 \cdots i_n j_1 \cdots j_n}$ in $P_{i_1 i_2 i_3}$ is the set of zeros of a section of an invertible sheaf L' such that $\tau^* L'$ is isomorphic to $p_1^*(\mathcal{O}(2)) \otimes \cdots \otimes p_n^*(\mathcal{O}(2))$ restricted to $U_{i_1 i_2 i_3}$. In fact,

$$L' \simeq \iota^*(p_1^*(\mathcal{O}(2)) \otimes \cdots \otimes p_n^*(\mathcal{O}(2)))$$

where ι is a section of τ over $P_{i_1 i_2 i_3}$. Hence L' corresponds to

$$p_1^*(\mathcal{O}(2)) \otimes \cdots \otimes p_{n-3}^*(\mathcal{O}(2))$$

under the isomorphism $P_{i_1 i_2 i_3} \to (\boldsymbol{P}^1)^{n-3}$. But

$$p_1^*(\mathcal{O}(1)) \otimes \cdots \otimes p_{n-3}^*(\mathcal{O}(1))$$

is very ample (it defines the Segre morphism $(\boldsymbol{P}^1)^{n-3} \to \boldsymbol{P}^{2^{n-3}-1}$, cf. EGA II, 4.3). Therefore L' is ample. Thus we conclude that $M_{i_1 \cdots i_n j_1 \cdots j_n}$ is affine (EGA II, 5.5.7). This ends the proof of theorem 1.

To finish the chapter we shall discuss quotients of projective schemes more generally but without giving proofs. Let G be a reductive group

(definition I.6) acting on a projective k-scheme X, and let L be an ample invertible sheaf on X to which the action of G may be lifted (in the sense of GIT, Ch. 1, § 3). For example, if E is a finite-dimensional k-vector space on which G acts, and X is a closed invariant subscheme of $P = \boldsymbol{P}(E)$ then L might be $\mathcal{O}_P(1)$ restricted to X. Conversely, if L is ample, then for some integer n, X embeds in $\boldsymbol{P}\,[\Gamma(X, L^{\otimes n})]$, on which G acts canonically.

THEOREM 2. *Let G, X, and L be as above. Then there are two canonical invariant open subsets of X: $X_S \subset X_{SS} \subset X$ such that*

(i) *a quotient (Y, π) of X_{SS} by G exists and is a projective scheme.*

(ii) *there is an open subset Y_0 of Y such that $(Y_0, \pi/X_S)$ is a geometric quotient of X_S.*

Moreover:

a) $X_S = \pi^{-1}(Y_0)$

b) *if x and y are closed points of X_{SS}, then $\pi(x) = \pi(y)$ if and only if $\overline{O(x)} \cap \overline{O(y)} \cap X_{SS} \neq \phi$.*

c) *for each closed point y of Y, $\pi^{-1}(y)$ contains a unique orbit closed in X_{SS}.*

d) *a closed point x of X_{SS} is in X_S if and only if $O(x)$ is closed in X_{SS} and the stabilizer $S(x)$ of x has minimal dimension.*

The points of X_S are called *stable* and those of X_{SS} *semistable.* For the definition X_S and X_{SS} as well as the proof of this theorem we refer to GIT, Ch. 1, § 4. The basic idea, however, is to define Y to be $\mathrm{Proj}(R^G)$, where $R = \sum \Gamma(X, L^n)$ is the homogeneous coordinate ring of X.

There is an important numerical criterion for finding X_S and X_{SS} (GIT, Ch. 2, § 1). Namely, if x is a closed point of X, then for each 1-parameter sub-group λ of G, i.e., for each homomorphism $\lambda : \boldsymbol{G}_m \to G$, the morphism $\boldsymbol{G}_m = \mathrm{Spec}(k[\alpha, \alpha^{-1}]) \to X$ defined by $\alpha \mapsto \lambda(\alpha) \cdot x$ extends uniquely to a morphism $f : \boldsymbol{A}^1 = \mathrm{Spec}(k[\alpha]) \to X$, since X is separated and complete and the local ring of 0 in $\boldsymbol{A}^1$ is a valuation ring (proposition 1). Then $z = f(0)$ is fixed under the action of $\boldsymbol{G}_m$ induced by λ, and therefore $\boldsymbol{G}_m$ acts on the 1-dimensional fiber $L \otimes k(z)$. But such an action is given by a character χ of $\boldsymbol{G}_m$; hence there is an integer r such that $\lambda(\alpha) \cdot v = \alpha^r \cdot v$ for each $v \in L \otimes k(z)$. Then the point x is stable if $r < 0$, and semi-stable if $r \leqq 0$, for each 1-parameter subgroup λ of G.

To see how this criterion works in a concrete example, let us return to the group $PGL(2)$ acting on $X = (\boldsymbol{P}^1)^n$. ($PGL(2)$ is simple, hence reductive if $\mathrm{char}(k) = 0$.)

To find an ample invertible sheaf to which the action of $PGL(2)$ extends, we first write out explicitly the action of $PGL(2)$ on $\boldsymbol{P}^1$ (cf. GIT, p. 33). If $X_0, X_1 \in \Gamma(\boldsymbol{P}^1, \mathcal{O}(1))$ are the homogeneous coordinates of $\boldsymbol{P}^1$ then

$(a_{ij}) \in GL(2)$ acts on $\Gamma(\boldsymbol{P}^1, \mathcal{O}(1))$ (on the right) by $X_i \to \sum a_{ij} X_j$. This defines an automorphism $\boldsymbol{P}^1 \to \boldsymbol{P}^1$ which depends only on the class of (a_{ij}) in $PGL(2)$. Unfortunately, there is no action of $PGL(2)$ on $\Gamma(\boldsymbol{P}^1, \mathcal{O}(1))$ compatible with the action on $\boldsymbol{P}^1$. However, the operation

$$X_i \otimes X_j \to \frac{\sum a_{ik} a_{jl} X_k \otimes X_l}{\det (a_{ij})}$$

of $GL(2)$ on $\Gamma(\boldsymbol{P}^1, \mathcal{O}(2))$ factors through $PGL(2)$. Hence the action of $PGL(2)$ lifts to $\mathcal{O}(2)$.

Let $\lambda : \boldsymbol{G}_m \to PGL(2)$ be the homomorphism such that $\lambda(\alpha)$ is the class of

$$\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}$$

in $PGL(2)$ for $\alpha \in k^*$. The fixed points of $\boldsymbol{P}^1$ under the action of $\boldsymbol{G}_m$ induced by λ are 0 and ∞, defined by $X_1(0) = 0$, $X_0(\infty) = 0$. If $x \in \boldsymbol{P}^1$ is different from 0 and ∞, then $\lambda(\alpha) \cdot x$ specializes to 0 as $\alpha \to 0$ and to ∞ as $\alpha \to \infty$. Moreover, the action of $\boldsymbol{G}_m$ on the fibers of $\mathcal{O}(2)$ at 0 and ∞ is given by multiplication with α^{-1} and α, respectively. To see this, it suffices to consider the behaviour of $X_0 \otimes X_0$ and $X_1 \otimes X_1$.

Now, each non-trivial 1-parameter subgroup λ' of $PGL(2)$ is conjugate to λ^m for some integer $m > 0$. Hence there are exactly two points a, b of $\boldsymbol{P}^1$ fixed under the action of $\boldsymbol{G}_m$ induced by λ'. Besides, if $x \neq a, b$ is a point of $\boldsymbol{P}^1$, $\lambda'(\alpha) \cdot x$ specializes to one of these points, say a, as $\alpha \to 0$, and so $\lambda'(\alpha) \cdot x$ specializes to b as $\alpha \to \infty$. Finally, the action of $\boldsymbol{G}_m$ on the fibers of $\mathcal{O}(2)$ at a and b is given by multiplication with α^{-m} and α^m respectively.

Returning to $(\boldsymbol{P}^1)^n$ we find that the action of $PGL(2)$ lifts to the ample invertible sheaf $L = p_1^*(\mathcal{O}(2)) \otimes \cdots \otimes p_n^*(\mathcal{O}(2))$. Let $x = (x_1, \cdots, x_n)$ be a closed point of $(\boldsymbol{P}^1)^n$ and let a, b denote the fixed points of a 1-parameter subgroup λ' of $PGL(1)$ as above. Permuting the indices if necessary, we assume that $x_i = b$ for $1 \leqq i \leqq r$ and $x_i \neq b$ for $r+1 \leqq i \leqq n$. It follows that $\lambda'(\alpha) \cdot x$ specializes to

$$z = (\overbrace{b, \cdots, b}^{r}, \overbrace{a, \cdots, a}^{n-r})$$

as $\alpha \to 0$. Considering each factor of L separately we find that the action of $\boldsymbol{G}_m$ on the fiber $L \otimes k(z)$ induced by λ' is given by multiplication with $\alpha^{m(2r-n)}$. As b may be any point of $\boldsymbol{P}^1$, we conclude:

A closed point $(x_1, \cdots, x_n)$ of $(\boldsymbol{P}^1)^n$ is stable (semistable) if and only if no point of $\boldsymbol{P}^1$ occurs with multiplicity $\geqq n/2$ ($> n/2$) in $(x_1, \cdots, x_r)$.

If n is odd, the set of stable points $(\boldsymbol{P}^1)^n_S$ is the same as the set of semi-

stable points $(\boldsymbol{P}^1)^n_{SS}$, and both coincide with the set U above. If n is even, $(\boldsymbol{P}^1)^n_S$ is a proper subset of $(\boldsymbol{P}^1)^n_{SS}$. Hence the quotient of $(\boldsymbol{P}^1)^n_S$ is not complete.

3. Elliptic curves

Let us consider an algebraic curve X over k, i.e., a reduced, irreducible, and separated algebraic k-scheme of dimension 1. We recall that X is non-singular if and only if the sheaf of differentials $\Omega_{X/k}$ is a locally free $\mathcal{O}_X$-Module of rank 1 or equivalently, if and only if the local ring $\mathcal{O}_x$ is a discrete valuation ring for each closed point x of X. In addition, if X is non-singular, x is a closed point of X, and f is an element of the maximal ideal m of $\mathcal{O}_x$, then f is a generator of m if and only if df is a local basis for $\Omega_{X/k}$ at x. It is also useful to note that a complete, non-singular algebraic curve is uniquely determined by its field of rational functions.

If X is complete and non-singular, then

$$g = \dim_k H^0(X, \Omega_{X/k})$$

is a finite integer, called the *genus* of X. An *elliptic curve* is a complete, non-singular algebraic curve of genus 1.

To examine elliptic curves in greater detail we have to know their cohomology.

PROPOSITION 1. *Let $\mathcal{D}$ be a divisor of degree n on an elliptic curve E over k.*

(i) *For $n > 0$, $\dim_k H^0(E, \mathcal{O}_E(\mathcal{D})) = n$ and $H^1(E, \mathcal{O}_E(\mathcal{D})) = 0$.*

(ii) *For $n < 0$, $H^0(E, \mathcal{O}_E(\mathcal{D})) = 0$ and $\dim_k H^1(E, \mathcal{O}_E(\mathcal{D})) = -n$.*

(iii) *For $n = 0$, $\dim_k H^0(E, \mathcal{O}_E(\mathcal{D})) = \dim_k H^1(E, \mathcal{O}_E(\mathcal{D})) = 1$ if $\mathcal{D}$ is linearly equivalent to 0, and $H^0(E, \mathcal{O}_E(\mathcal{D})) = H^1(E, \mathcal{O}_E(\mathcal{D})) = 0$ otherwise.*

Furthermore, $H^i(E, \mathcal{O}_E(\mathcal{D})) = 0$ for $i > 2$.

