Proc. Indian Acad. Sci. (Math. Sci.), Vol. 91, Number 2, July 1982, pp. 73–122.
© Printed in India.

The fundamental group-scheme*

MADHAV V NORI
School of Mathematics, Tata Institute of Fundamental Research, Colaba, Bombay 400 005, India

MS received 2 November 1981

1. Introduction

Let X be a compact Riemann surface, $\tilde{X}$ a finite Galois unramified covering, with Galois group G. Let V be a vector space with G-action. The diagonal action of G on $\tilde{X} \times V$ is free and the quotient is a vector bundle W on X. It was shown by A Weil that there are two polynomials f and g with non-negative integer coefficients with $f \neq g$ and $f(V)$ isomorphic to $g(V)$. Isomorphism classes of vector bundles on X form a semi-ring with respect to direct sums and tensor products, so the expressions $f(V)$ and $g(V)$ make sense as vector bundles on X.

A vector bundle W on X satisfying this property is called *finite*. We prove the converse : a finite vector bundle W arises from a representation of the Galois group for a suitable unramified covering $\tilde{X} \to X$.

It is easy to see that a line bundle L is finite if and only if L is a point of finite order in the Jacobian of X. For such a line bundle, the function field of $\tilde{X}$ is just