The proposition follows from the Riemann-Roch formula

$$\dim_k H^0(E, \mathcal{O}_E(\mathcal{D})) - \dim_k H^1(E, \mathcal{O}_E(\mathcal{D})) = n$$

(Serre, Groupes algébriques et corps de classes, Théorème 1, p. 21) and Serre duality

$$\dim_k H^0(E, \mathcal{O}_E(\mathcal{D})) = \dim_k H^1(E, \mathcal{O}_E(K - \mathcal{D}))$$

(loc.cit., Théorème 2, p. 26) noting that the canonical class K is 0. Indeed, the degree of K is 0 (Loc. cit., p. 27) and

$$\dim_k H^0(E, \mathcal{O}_E(K)) = \dim_k H^0(E, \Omega_{E/k}) = 1$$

by assumption. Hence $K = \mathrm{div}(f)$ for some rational function $f \in H^0(E, \mathcal{O}_E(K))$.

Now let E be an elliptic curve. We fix a closed point 0 of E. The reason for this notation is the following:

PROPOSITION 2. *There is a unique abelian group structure on the set of closed points E_k of E such that the map*

$$x \mapsto \text{the class of } \mathcal{O}_E((x)-(0)),$$

where (x) is the divisor associated with x, is a group homomorphism from E_k to the Picard group $\mathrm{Pic}(E)$ *of E.*

PROOF. It is enough to show that the map

$$x \mapsto \text{the class of } (x)-(0)$$

is a bijection from E_k to the set of linear equivalence classes of divisors of degree 0. But if $\mathcal{D}$ is a divisor of degree 0 on E, then

$$\dim H^0(E, \mathcal{O}_E(\mathcal{D}+(0))) = 1$$

by proposition 1(i). Thus there is a unique principal divisor

$$\mathrm{div}(f) \geqq -\mathcal{D}-(0).$$

Then $\mathrm{div}(f)+\mathcal{D}+(0)$ is an effective divisor of degree 1, hence of the form (x) for some $x \in E_k$. Q.E.D.

Clearly, 0 is the neutral element of the group E_k.

REMARK. It may be shown that the group structure of E_k is induced by an algebraic group structure on E. It follows, in particular, that the full group of automorphisms of an elliptic curve is transitive. Hence the results are independent of the base point 0.

If A is the divisor associated with the point 0, the vector space $V = H^0(E, \mathcal{O}_E(2A))$ is 2-dimensional by proposition 1 (i). Hence there are non-constant rational functions in V, having necessarily a double pole at 0. Any such function f defines a morphism from $E-\{0\}$ to the affine line $\boldsymbol{A}^1$ over k, and this morphism has a unique extension π from E to the projective line $\boldsymbol{P}^1$ over k by proposition II.1. If f' is another non-constant function in V, and $\pi' : E \to \boldsymbol{P}^1$ is the corresponding morphism, there is a unique automorphism μ of $\boldsymbol{P}^1$ such that $\pi' = \mu \circ \pi$. In fact, since V/k is 1-dimensional, there is a unique pair $(\alpha, \beta) \in k^* \times k$ satisfying $f' = \alpha f + \beta$.

To find the fibers of π, let $\lambda \in k$ be a closed point of $\boldsymbol{A}^1 \subset \boldsymbol{P}^1$. Then $\pi^{-1}(\lambda)$ is the support of the divisor of zeros $\mathcal{D}$ of $f-\lambda$. Since the divisor of poles of $f-\lambda$ is of degree 2, $\mathcal{D} = (x)+(y)$ for some $x, y \in E_k$. But

then $x+y = 0$ by proposition 2. Hence the branch points of π are the points of order 2 in the group E_k. It is shown in the theory of abelian varieties that their number is four if $\mathrm{char}(k) \neq 2$.

More directly, this may be seen by calculating the order of $\mathrm{div}(df)$. If $x \in E_k$ is not a ramification point, then df_x is a generator of $(\Omega_{E/k})_x$, hence of order 0 at x. If $x \in E_k - \{0\}$ is a ramification point, then

$$f_x = f(x) + ut^2,$$

where t is a generator of the maximal ideal m_x of $\mathcal{O}_x$ and $u \in \mathcal{O}_x^*$ is a unit, and therefore

$$df_x = 2ut\,dt + t^2 du$$

is of order 1 if $2 \neq 0$ in k. Finally, if t generates $m_0 \subset \mathcal{O}_0$, we have

$$t^2 f_0 = u \in \mathcal{O}_0^*,$$
$$2tf_0 dt + t^2 df_0 = du,$$

so that df_0 is of order -3. Since the canonical divisor class on an elliptic curve is of degree 0, there are exactly 3 ramification points in addition to 0.

From now on we assume k of characteristic $\neq 2, 3$.

Let $a, b, c \in \boldsymbol{A}^1$ and ∞ be the images by π of the ramification points. By a projective transformation they may be normalized to

$$0, 1, \lambda, \infty,$$

where λ is a cross-ratio of the four points a, b, c, ∞. Since the order of the points a, b, c is not specified, there are, in general, 6 different normalisations $(0, 1, \mu, \infty)$, where μ appears in the following list:

$$\lambda,\ 1-\lambda,\ 1/\lambda,\ \frac{\lambda-1}{\lambda},\ \frac{\lambda}{\lambda-1},\ \frac{1}{1-\lambda}.$$

However, any rational function $j(\lambda)$ which has the same value at each of the above points defines an invariant of the curve E. To find such a function we note that there are three series of equivalent points which are left fixed by some non-trivial substitution:

$$\tfrac{1}{2},\ 2,\ -1,$$
$$0,\ 1,\ \infty,$$
$$-\omega,\ -\omega^2$$

where $\omega^2+\omega+1 = 0$ ($\omega \neq 1$ since $\mathrm{char}(k) \neq 3$). Hence $j(\lambda)$ must be ramified at these points. If we assume that

$$j(-\omega) = j(-\omega^2) = 0,$$
$$j(0) = j(1) = j(\infty) = \infty,$$

will be proportional to

$$\frac{(\lambda^2-\lambda+1)^3}{\lambda^2\cdot(\lambda-1)^2}.$$

On the other hand, this is seen to be invariant by direct substitution (or more elegantly, noting that the function in the brackets is invariant up to a multiplicative constant determined by a character of the symmetric group S_3, hence necessarily equal to ± 1). For reasons involving the omitted characteristics 2 and 3, j is normalized by

$$j(-1) = 12^3,$$

therefore we obtain

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

Thus we have constructed a map from the set of elliptic curves over k, up to isomorphism, to the set of closed points of $\boldsymbol{A}^1 = \mathrm{Spec}(k[j])$. To show that this map is bijective, we embed elliptic curves into the projective plane.

Let E be an elliptic curve over k and denote by A the divisor associated with a fixed base point 0 of E. Let $f \in H^0(E, \mathcal{O}_E(2A))$ be a rational function having a double pole at 0 as above.

By proposition 1

$$\dim_k H^0(E, \mathcal{O}_E(3A)) = 3$$

while

$$\dim_k H^0(E, \mathcal{O}_E(2A)) = 2.$$

Hence there is a rational function

$$g \in H^0(E, \mathcal{O}_E(3A))$$

with a triple pole at 0.

LEMMA 1. *For each integer $n \geqq 2$, the functions*

$$1, f, \cdots, f^k, g, fg, \cdots, f^l g,$$

where $k = [n/2]$, $l = [(n-3)/2]$, form a basis of $H^0(E, \mathcal{O}_E(nA))$.

PROOF. The orders of these functions at 0 are

$$0, -2, \cdots, -2k, -3, -5, \cdots, -2l-3,$$

respectively. Hence they are linearly independent. In the other hand, their number is $n = \dim H^0(E, \mathcal{O}_E(nA))$. Q.E.D.

Since $g^2 \in H^0(E, \mathcal{O}_E(6A))$, there are constants $a_i \in k$ $(1 \leqq i \leqq 6)$ such that

$$g^2 = a_1 fg + a_2 g + a_3 f^3 + a_4 f^2 + a_5 f + a_6.$$

Replacing g by $g-\frac{1}{2}a_1 f-\frac{1}{2}a_2$, we may assume $a_1 = a_2 = 0$. Since g^2 has a pole of order 6 at 0, we must have $a_3 \neq 0$. Therefore, replacing g by $a_3^{-\frac{1}{2}} g$ we obtain

$$g^2 = (f-a)(f-b)(f-c)$$

for some constants $a, b, c \in k$.

It is not hard to see that a, b, and c must be distinct. Indeed, if $a = b$, then $g/(f-a)$ has a simple pole at 0 and no other poles, since its square is $f-c$. But this is impossible by proposition 1.

Let $\boldsymbol{P}$ be a projective plane over k, with homogeneous coordinates $X, Y, Z \in H^0(\boldsymbol{P}, \mathcal{O}_{\boldsymbol{P}}(1))$. Since $1, f, g$ generate the invertible sheaf $\mathcal{O}_E(3A)$, there is a unique morphism $\varphi : E \to \boldsymbol{P}$ such that

$$\varphi^*(\mathcal{O}_{\boldsymbol{P}}(1)) \simeq \mathcal{O}_E(3A)$$

with $\varphi^*(X)$, $\varphi^*(Y)$, $\varphi^*(Z)$ corresponding to f, g, and 1.

PROPOSITION 3. *The morphism φ is an embedding of E onto the cubic curve C with homogeneous equation*

$$P(X, Y, Z) = Y^2Z-(X-aZ)(X-bZ)(X-cZ) = 0.$$

PROOF. It is clear that φ factors through C. If h is a rational function on E, and $\mathcal{D}$ is its divisor of poles ($\mathcal{D} \geqq 0$), then, for each integer $n > \deg(\mathcal{D})$, there is a rational function h' with $\operatorname{div}(h') \geqq \mathcal{D}-nA$ by proposition 1. This implies that hh' is defined on $E-\{0\}$. Thus any rational function on E is a quotient of two rational functions with poles at 0 only. But such functions are polynomials of f and g by lemma 1. Hence the rational function field of E is $k(f, g)$; in other words, φ defines a birational morphism from E to C. Therefore it is enough to show that C is non-singular. This follows from the fact that each singular cubic plane curve is rational, or by direct calculation as follows:

Let (x, y, z) be a point of C. If $y \neq 0$, then $P_Y(x, y, z) = 2yz \neq 0$ unless $z = 0$, in which case $x = 0$ and $P_Z(x, y, z) = y^2 \neq 0$. On the other hand, if $y = 0$, then $x = az, bz,$ or cz. Therefore $P_X(x, y, z) \neq 0$, since the constants a, b, c are distinct. Q.E.D.

It follows immediately that a, b, and c are the points of $\boldsymbol{A}^1$ over which the morphism $\pi : E \to \boldsymbol{P}^1$ defined by f is ramified.

REMARK. The assumption $\operatorname{char}(k) \neq 3$ has not been used in the proof of proposition 3.

COROLLARY. *The invariant function $j(\lambda)$ defines a bijection from the set of isomorphism classes of elliptic curves over k to the set of k-valued points of $\boldsymbol{A}^1_j$.*

PROOF. Since $\lambda \mapsto j(\lambda)$ is a surjective map from $k-\{0, 1\}$ to k, there is an elliptic curve for each $j \in k$, namely

$$P_\lambda(X, Y, Z) = Y^2Z - X(X-Z)(X-\lambda Z) = 0$$

for some $\lambda \in k-\{0, 1\}$ with $j = j(\lambda)$. Hence the map is surjective.

On the other hand, let E and E' be two elliptic curves with the same j. By proposition 3 we may assume that they are plane curves given by $P_\lambda(X, Y, Z) = 0$ and $P_{\lambda'}(X, Y, Z) = 0$. Since $j(\lambda)$ is of degree 6, $j(\lambda) = j(\lambda')$ implies that λ' is in the sequence

$$\lambda,\ 1-\lambda,\ 1/\lambda,\ \frac{\lambda-1}{\lambda},\ \frac{\lambda}{\lambda-1},\ \frac{1}{1-\lambda}.$$

Therefore E and E' are in fact projectively equivalent. Q.E.D.

Thus we have classified elliptic curves over k by the k-valued points of a scheme A_j^1. The question now arises: what is the role of the scheme structure of A_j^1? To answer this we introduce the notion of a family of elliptic curves in analogy with chapter 1.

DEFINITION 1. *A family of elliptic curves* over a k-variety S is a morphism of k-varieties $p : E \to S$ together with a section $0 : S \to E$ such that E is proper and smooth over S, and the closed fibers of p are elliptic curves.

REMARK. By the definition of an elliptic curve, the last condition implies that the closed fibers of p are non-singular. Therefore p is smooth if and only if it is flat.

To generalize the results of proposition 1 concerning the cohomology of elliptic curves for families of elliptic curves we need a base change theorem. We first introduce some notation.

If $p : E \to S$ is a morphism, we denote by E_s the fiber $p^{-1}(s)$ (considered as a subscheme of E) for each point s of S. For each $\mathcal{O}_E$-Module $\mathcal{F}$, $\mathcal{F} \otimes_{\mathcal{O}_s} k(s)$ may be regarded as an $\mathcal{O}_{E_s}$-Module denoted by $\mathcal{F}_s$. Then, for each integer i, the homomorphism

$$R^ip_*(\mathcal{F}) \to H^i(E_s, \mathcal{F}_s)$$

induced by the canonical epimorphism $\mathcal{F} \to \mathcal{F}_s$ defines a homomorphism

$$t_s^i : R^ip_*(\mathcal{F}) \underset{\mathcal{O}_s}{\otimes} k(s) \to H^i(E_s, \mathcal{F}_s).$$

PROPOSITION 4. *Let $p : E \to S$ be a proper morphism of locally noetherian schemes, and let $\mathcal{F}$ be a coherent $\mathcal{O}_E$-Module flat over S.*

(i) *If $t_s^i : R^ip_*(\mathcal{F}) \otimes_{\mathcal{O}_s} k(s) \to H^i(E_s, \mathcal{F}_s)$ is surjective for some integer i and some point $s \in S$, then it is bijective.*

(ii) *If the condition of* (i) *is satisfied, then*

$$t_s^{i-1} : R^{i-1}p_*(\mathscr{F}) \underset{\mathscr{O}_s}{\otimes} k(s) \to H^{i-1}(E_s, \mathscr{F}_s)$$

is also surjective if and only if $R^i p_*(\mathscr{F})$ *is a free* $\mathscr{O}_s$*-Module in a neighborhood of* s.

For the proof we refer to EGA III: (i) follows from (7.7.5.3) in view of (7.7.10), and for the same reason (ii) amounts to the equivalence of (7.8.3.b) and (7.8.4.d). (or better, see Mumford, Abelian Varieties, § 5).

COROLLARY 1. *With the assumptions of proposition* 4, *if* $H^{i+1}(E_s, \mathscr{F}_s) = 0$ *for some integer* i *and some point* $s \in S$, *then* t_s^i *is an isomorphism.*

In fact, t_s^{i+1} is surjective, hence bijective by (i). Then $R^{i+1}p_*(\mathscr{F}) = 0$ in a neighborhood of s by Nakayawa's lemma. Therefore the conclusion from (ii), and (i) again.

COROLLARY 2. *With the assumptions of proposition* 4, *if* $\mathscr{E}$ *is a coherent* $\mathscr{O}_s$*-Module and* $\varphi : \mathscr{E} \to p_*(\mathscr{F})$ *is a homomorphism such that the induced map*

$$\mathscr{E} \underset{\mathscr{O}_s}{\otimes} k(s) \to H^0(E_s, \mathscr{T}_s)$$

is bijective for each point s *of* S, *then* φ *is an isomorphism and* $\mathscr{E}$ *is locally free.*

PROOF. The assumption implies that $t_s^0 : p_*(\mathscr{F}) \otimes k(s) \to H^0(E_s, \mathscr{F}_s)$ is surjective, hence bijective for each $s \in S$ by (i). Then

$$\varphi \otimes 1 : \mathscr{E} \otimes k(s) \to p_*(\mathscr{F}) \otimes k(s)$$

is bijective, and therefore φ is surjective by Nakayama's lemma. Finally $p_*(\mathscr{F})$ is locally free by (ii); so, if $\mathscr{G}$ is the kernel of φ, $\mathscr{G} \otimes k(s)$ is the kernel of $\varphi \otimes 1$ for each $s \in S$, whence $\mathscr{G} = 0$. Q.E.D.

Let us consider a family $p : E \to S$ of elliptic curves. Since p is proper, hence separated, the section $0 : S \to E$ is a closed immersion (EGA I, 5.4.b), i.e., it defines an isomorphism from S onto a closed subscheme A of E. Let $I \subset \mathscr{O}_E$ denote the sheaf of ideals of A.

LEMMA 2. *I is an invertible sheaf.*

PROOF. Let x be a closed point of A, $s = p(x)$, and $E_s = p^{-1}(s)$. It is clear that the maximal ideal m of $\mathscr{O}_{x,E_s}$ is generated by the image of

$$I_x \subset \mathscr{O}_{x,E} \text{ in } \mathscr{O}_{x,E_s} = \mathscr{O}_{x,E} \underset{\mathscr{O}_s}{\otimes} k(s).$$

By assumption, $\mathscr{O}_{x,E_s}$ is a discrete valuation ring, hence there is a section f of I over some open neighborhood U of x such that $f_x \otimes 1$ is a basis of

m. Then f defines a closed subscheme A' of U containing $A \cap U$ such that the fibers of A and A' over K are equal at x. As A is flat over S, it coincides with A' near x, i.e., f generates I in a neighborhood V of x.

To show that f is a free generator of I locally at x, let J denote the kernel of the epimorphism $\mathcal{O}_E|V \to I|V$ defined by f. Since I is flat over S, $J_x \otimes_{\mathcal{O}_s} k(s)$ is the kernel of

$$\mathcal{O}_{x,E_s} \xrightarrow{f_x \otimes 1} I_x \underset{\mathcal{O}_s}{\otimes} k(s) = m.$$

Therefore $J_x \otimes_{\mathcal{O}_s} k(s) = 0$, and we conclude that $J_x \otimes_{\mathcal{O}_x} k(x)$ is 0 as a quotient of $J_x \otimes_{\mathcal{O}_s} k(s)$. Hence $J = 0$ in a neighborhood of x by Nakayama's lemma. This completes the proof. Q.E.D.

This result means that A is the support of a divisor on E. The divisor will also be denoted by A, hence the sheaf of functions $\mathcal{O}_E(nA)$ with n-fold poles along A will be isomorphic to the invertible sheaf $I^{\otimes(-n)}$ for each integer n. For each n the quotient $\mathcal{O}_E(nA)/\mathcal{O}_E((n-1)A)$ may be identified with $i^*(\mathcal{O}_E(nA))$ where $i : A \to E$ is the inclusion. Hence

$$p_*(\mathcal{O}_E(nA)/\mathcal{O}_E((n-1)A))$$

is isomorphic to $i^*(\mathcal{O}_E(nA))$ and

$$R^i p_*(\mathcal{O}_E(nA)/\mathcal{O}_E((n-1)A)) = 0 \text{ for } i > 0.$$

In particular, $p_*(\mathcal{O}_E(nA)/\mathcal{O}_E((n-1)A))$ is an invertible $\mathcal{O}_S$-Module, canonically isomorphic to $\mathcal{L}^{\otimes n}$ where $\mathcal{L} = p_*(\mathcal{O}_E(A)/\mathcal{O}_E)$. Other important higher direct images are supplied by the following proposition.

PROPOSITION 5. (i) *The canonical homomorphism*

$$\mathcal{O}_S \to p_*(\mathcal{O}_E)$$

is an isomorphism.

(ii) $p_*(\mathcal{O}_E(nA))$ *is locally free of rank* n *for* $n > 0$.

(iii) $R^1 p_*(\mathcal{O}_E(nA)) = 0$ *for* $n > 0$, *and locally free of rank* 1 *for* $n = 0$.

(iv) $R^i p_*(\mathcal{O}_E(nA)) = 0$ *for* $i > 1$ *and all integers* n.

Moreover, in each case the canonical homomorphism

$$R^i p_*(\mathcal{O}_E(nA)) \underset{\mathcal{O}_s}{\otimes} k(s) \to H^i(E_s, \mathcal{O}_E(nA)_s)$$

is bijective for all $s \in S$.

PROOF. (i) is an immediate consequence of corollary 2 of proposition 4. Then (ii), (iii), and (iv) follow from corollary 1 and part (ii) of proposition 4 applying proposition 1. The final assertion is established in the course of the proof. Q.E.D.

REMARK. It may be proved similarly that, for $n < 0$, $R^i p_*(\mathcal{O}_E(nA))$ is locally free of rank $-n$ if $i = 1$, and 0 otherwise.

COROLLARY 1. *The natural injection* $\mathcal{O}_S \to p_*(\mathcal{O}_E(A))$ *is an isomorphism.*

PROOF. Let us consider the long exact sequence

$$0 \to p_*(\mathcal{O}_E) \xrightarrow{i} p_*(\mathcal{O}_E(A)) \xrightarrow{j} p_*(\mathcal{O}_E(A)/\mathcal{O}_E) \xrightarrow{k} \\ \to R^1 p_*(\mathcal{O}_E) \to R^1 p_*(\mathcal{O}_E(A)) \to \cdots$$

By the proposition $R^1 p_*(\mathcal{O}_E(A)) = 0$ and $R^1 p_*(\mathcal{O}_E)$ is locally free of rank 1. Hence k is surjective and its kernel is locally a direct summand of $\mathcal{L} = p_*(\mathcal{O}_E(A)/\mathcal{O}_E)$. Since $\mathcal{L}$ is also invertible, $\mathrm{Ker}(k) = 0$, and therefore i is an isomorphism. Q.E.D.

COROLLARY 2. *The canonical homomorphism*

$$p_*(\mathcal{O}_E(nA)) \to p_*(\mathcal{O}_E(nA)/\mathcal{O}_E(n-1)A)) = \mathcal{L}^{\otimes n}$$

is surjective for $n > 1$.

This follows immediately from (iii) of proposition 5.

We are now ready to prove the main result of this chapter.

THEOREM 1 (*Weierstrass Normal Form*). *Let* $p : E \to S$ *be a family of of elliptic curves over a k-variety S. Then each point of S has an affine open neighborhood* $U = \mathrm{Spec}(R)$ *such that* $p^{-1}(U)$ *is isomorphic over U to the subscheme of* $\mathbf{P}^2 \times U$ *defined by*

$$Y^2Z = X^3 + aXZ^2 + bZ^3,$$

where $a, b \in R$ *are unique up to the substitutions*

$$a \mapsto \lambda^4 a, b \mapsto \lambda^6 b$$

for $\lambda \in R^*$. *Moreover* $4a^3 + 27b^2$ *is invertible in R.*

REMARK. It is always assumed that the subscheme A defined by the zero section $0 : S \to E$ is mapped to the set where $Z = 0$.

PROOF. Each point of S has an affine open neighborhood $U = \mathrm{Spec}(R)$ such that $\mathcal{L} = p_*(\mathcal{O}_E(A)/\mathcal{O}_E)$ is free on U. We simplify the notation by assuming that U equals S.

If t is a generator of the R-module $\Gamma(S, \mathcal{L})$, then $t^n = t^{\otimes n}$ is a basis of $\Gamma(S, \mathcal{L}^{\otimes n})$ for each integer n. By the corollaries of proposition 5 we have

$$\Gamma(E, \mathcal{O}_E(2A)) = R \oplus R \cdot f$$

where f has image t^2 in $\Gamma(E, \mathcal{O}_E(2A))/R = \Gamma(S, \mathcal{L}^{\otimes 2})$. Similarly,

$$\Gamma(E, \mathcal{O}_E(3A)) = R \oplus R \cdot f \oplus R \cdot g$$

where g projects to t^3 in $\Gamma(S, \mathscr{L}^{\otimes 3})$. Since f^2, fg, f^3 have the leading parts t^4, t^5 and t^6 respectively, it is easy to see that $1, f, g, f^2, fg, f^3$ form a basis of the R-module $\Gamma(E, \mathcal{O}_E(6A))$. In particular, we have

$$g^2 = a_1 fg + a_2 g + a_3 f^3 + a_4 f^2 + a_5 f + a_6$$

where $a_i \in R$ $(1 \leqq i \leqq b)$ are uniquely defined. Taking the leading parts in $\Gamma(S, \mathscr{L}^{\otimes 6})$ we find that $a_3 = 1$. Redefining f and g we may further simplify the equation. Replacing g by $g - \frac{1}{2}a_1 f - \frac{1}{2}a_2$ yields a new equation with $a_1 = a_2 = 0$ without affecting the principal part of g.

Similarly, if f is replaced by $f + \frac{1}{3}a_4$, we get $a_4 = 0$. Hence we may assume that

$$g^2 = f^3 + af + b$$

for some $a, b \in R$.

From the last assertion of proposition 5 we see that $1, f$, and g generate $\mathcal{O}_E(3A)$ on each geometric fiber of p. Hence they generate $\mathcal{O}_E(3A)$ and define a morphism

$$\varphi : E \to \boldsymbol{P}(p_*(\mathcal{O}_E(3A))) \simeq \boldsymbol{P}^2 \times S$$

over S. We claim that φ is an immersion, i.e., $\mathcal{O}_E(3A)$ is very ample.

Since p is proper by assumption, φ is proper (EGA II, 5.4.3). It is injective on the closed fibers (proposition 3), hence injective. So, being closed, φ is a homeomorphism of E onto a closed subspace $\varphi(E)$ of $\boldsymbol{P}^2 \times S$, and $\varphi_*(\mathcal{O}_E)$ is essentially the extension of $\mathcal{O}_E$ by zero. Since $\varphi_*(\mathcal{O}_E)$ is coherent on $\boldsymbol{P}^2 \times S$ (EGA III, 3.2.1), it is enough to show that the canonical homomorphism $u : \mathcal{O}_{\boldsymbol{P}^2 \times S} \to \varphi_*(\mathcal{O}_E)$ is surjective.

If s is a closed point of S, and φ_s is the restriction of φ to E_s, then

$$u_s : \mathcal{O}_{\boldsymbol{P}^2} \to \varphi_*(\mathcal{O}_E) \otimes k(s) = \varphi_{s,*}(\mathcal{O}_{E_s})$$

is surjective by proposition 3. Then the conclusion follows by Nakayama's lemma.

Let E' be the closed subscheme of $\boldsymbol{P}^2 \times S$ defined by

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

It is clear that $\varphi(E)$ is a subscheme of E'. But the closed fibers of $\varphi(E)$ and E' are equal by proposition 3, hence $\varphi(E) = E'$. Since the closed fibers of E are non-singular, the discriminant $4a^3 + 27b^2$ is non-zero at each closed point of S. This means that it is invertible in R.

Finally we note that the section t may be replaced by any section of the form λt where λ is a unit of R. Then f and g are replaced by $\lambda^2 f$ and $\lambda^3 g$, so $\lambda^4 a$ and $\lambda^6 b$ appear in place of a and b. Q.E.D.

Since the coefficients a and b of the Weierstrass normal form

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

given by the theorem are defined only locally and up to multiplication by certain invertible functions, the reader may naturally suspect that they should be connected with some invertible sheaves. To find this connection we introduce global coordinates on projective bundles.

Let Y be a scheme, $\mathscr{E}$ a quasicoherent $\mathcal{O}_Y$-Module, and $S(\mathscr{E})$ the symmetric $\mathcal{O}_Y$-Algebra of $\mathscr{E}$. Then the scheme $P = \mathrm{Proj}(S(\mathscr{E}))$ is called the projective bundle over Y defined by $\mathscr{E}$ and denoted by $\boldsymbol{P}(\mathscr{E})$ (EGA II, 4.1.1). Let us assume that $\mathscr{E}$ is the direct sum of invertible $\mathcal{O}_Y$-Modules:

$$\mathscr{E} = \mathscr{L}_0 \oplus \mathscr{L}_1 \oplus \cdots \oplus \mathscr{L}_n.$$

For each i, let $\eta_i \in \Gamma(Y, \mathscr{L}_i^{-1} \otimes_{\mathcal{O}_Y} \mathscr{E})$ be the section which corresponds to the inclusion of $\mathscr{L}_i$ into $\mathscr{E}$ under the natural isomorphism

$$\mathscr{L}_i^{-1} \underset{\mathcal{O}_Y}{\otimes} \mathscr{E} \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}_Y}(\mathscr{L}_i, \mathscr{E}).$$

If $p : P \to Y$ is the projection, the canonical epimorphism (EGA II, 4.1.5.1) $p^*(\mathscr{E}) \to \mathcal{O}_P(1)$ induces a homomorphism

$$p^*(\mathscr{L}_i^{-1} \underset{\mathcal{O}_Y}{\otimes} \mathscr{E}) \simeq p^*(\mathscr{L}_i^{-1}) \underset{\mathcal{O}_P}{\otimes} p^*(\mathscr{E}) \to p^*(\mathscr{L}_i^{-1})(1)$$

for each i. If $X_i \in \Gamma(P, p^*(\mathscr{L}_i^{-1})(1))$ is the image of η_i by this homomorphism, then $(X_0, X_1, \cdots, X_n)$ is called the gobal coordinate system of P relative to $(\mathscr{L}_0, \cdots, \mathscr{L}_n)$.

Returning to theorem 1, it is obvious that we have constructed, in effect, a canonical splitting

$$p_*(\mathcal{O}_E(3A)) = \mathcal{O}_S \oplus \mathscr{L}^{\otimes 2} \oplus \mathscr{L}^{\otimes 3}$$

where $\mathscr{L} = p_*(\mathcal{O}_E(A)/\mathcal{O}_E)$ and $\mathscr{L}^{\otimes 2}$, $\mathscr{L}^{\otimes 3}$ are locally generated by the functions f, and g, respectively. It is then easy to deduce the following variant of theorem 1.

THEOREM 1′. *Let $p : E \to S$ be a family of elliptic curves over a k-variety S. Then there is an invertible $\mathcal{O}_S$-Module $\mathscr{L}$ such that E is isomorphic over S to the subscheme of $P = \boldsymbol{P}(\mathcal{O}_S \oplus \mathscr{L}^{\otimes 2} \oplus \mathscr{L}^{\otimes 3})$ defined by*

$$Y^2Z = X^3 + aXZ^2 + bZ^3,$$

where $a \in \Gamma(S, \mathscr{L}^{\otimes(-4)})$, $b \in \Gamma(S, \mathscr{L}^{\otimes(-6)})$, and (X, Y, Z) is the global coordinate system of P relative to $(\mathscr{L}^{\otimes 2}, \mathscr{L}^{\otimes 3}, \mathcal{O}_S)$. Furthermore, $(\mathscr{L}, a, b)$ is unique up to isomorphism, and

$$4a^3 + 27b^2 \in \Gamma(S, \mathscr{L}^{\otimes(-12)})$$

is invertible.

Notice that the equation makes sense: both sides are sections of $\mathscr{L}^{\otimes(-6)}(3)$ and the divisor of their difference is associated with a subscheme of P.

For each k-variety S, let $\mathscr{M}(S)$ denote the set of isomorphism classes of families of elliptic curves over S. If E is a family of elliptic curves over S, then for each morphism $S' \to S$, $E \times_S S'$ is a family of elliptic curves over S'. Thus $\mathscr{M}$ becomes a contravariant functor from the category of k-varieties to the category of sets. Also recall that each k-variety M defines a functor h_M by $h_M(S) = \mathrm{Hom}(S, M)$.

COROLLARY. *There is a morphism of functors*

$$\Phi : \mathscr{M} \to h_{A_j^1},$$

where $A_j^1 = \mathrm{Spec}(k[j])$, *such that*

$$\Phi(\mathrm{Spec}\,(k)) : \mathscr{M}(\mathrm{Spec}\,(k)) \to A_j^1(k)$$

is the bijection given by the invariant j (*cf. the corollary of proposition* 3). A_j^1 *is a coarse moduli space for elliptic curves over* k.

PROOF. Each family of elliptic curves over S defines an invertible $\mathscr{O}_S$-Module $\mathscr{L}$ and sections $a \in \Gamma(S, \mathscr{L}^{\otimes(-4)})$, $b \in \Gamma(S, \mathscr{L}^{\otimes -(6)})$ with $4a^3+27b^2 \in \Gamma(S, \mathscr{L}^{\otimes(-12)})$ invertible. Then

$$j_1 = 12^3 \frac{4a^3}{4a^3+27b^2} \in \Gamma(S, \mathscr{O}_S) \tag{1}$$

corresponds to a morphism $S \to A_j^1$. It is clear that this construction is functorial. The second point may be verified by direct calculation starting with the two representations of the same elliptic curve:

$$Y^2 = X'(X'-1)(X'-\lambda) \text{ and } Y^2 = X^3+aX+b$$

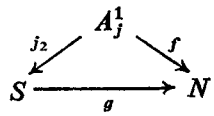
related by $Y = Y'$, $X = X'-(\lambda+1/3)$, and the previous definition:

$$j_2(\lambda) = 256 \left[\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}\right]^3 \tag{2}$$

and verifying that (1) and (2) define the same j. To check the universal property of Φ, suppose $\psi : \mathscr{M} \to h_N$ is another morphism of functors. Let $S = \mathrm{Spec}\, k[\lambda, (1/\lambda)(1/\lambda-1)]$, and let E be the subscheme of $\boldsymbol{P}^2 \times S$ defined by:

$$Y^2Z = X(X-Z)(X-\lambda Z).$$

Then E is an elliptic curve over S and defines an element $(E/S) \in \mathscr{M}(S)$. Let $\psi(E/S)$ be the morphism $g : S \to N$. On the other hand, we just checked that $\Phi(E/S)$ is the morphism $j_2 : S \to A_j^1$ given by formula (2). I claim that g factors:



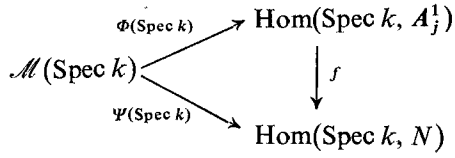
To see this, let $\Gamma \subset A_j^1 \times N$ be the image of (i_2, g). It is clear from the defining formula that j_2 is a finite morphism hence so is (j_2, g), hence Γ is closed. Since

$$j_2(\lambda) = j_2(\lambda') \Rightarrow E_\lambda \simeq E_{\lambda'}$$
$$\Rightarrow g(\lambda) = g(\lambda'),$$

the projection $\Gamma \to A_j^1$ is injective. But j_2 is separable and surjective, hence $\Gamma \to A_j^1$ is separable and surjective. Therefore $\Gamma \to A_j^1$ is an isomorphism by Zariski's Main Theorem. If f is the composition

$$A_j^1 \xleftarrow[p_1]{\sim} \Gamma \xrightarrow[p_2]{} N$$

then $f \circ j_2 = g$. f defines a map of functors $h_{A_j^1} \to h_N$ and it follows from the definition that



commutes. But therefore $f \circ \Phi(s) = \Psi(S)$ for any S as required. Q.E.D.

We now show by examples that the map

$$\Phi(S) : \mathscr{M}(S) \to \mathrm{Hom}\,(S, A_j^1)$$

is neither injective nor surjective in general. In particular, A_j^1 cannot be a fine moduli space for elliptic curves.

EXAMPLE A. Let A be a finitely generated integral domain containing a unit μ which has no square root in A, and put $S = \mathrm{Spec}(A)$. Then for any elliptic curve E over A with equation

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

there is another elliptic curve E', a twisted form of E.

$$Y^2 = X^3 + \mu^2 aX + \mu^3 b$$

which is not isomorphic to E over A, but has the same j. In fact, E and E' become isomorphic over $A(\sqrt{\mu})$. Hence the map $\Phi(S)$ is not injective.

It is also easy to see that the map $\Phi(S)$ need not be surjective. In fact, each morphism $j: S \to A_j^1$ which corresponds to a family of elliptic curves over a scheme S is given locally by the formula

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

where a and b are sections of $\mathcal{O}_S$. If $s \in S$ is a point where $j(s) = 0$, and $\mathcal{M}$ is the maximal ideal of $\mathcal{O}_s$, then $a \in \mathcal{M}$, and therefore $j \in \mathcal{M}^3$. In other words, j must be *ramified* at s. In the same way it follows from the formula

$$j-12^3 = -12^3 \frac{27b^2}{4a^3+27b^2}$$

that j is ramified at each point $s \in S$ with $j(s) = 12^3$.

To explain this phenomenon we study the automorphisms of elliptic curves.

Let E be an elliptic curve over an algebraically closed field k of characteristic $\neq 2,3$, and let $\pi : E \to \boldsymbol{P}^1$ be the morphism defined by a function f with a double pole at the base point 0 of E. Then π is ramified over 4 distinct points a, b, c, and ∞. If α is an automorphism of E leaving 0 fixed, $\pi \circ \alpha$ is a morphism of the same type. Hence there is a projective transformation $\bar{\alpha}$ such that

$$\begin{array}{ccc} E & \xrightarrow{\alpha} & E \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ \boldsymbol{P}^1 & \xrightarrow[\bar{\alpha}]{} & \boldsymbol{P}^1 \end{array}$$

commutes. Then $\bar{\alpha}$ leaves ∞ fixed and permutes the points a, b, and c. But $\bar{\alpha}$ is of order 1, 2, or 3 on the set $\{a, b, c\}$, hence on $\boldsymbol{P}^1$:

(i) If $\bar{\alpha} = \mathrm{Id}$, $\alpha(x) = x$ or $-x$, for all x. Hence $\alpha = \mathrm{Id}$ or $\alpha = -\mathrm{Id}$. These automorphisms exist on any elliptic curve.

(ii) If $\bar{\alpha}$ is of order 2, it is a transposition on $\{a, b, c\}$. Hence we may normalize $\{a, b, c\}$ to $\{0, 1, -1\}$, $\bar{\alpha}(t) = -t$; so $\lambda = -1$ and $j = 12^3$. In fact, on $E_0 : Y^2 = X^3 - X$ there is the automorphism $X \mapsto -X$, $Y \mapsto iY$ of order 4.

(iii) If $\bar{\alpha}$ is of order 3, it is a cyclic permutation on $\{a, b, c\}$. Hence $\{a, b, c\}$ may be normalized to $\{1, \omega, \omega^2\}$ where $\omega^3 = 1$; so $j = 0$. Finally, on $E_{(123)} : Y^2 = X^3 - 1$, there is the automorphism $X \mapsto \omega X$, $Y \mapsto -Y$ of order 6.

Collecting the results we get:

THEOREM 2. *The group of automorphisms* $\mathrm{Aut}(E_j)$ *of an elliptic curve* E_j *with invariant* j *is* $\mathbf{Z}/2\mathbf{Z}$ *if* $j \neq 0, 12^3$. *In addition,* $\mathrm{Aut}(E_0) = \mathbf{Z}/6\mathbf{Z}$ *and* $\mathrm{Aut}(E_{(12^3)}) = \mathbf{Z}/4\mathbf{Z}$.

It is now quite plausible that the nontrivial automorphisms of E_0 and $E_{(12^3)}$ are the cause for the non-existence of families of elliptic curves with an arbitrarily prescribed invariant $j \in \Gamma(S, \mathcal{O}_S)$. To disclose the connection more clearly we turn to complex analytic families of elliptic curves. It is sufficient for our purposes to define them in the following way.

DEFINITION 2. An analytic family of elliptic curves over a complex analytic space S is the quotient of a line bundle L over S by a lattice $\Gamma \subset L$ (i.e., Γ is a closed discrete subgroup bundle with fibre $\mathbf{Z} \times \mathbf{Z}$).

EXAMPLE B. Let H be the upper half plane of the complex plane $\mathbf{C}$, and denote by E the quotient of the trivial line bundle $H \times \mathbf{C}$ by the lattice generated by the sections corresponding to the constant 1 and the identity map $H \to \mathbf{C}$. It is immediate that each analytic family of elliptic curves is induced locally by the family E.

The fiber E_z of E over a point $z \in H$ is the quotient of $\mathbf{C}$ by the lattice Γ_z generated by 1 and z. Any isomorphism $E_z \xrightarrow{\sim} E_{z'}$ between two fibers may be lifted to an isomorphism of $\mathbf{C}$. This means that there is a constant $k \in \mathbf{C}^*$ such that (kz, k) is a basis for $\Gamma_{z'}$, i.e.,

$$kz = az' + b$$
$$k = cz' + d,$$

for some $a, b, c, d \in \mathbf{Z}$ with $ad - bc = 1$. Hence z is in the orbit of z' under the action of $SL(\mathbf{Z}, 2)$ on H given by

$$z \mapsto \frac{az+b}{cz+d}$$

for

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(\mathbf{Z}, 2).$$

Conversely, it is clear that this is a sufficient condition for the existence of an isomorphism $E_z \xrightarrow{\sim} E_{z'}$. In fact, it may be shown that the map

$$z \mapsto (j \text{ of } E_z)$$

defines an analytic morphism $j : H \to \mathbf{C}$ whose fibers are the orbits of the points $z \in H$ under $SL(\mathbf{Z}, 2)$. This function j is the classical elliptic modular function (see e.g. Serre, Cours d'Arithmétique, chap. VII).

In particular, the group of automorphisms of E_z is isomorphic to the subgroup of elements

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(\mathbf{Z}, 2)$$

which leave z fixed and therefore induce maps from E_z to itself.

It follows that a point $z \in H$ is left fixed by some element $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of $SL(Z, 2)$ other than

$$\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

if and only if there is a nontrivial automorphism on E_z. In each neighborhood of such a point z_0 there are always distinct points w and $(aw+b/cw+d)$ with isomorphic fibers in the family E. Hence j must be ramified at z_0. The same conclusion holds for any analytic family of elliptic curves because of the locally universal character of E.

REMARK. It is not hard to see that there are two $SL(\mathbf{Z}, 2)$-orbits of points of H left fixed by some nontrivial element of $SL(\mathbf{Z}, 2)$, namely ω and i corresponding to $j = 0$ and $j = 12^3$, in agreement with theorem 2.

4. Binary quartics [2]

Thus far, we have taken an *ad hoc* approach to classifying elliptic curves, relying on explicit formulae. What happens more often in moduli problems is that in the first stage you construct either

(a) embeddings in some $\mathbf{P}^n$, $n > 1$, or

(b) finite morphisms to $\mathbf{P}^1$, with branch locus B, or

(c) some other reduction to projective data,

which is canonical except for a projective transformation. To illustrate, given an elliptic curve E, with base point 0, using an arbitrary basis of $H^0(\mathcal{O}_E(3(0)))$, we construct an isomorphism of E with a plane cubic curve C, which is then canonically determined up to a change $C' = \gamma(C)$, $\gamma \in PGL(3, k)$. Or, using an arbitrary basis of $H^0(\mathcal{O}_E(2(0)))$, we construct a finite morphism of degree 2 from E to $\mathbf{P}^1$, with branch locus B of degree 4; then B determines E, and conversely, E determines B up to a change $B' = \gamma(B)$, $\gamma \in PGL(2, k)$. Once the general moduli problem is reduced to the classification of some subvarieties, cycles etc. on $\mathbf{P}^n$ modulo $PGL(n+1, k)$, the second stage is to use the theory sketched in Chapters 1 and 2 to find moduli for these projective objects. In this chapter, I would

[2] The following chapter is completely different from Chapter 4 in the original notes and was not presented at Oslo. I have substituted it because it seems to me a much more logical continuation, tieing everything up and keeping to elementary constructions.

like to illustrate how this general procedure works when the classification of elliptic curves is carried out in 2 stages: first reduction to cycles in $\boldsymbol{P}^1$ of degree 4; second construction of the quotient of the space of such cycles by $PGL(2, k)$.

The space of cycles of degree n on $\boldsymbol{P}^1$, or what is the same, the space of *unordered* sets of n points on $\boldsymbol{P}^1$, is just $\boldsymbol{P}^n$! In fact, let

$$\boldsymbol{P}^n_{\langle a\rangle} = \boldsymbol{P}(k\cdot a_0 + \cdots + k\cdot a_n)$$

be the projective space with homogeneous coordinates $a_0, \cdots, a_n$, and let

$$\boldsymbol{P}^1 = \boldsymbol{P}(k\cdot X_0 + k\cdot X_1)$$

be the projective line with homogeneous coordinates X_0, X_1. Then define

$$\mathscr{D} \subset \boldsymbol{P}^1 \times \boldsymbol{P}^n_{\langle a\rangle}$$

by

$$\mathscr{D} = \left\{ \begin{array}{l} \text{locus of solutions of} \\ a_0 X_0^n + a_1 X_0^{n-1} X_1 + \cdots + a_n X_1^n = 0 \end{array} \right\}.$$

If α is a closed point of $\boldsymbol{P}^1_{\langle a\rangle}$ and $D_\alpha = \mathscr{D} \cap (\boldsymbol{P}^1 \times (\alpha))$, then D_α is the set of roots of the equation $\sum \alpha_i X_0^{n-i} X_1^i = 0$ where (α_i) are homogeneous coordinates of α. Even better though, $\mathscr{D}$ is a Cartier divisor on $\boldsymbol{P}^1 \times \boldsymbol{P}^n$, i.e. it is defined locally everywhere by 1 equation, and since $\mathscr{D} \not\supset \boldsymbol{P}^1 \times (\alpha)$ for any $(\alpha) \in \boldsymbol{P}^n$, we can define $D_\alpha = \mathscr{D} \cdot (\boldsymbol{P}^1 \times (\alpha))$ as a Cartier divisor too, i.e. restrict the defining equation of $\mathscr{D}$ to $\boldsymbol{P}^1 \times (\alpha)$. But divisors on a curve are just cycles, i.e. formal linear combinations of closed points $\sum n_i(x_i)$. It is clear that the divisor D_α is defined locally by the equation $\sum \alpha_i (X_1/X_0)^i = 0$, or by $\sum \alpha_i (X_0/X_1)^{n-i} = 0$, and as a cycle D_α is just the set of roots of the polynomial $\sum \alpha_i X_0^{n-1} X_1^i$ *counted with their multiplicities*. Now since every set of n points (λ_i, μ_i) in $\boldsymbol{P}^1$, with or without repetitions, is the set of solutions of a unique homogeneous polynomial (up to a scalar), viz:

$$\prod_{i=1}^{n} (\mu_i X_0 - \lambda_i X_1),$$

it follows that every cycle of degree n on $\boldsymbol{P}^1$ equals D_α for one and only one $\alpha \in \boldsymbol{P}^n$.

From another point of view, $\boldsymbol{P}^n_{\langle a\rangle}$ can be viewed as the quotient of $(\boldsymbol{P}^1)^n$ by the group $\sum_n$ of permutations on n letters. In fact, $(\boldsymbol{P}^1)^n$ parametrizes the *ordered* sets of n points and $\boldsymbol{P}^n_{\langle a\rangle}$ the *unordered* sets. Explicitly, expand:

$$\prod_{i=1}^{n} (\mu_i X_0 - \lambda_i X_1) = \sum_{i=0}^{n} a_i(\lambda, \mu) X_0^{n-i} X_1^i .$$

Then define

$$\pi : (\boldsymbol{P}^1)^n \to \boldsymbol{P}^n_{\langle a \rangle}$$

by

$$\pi((\lambda_1, \mu_1), \cdots, (\lambda_n, \mu_n)) = (a_0(\lambda, \mu), \cdots, a_n(\lambda, \mu)).$$

It is easy to see that $\pi(x) = \pi(y)$ if and only if $x = \sigma(n)$ for some permutation $\sigma \in \sum_n$. In fact, $\boldsymbol{P}^n_{\langle a \rangle}$ is a geometric quotient of $(\boldsymbol{P}^1)^n$ by $\sum_n$. On an affine level, π restricts to the map:

$$\text{res } \pi : (\boldsymbol{A}^1) \xrightarrow{n} \boldsymbol{A}^n$$
$$\pi(\lambda_1, \cdots, \lambda_n) = (\lambda_1 + \cdots + \lambda_n; \sum_{i<j} \lambda_i \lambda_j; \cdots; \lambda_1 \cdots \lambda_n),$$

the elementary symmetric functions,

and it is a classical fact that the elementary symmetric functions generate the full ring of permutation-invariant polynomials in n indeterminants $\lambda_1, \cdots, \lambda_n$.

Now consider double coverings of $\boldsymbol{P}^1$. *Assume for the rest of this chapter* $\text{char}(k) \neq 2, 3$. We want to prove that a double covering is determined by its branch locus.

PROPOSITION 1. *Let C be a non-singular curve and let $\pi : C \to \boldsymbol{P}^1$ be a finite surjective morphism of degree 2. Let $x_1, \cdots, x_n \in \boldsymbol{P}^1$ be the branch points of π. Then $n = 2m$, and C can be constructed as*:

$$C = \underline{\text{Spec}}(\mathscr{A}),$$

where $\mathscr{A}$ is the sheaf of $\mathcal{O}_{\boldsymbol{P}^1}$ algebras $\mathcal{O}_{\boldsymbol{P}^1} \oplus \mathcal{O}_{\boldsymbol{P}^1}(-m)$, where 2 functions are multiplied by the rule:

$$(*) \qquad (f_1, g_1) \cdot (f_2, g_2) = (f_1 f_2 + \phi(g_1, g_2), f_1 g_2 + f_2 g_1)$$

and ϕ is the map:

$$(**) \quad \mathcal{O}_{\boldsymbol{P}^1}(-m) \times \mathcal{O}_{\boldsymbol{P}^1}(-m) \to \mathcal{O}_{\boldsymbol{P}^1}(-2m) \cong \mathcal{O}_{\boldsymbol{P}^1}(-\sum_{i=1}^{n} x_i) \subset \mathcal{O}_{\boldsymbol{P}^1}.$$

PROOF. C will have an automorphism $\lambda : C \to C$ of order 2 interchanging the 2 points over each point of $\boldsymbol{P}^1$. Now since π is a finite morphism, C is automatically equal to $\underline{\text{Spec}}(\pi_* \mathcal{O}_C)$. The automorphism λ acts as an automorphism of $\pi_*(\mathcal{O}_C)$, and since $\text{char} \neq 2$, $\pi_*(\mathcal{O}_C)$ splits into a sum $F^+ \oplus F^-$, where $\lambda(f) = f$, $f \in \Gamma(U, F^+)$; $\lambda(f) = -f$, $f \in \Gamma(U, F^-)$. Now the λ-invariant functions F^+ on C must be the functions of the form $g \circ \pi$, $g \in \Gamma(U, \mathcal{O}_{\boldsymbol{P}^1})$, so $F^+ \cong \mathcal{O}_{\boldsymbol{P}^1}$. Since π has degree 2, $\pi_*(\mathcal{O}_C)$ is a locally free sheaf of $\mathcal{O}_{\boldsymbol{P}}$-modules of rank 2, hence the second factor F^- is locally free of rank 1. Therefore $F^- \cong \mathcal{O}_{\boldsymbol{P}^1}(k)$, some $k \in \boldsymbol{Z}$. Now the product of 2 odd functions is even, hence the multiplication in

$\pi_* \mathcal{O}_C \cong \mathcal{O}_{\boldsymbol{P}^1} \oplus \mathcal{O}_{\boldsymbol{P}^1}(k)$ must be given by a rule of the form (*). Finally any non-zero bilinear $\phi : \mathcal{O}_{\boldsymbol{P}}(k) \times \mathcal{O}_{\boldsymbol{P}}(k) \to \mathcal{O}_{\boldsymbol{P}}$ is induced by a composition:

$$\mathcal{O}_{\boldsymbol{P}^1}(k) \times \mathcal{O}_{\boldsymbol{P}^1}(k) \to \mathcal{O}_{\boldsymbol{P}^1}(2k) \simeq \mathcal{O}_{\boldsymbol{P}^1}(-\sum y_i) \subset \mathcal{O}_{\boldsymbol{P}^1}$$

for some cycle $\sum y_i$ of degree $-2k$. Now reverse the construction and start from the cycle $\sum y_i$, use this to define ϕ and set $C^* = \underline{\mathrm{Spec}}(\mathcal{O}_{\boldsymbol{P}^1} \oplus \mathcal{O}_{\boldsymbol{P}^1}(k))$. If $y \in \boldsymbol{P}^1$, t is a generator of the maximal ideal $m_{y, \boldsymbol{P}^1}$, and s is a generator of the stalk $\mathcal{O}_{\boldsymbol{P}^1}(k)_y$, then near y, $\boldsymbol{C}^*$ is given explicitly by the equation:

$$s^2 = u \cdot t^r$$

where u is a unit in $\mathcal{O}_{y, \boldsymbol{P}^1}$ and

$$r = \text{mult. of } y \text{ in } \sum y_i.$$

Therefore C^* is singular if $r > 1$; C^* is non-singular and y is a branch point if $r = 1$; and C^* is non-singular and unbranched over y if $r = 0$. It follows that in the case of the proposition $\sum y_i = \sum x_i$ and $n = -2k$.

Q. E. D.

Combining this with the results of Chapter 3, we find:

COROLLARY. *The set of elliptic curves over k is canonically isomorphic to the set*:

$$\left\{ \begin{array}{l} \text{cycles of degree 4 on } \boldsymbol{P}^1 \\ \text{with no multiple points} \end{array} \right\} \Big/ PGL(2, k)$$

We could refine this result, using elliptic curves over S and the methods of Chapter 3 to show in addition:

PROPOSITION 2: *If $U \subset \boldsymbol{P}^4_{\langle a \rangle}$ is the open set of cycles of degree 4 with no multiple points, then using the map of points in the previous Corollary, a geometric quotient of U by $PGL(2, k)$ becomes a coarse moduli space for elliptic curves.*

We omit the proof which follows the techniques already discussed.

The next step is to ask what Theorem 2, Ch. II says about the quotient of $\boldsymbol{P}^4_{\langle a \rangle}$ by $PGL(2, k)$. We make contact at this point with some of the oldest work in invariant theory. In fact, to work out Theorem 2, first we replace $PGL(2, k)$ by its double covering $SL(2, k)$ in order that the action of the group on $\boldsymbol{P}^4_{\langle a \rangle}$ should lift to the invertible sheaf $\mathcal{O}_{\boldsymbol{P}^4}(1)$. Then $SL(2, k)$ acts on the whole homogeneous coordinate ring

$$k[a_0, a_1, a_2, a_3, a_4]$$

of $\boldsymbol{P}^4_{\langle a \rangle}$. This action is the obvious one, i.e. let

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, k)$$

It acts on $\boldsymbol{P}^1$ by the linear map

$$(X_0, X_1) \to (aX_0 + bX_1, cX_0 + dX_1)$$

in homogeneous coordinates. We must make it act on the a_i so that the form $\sum a_i X_0^{4-i} X_1^i$ has invariant meaning, since in its action on $\boldsymbol{P}^4_{\langle a \rangle}$, the subvariety $\mathscr{D} \subset \boldsymbol{P}^1 \times \boldsymbol{P}^4_{\langle a \rangle}$ should be taken into itself. In other words

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ induces the map $a_i \to a_i'$ such that

$$\sum a_i'(aX_0 + bX_1)^{4-i}(cX_0 + dX_1)^i \equiv \sum a_i X_0^{4-i} X_1^i .$$

Alternatively, $SL(2, k)$ acts on the vector space $\sum k \cdot a_i$ by the dual of the 4th symmetric power of its action on $kX_0 + kX_1$. The whole construction hinges on the subring

$$R = k[a_0, a_1, a_2, a_3, a_4,]^{SL(2,k)}$$

of invariants. In classical terminology, one wrote $f = \sum a_i X_0^{4-i} X_1$, and called f a *binary quartic*. The elements of R were called the *invariants of a binary quartics*. More generally, the elements of

$$k[X_0, X_1, a_0, a_1, a_2, a_3, a_4]^{SL(2,k)}$$

(such as f itself) were called the *covariants of a binary quartic*. Generators of both of these rings are classical. (Good references are Elliott, *Algebra of Quantics*, Grace and Young, *The algebra of invariants*, or Schur, *Vorl. über Invarianten theorie*.) They are written down quickest by an amazing technique known as the symbolic method – the only bit of linear algebra I believe that has not been thoroughly 'Bourbakized'[3]. One does this: one takes the form f and formally writes it out as though it were a power of a linear form in several different ways, i.e.

$$f = \alpha_x^4 = \beta_x^4 = \gamma_x^4 = \cdots$$

where

$$\alpha_x = \alpha_0 X_0 + \alpha_1 X_1$$

$$\beta_x = \beta_0 X_0 + \beta_1 X_1$$

etc.

One then makes a monomial in α_x, β_x, etc. and the 2×2 determinants:

$$(\alpha, \beta) = \alpha_0\beta_1 - \alpha_1\beta_0$$

$$(\alpha, \gamma) = \alpha_0\gamma_1 - \alpha_1\gamma_0$$

[3] (Added in proof) Now it has been ...
cf. Dieudonné, Seminaire Bourbaki, June 1971.

such that the total degree in each α, β etc. used is 4. For instance:

$$\begin{aligned} f &= \alpha_x^4 \\ h &= (\alpha, \beta)^2 \alpha_x^2 \beta_x^2 \\ j &= (\alpha, \beta)^2 (\gamma, \beta) \alpha_x^2 \beta_x \gamma_x^3 \\ P &= (\alpha, \beta)^4 \\ Q &= (\alpha, \beta)^2 (\alpha, \gamma)^2 (\beta, \gamma)^2 \end{aligned}$$

Each of these can be re-interpreted as a polynomial in the coefficients a_i and the variables (X_0, X_1) by simply taking each monomial $\alpha_0^{4-i}\alpha_1^i$, $\beta_0^{4-i}\beta_1^i$, etc. and replacing it by $\binom{4}{i}^{-1} a_i$ which it equals in purely formal identity $f = \alpha_x^4, f = \beta_x^4$ etc. One must obtain in this way a covariant. Here is an example:

$$\begin{aligned} P &= (\alpha_0 \beta_1 - \alpha_1 \beta_0)^4 \\ &= \alpha_0^4 \beta_1^4 - 4\alpha_0^3 \alpha_1 \beta_0 \beta_1^3 + 6\alpha_0^2 \alpha_1^2 \beta_0^2 \beta_1^2 - 4\alpha_0 \alpha_1^3 \beta_0^3 \beta_1 + \alpha_1^4 \beta_0^4 \\ &= a_0 a_4 - \tfrac{1}{4} a_1 a_3 + \tfrac{1}{6} a_2^2 - \tfrac{1}{4} a_3 a_1 + a_4 a_0 \\ &= \tfrac{1}{6}(a_2^2 - 3a_1 a_3 + 12 a_0 a_4) \end{aligned}$$

Similarly, but with a bit more sweat, Q comes out as the determinant:

$$\begin{aligned} Q &= 6 \cdot \det \begin{pmatrix} a_0 & a_1/4 & a_2/6 \\ a_1/4 & a_2/6 & a_3/4 \\ a_2/6 & a_3/4 & a_4 \end{pmatrix} \\ &= a_0 a_2 a_4 - \tfrac{3}{8} a_0 a_3^2 - \tfrac{3}{8} a_1^2 a_4 + \tfrac{1}{8} a_1 a_2 a_3 - \tfrac{1}{36} a_2^3 \end{aligned}$$

It is an old theorem that f, h, j, P and Q generate the ring of covariants. For instance another well-known invariant is the discriminant D of the form f: i.e. for the form

$$f = \prod_{i=1}^{4} (\mu_i X_0 - \lambda_i X_1)$$

let

$$D = \prod_{1 \leqq i < j \leqq 4} (\lambda_j \mu_i - \lambda_i \mu_j)^2$$

Then D can be rewritten as a homogeneous polynomial in the coefficients a_0, a_1, a_2, a_3, a_4 of f of degree 6. But in fact, one sees easily that:

LEMMA 1. $D = \text{const.}\ (P^3 - 6Q^2)$.

PROOF. In fact, on a k-valued form f, $D(f) = 0$ if and only if f has a double zero. And D is zero to 1st order on the irreducible variety of f's with multiple zeros. Since D, P^3 and Q^2 all have degree 6 in the a's, it suffices to show that $D | P^3 - 6Q^2$ and for this it suffices to show that $P(f)^3 = 6Q(f)^2$ if f is a form with double zeroes. But such an f is equivalent to a form $\bar{f}$ with double zero at $X_1 = 0$, i.e. with $a_0 = a_1 = 0$.

Therefore

$$P(\bar{f}) = \tfrac{1}{6}\bar{a}_2^2,\ Q(\bar{f}) = -\tfrac{1}{36}\bar{a}_2^3,$$

hence indeed

$$P(f)^3 = P(\bar{f})^3 = (\tfrac{1}{6})^3\bar{a}_2^6 = 6Q(\bar{f})^2 = 6Q(f)^2.$$

Q. E. D.

We will not prove or use the result on the generators of ring of covariants although it is not too hard. Instead we want to see geometrically what P and Q do. The first point is:

LEMMA 2: $P(f) = Q(f) = 0 \Leftrightarrow$ *the form f has a triple zero.*

PROOF. This is clear from lemma 1 and the fact that if f has a double zero at $X_1 = 0$, then $P(f) = \frac{1}{6}a_2^2$, so that $P(f) = 0$ if and only if the double zero is a triple zero.

Q. E. D.

Let $X_{ss} \subset \boldsymbol{P}^4_{\langle a\rangle}$ be the open set of forms f with no triple zero. Then we obtain a morphism:

$$\pi : X_{ss} \to \text{Proj } k[P, Q].$$

Since deg $P = 2$, deg $Q = 3$, the subring of $k[P, Q]$ of elements whose degrees are multiples of 6 is just the ring $k[P^3, Q^2]$, and

$$\text{Proj } k[P, Q] = \text{Proj } k[P^3, Q^2] \cong \boldsymbol{P}^1.$$

Thus π is just the map from X_{ss} to $\boldsymbol{P}^1$ defined by P^3/Q^2. To examine the orbits of $PGL(2, k)$ in X_{ss}, note that any form f with at least 3 distinct zeroes is equivalent to a constant times a form

$$f_\lambda(X) = X_0 \cdot X_1 \cdot (X_0 - X_1)(X_0 - \lambda X_1)$$

by a projective transformation. But computing we find

$$a_0 = 0,\ a_1 = 1,\ a_2 = -(\lambda+1),\ a_3 = \lambda,\ a_4 = 0$$

hence

$$P(f_\lambda) = \tfrac{1}{6}(\lambda^2 - \lambda + 1)$$

$$Q(f_\lambda) = \tfrac{1}{72}(\lambda+1)(\lambda-2)(2\lambda-1)$$

and by lemma 1:

$$P(f_\lambda)^3 - 6Q(f_\lambda)^2 = \text{cnst. } \lambda^2(\lambda-1)^2.$$

Therefore

$$j(\lambda) = \text{cnst.} \frac{P(f_\lambda)^3}{P(f_\lambda)^3 - 6Q(f_\lambda)^2}.$$

But we proved in Chapter 3 that

$$j(\lambda_1) = j(\lambda_2) \Leftrightarrow \left\{ \begin{array}{l} \text{the 2 sets of points } \{0, 1, \infty, \lambda_1\} \\ \text{and } \{0, 1, \infty, \lambda_2\} \text{ are projectively} \\ \text{equivalent} \end{array} \right\}$$

hence

$$P(f_{\lambda_1})^3/Q(f_{\lambda_1})^2 = P(f_{\lambda_2})^3/Q(f_{\lambda_2})^2 \Leftrightarrow j(\lambda_1) = j(\lambda_2)$$
$$\Leftrightarrow f_{\lambda_1} \text{ is equivalent to a constant times } f_{\lambda_2} \text{ by some } \sigma \in SL(2, K)$$

Finally, in X_{ss}, all orbits are represented by forms f_λ except for the forms with 2 distinct doubles zeroes, which are equivalent to a constant times the form:

$$f^*(X) = X_0^2 X_1^2.$$

It is clear that $P(f^*)^3/Q(f^*)^2 = 6$, just like the other forms with one double zero. Now define $X_s \subset X_{ss}$ to be the open set of forms f with no double zero. The we can summarize our conclusions in:

PROPOSITION 3. *Let $\delta \in \text{Proj } k[P, Q]$ be the point defined by $P^3/Q^2 = 6$. Then*

(i) $X_s = \pi^{-1}(\text{Proj}(k[P, Q]) - (\delta))$

(ii) *if $x \in \text{Proj } k[P, Q]$, $x \neq \delta$, then $\pi^{-1}(x)$ consists of one orbit and it is closed in X_{ss}.*

(iii) *$\pi^{-1}(\delta)$ consists of 2 orbits, the orbit of the form f_0 which is 3-dimensional and the orbit of the form f^* which is 2-dimensional. The first is open in $\pi^{-1}(\delta)$ and the second is closed.*

The final step is:

PROPOSITION 4. *$\text{Proj } k[P, Q] - (\delta)$ is a geometric quotient of X_s by $PGL(2, k)$.*

SKETCH OF PROOF. The only remaining point is that for all

$$U \subset \text{Proj } k[P, Q] - (\delta),$$

invariant functions f on $\pi^{-1}(U)$ are induced by functions on U itself. This can be checked by first restricting f to the curve in X_s of forms f_λ, $(\lambda \neq 0,1)$, and noting that this curve is separable and finite over

$$\text{Proj } k[P, Q] - (\delta).$$

But f is set theoretically a pull-back of a function on U, so by Zariski's Main Theorem, $f = g \circ \pi$, some $g \in \Gamma(U, \mathcal{O}_u)$. This is nothing but a rephasing of the final arguement in Ch. 3 that A_j^1 is a coarse moduli space.

This gives us a new proof of the main results of Ch. 3. It also gives us an idea of how to interpret the compactification $\boldsymbol{P}^1_j$ of A^1_j as a moduli space of a bigger moduli functor. Whenever a moduli space is not complete, the natural question is: what happens to the objects being classified when they move off to the boundary of the moduli space? As $j \to \infty$, or $P^3/Q^2 \to 6$, we see that $f_\lambda \to f_0$ or f^*, representatives of the 2 orbits in X_{ss} over δ. In the proof of Prop. 1, we saw how to construct double coverings of $\boldsymbol{P}^1$ from any cycle on $\boldsymbol{P}^1$ of even degree: if these cycles have multiplicities, the effect is to make the covering a singular curve. To be explicit, take as branch locus the cycle $f_0 = 0$, i.e. $2(0)+(1)+(\infty)$. The associated double covering is the curve C_0 which is covered by the 2 affine pieces:

(i) $\pi^{-1}(\boldsymbol{P}^1-(\infty))$ which is given by

$$Y^2 = \left(\frac{X_0}{X_1}\right)^2\left(\frac{X_0}{X_1}-1\right)$$

(ii) $\pi^{-1}(\boldsymbol{P}^1-(0))$ which is given by

$$Z^2 = \left(\frac{X_1}{X_0}\right)\left(\frac{X_1}{X_0}-1\right).$$

The two are related by $Z = i(X_1/X_0)^2 \cdot Y$. Note that C_0 is non-singular except for an ordinary double point (or node) over (0), i.e. a double point at which the tangent cone consists of 2 distinct lines. If $t = Y/(X_0/X_1)$, then $t^2 = X_0/X_1 - 1$, hence

$$\frac{X_0}{X_1} = t^2+1$$
$$Y = t(t^2+1)$$

which proves that the field of rational functions on C_0 is $k(t)$. Thus C_0 is a rational curve with 1 node. On the other hand, take as branch locus the cycle $f^* = 0$, i.e. $2(0)+2(\infty)$. The associated double covering C^* is covered by:

(i) $\quad Y^2 = \left(\dfrac{X_0}{X_1}\right)^2$

and

(ii) $\quad Z^2 = \left(\dfrac{X_1}{X_0}\right)^2$

related by $Z = Y \cdot (X_1/X_0)$. Thus C^* has, in fact, 2 non-singular rational components:

$$C_1^* : \text{the union of } Y = \frac{X_0}{X_1} \text{ and } Z = \frac{X_1}{X_0}$$

C_2^* : the union of $Y = -\frac{X_0}{X_1}$ and $Z = -\frac{X_1}{X_0}$

meeting transversely at 2 points

$$Y = \frac{X_0}{X_1} = 0 \text{ and } Z = \frac{X_1}{X_0} = 0.$$

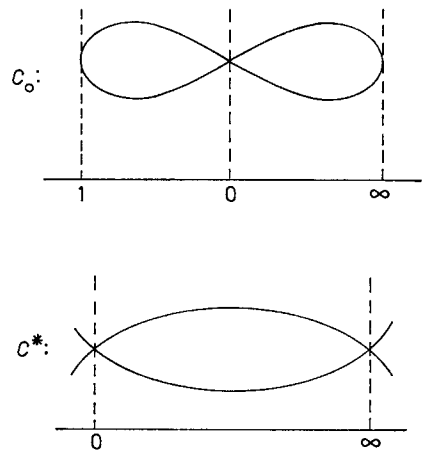


Figure 1

Moreover, consider the algebraic family of cycles $2(0)+(\mu)+(\infty)$. They are all projectively equivalent, but as $\mu \to \infty$, it 'jumps' to the cycle $2(0)+2(\infty)$. Taking double coverings, the curve C_0 can 'jump' to C^*. Topologically if $k = \boldsymbol{C}$, what happens is illustrated below:

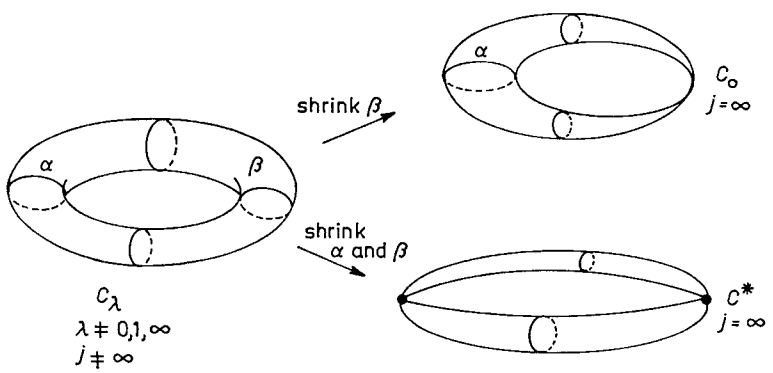


Figure 2

In other words, as $j \to \infty$, if we follow the differentiable family of surfaces C_λ, either one or two curves begin to shrink until when $j = \infty$,

we wind up with a topological space which is no longer a manifold but is homeomorphic to one of the 2 spaces C_0 or C^* as illustrated.

If we return to our functor $\mathscr{M}$, there is a very natural way to enlarge $\mathscr{M}$ allowing the curve C_0 to define a new element of $\mathscr{M}(\text{Spec } k)$.

DEFINITION. A *family of semi-elliptic curves* over a k-variety S is a morphism of k-varieties $p : E \to S$ together with a section $0 : S \to E$ such that E is proper and flat over S, the closed fibres are either elliptic curves or a rational curve with one node and in the latter case, $0(s) \neq$ the node.

DEFINITION. $\overline{\mathscr{M}}(S)$ = the set of all such families over S, up to isomorphism.

We can now extend the whole theory of Ch. 3 and 4 to semi-elliptic families: A = Image of 0 is a divisor, $p_* \mathscr{O}_E(2A)$ and $p_* \mathscr{O}_E(3A)$ are locally free sheaves in S of ranks 2 and 3, and locally over S, E can be defined either

a) as a covering of $\boldsymbol{P}^1 \times S$ ramified in a suitable family of cycles of degree 4 on $\boldsymbol{P}^1$ parametrized by S or

b) by an equation in Weierstrass normal form $y^2 = x^3 + ax + b$.

In case (a), the key point is that the cycle is semi-stable and has at most one double point; in case (b), $4a^3 + 27b^2$ need not be invertible, but a and b together should have no common zeroes. The final conclusion is that there is a canonical morphism

$$\bar{\Phi} : \overline{\mathscr{M}} \to h_{\boldsymbol{P}^1_j}$$

extending our previous Φ and making $\boldsymbol{P}^1_j$ into a coarse moduli space for semi-elliptic curves.

This gives us a rather satisfactory way to answer the question – what happens to the elliptic curve at ∞. However, as soon as we begin to admit singular curves into our moduli space, it raises another question – what happens if we admit *all* singular curves C of arithmetic genus 1 (i.e. $\chi(\mathscr{O}_C) = 0$) into our moduli space? As might be expected, we get more and wilder jump phenomenon. (Incidentally, when classifying 2-dimensional varieties, jump phenomenon can even appear with families of non-singular varieties). It turns out that there is a qualitative difference between curves with nodes only and curves with higher singularities such as cusps. I would like to give 2 examples illustrating how pathological curves with cusps are from the point of view of moduli.

EXAMPLE A. Take any elliptic curve E over k and write it in Weierstrass normal form:

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

For every $\lambda \in k$, $\lambda \neq 0$,

$$y^2 = x^3 + \lambda^2 ax + \lambda^3 \cdot b$$

represents the same elliptic curve. Consider the family E of curves over $S = \operatorname{Spec} k[\lambda]$ defined by this equation.

Then

$$E \cong E_\lambda \text{ all } \lambda \neq 0.$$

But E_0 is the curve $y^2 = x^3$: an irreducible plane cubic curve with a cusp at $x = y = 0$, which is rational (if $t = y/x$, then $x = t^2$, $y = t^3$). In other words, *every elliptic curve*, without changing j, can jump to the cuspidal cubic $y^2 = x^3$. Thus j is completely indeterminant on $y^2 = x^3$ and, topologically, it is impossible to fit E_0 into the moduli space $\boldsymbol{P}^1_j$ even allowing non-separated schemes!

EXAMPLE B. Let $k = \boldsymbol{C}$.

Let C_0 be a plane curve of degree n with one cusp and no other singularities. If we choose coordinates correctly, we can normalize C_0 so that the cusp is the origin $x = y = 0$ and the affine equation of C_0 is of the form:

$$0 = x^2 + y^3 + p_4(x, y)$$

where P_4 is a polynomial whose leading terms have degree $\geqq 4$. Let C_t be the nearby curve defined by the equation

$$t = x^2 + y^3 + P_4(x, y), \; |t| < \varepsilon.$$

It is easy to see that C_t is non-singular everywhere and I would like to describe the topological situation with C_t approaching C_0. Everywhere except in a neighbourhood of (0, 0), $\bigcup_{|t|<\varepsilon} C_t$ forms a nice differentiable family of surfaces over the t-disc. However near (0, 0), since $|P_4(s, y)|$ is much less than $|x^2|$ or $|y^3|$, C_t is essentially the surface

$$C_t^0 : \begin{matrix} x = \pm\sqrt{t - y^3} \\ |y| < \eta \end{matrix}$$

Take t even smaller: in fact $|t| < \frac{1}{2}\eta^3$. Then x is a branched covering of the y-disc $|y| < \eta$, branched at $y = \sqrt[3]{t}, \omega \cdot \sqrt[3]{t}, \omega^2 \cdot \sqrt[3]{t}$:

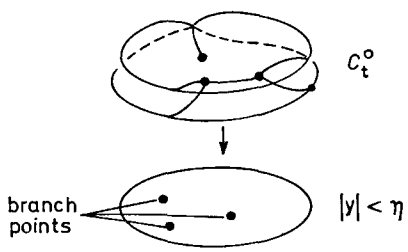


Figure 3

Topologically, the above surface with boundary is just a torus with a hole in it. Thus C_t, and its degeneration to C_0, looks like this:

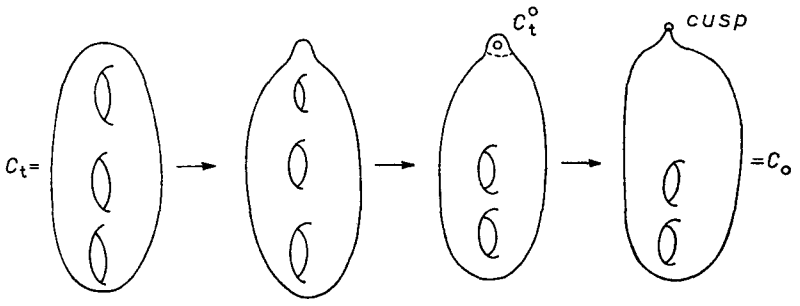


Figure 4

In other words, the cusp has swalled a whole infinitesimal elliptic curve!

REFERENCES

A. Borel
LAG – Linear algebraic groups (notes taken by H. Bass). Math. Lect. Notes series, Benjamin, 1969.

J. Fogarty
IT – Invariant theory. Math. Lect. Notes series, Benjamin, 1969.

A. Grothendieck & J. Dieudonné
EGA – Eléments de géométrie algébrique. Publ. Math. No. 4, . . ., Inst. Hat. Et. Sc., 1960, . . .

D. Mumford
GIT – Geometric invariant theory. Ergeb. Math. Bd. 34, Springer Verlag, 1965.

D. Mumford
IAG – Introduction to algebraic geometry (preliminary version of the first three chapters, lecture notes Harvard University).

(Oblatum 4–III–1971)

D. Mumford
Dept. Math.
Harvard University
2 Divinity Ave.
CAMBRIDGE, Mass., 02138
U.S.A.

K. Suominen
Dept. Math.
University of Helsinki
HALLITUSK 11–13
Finland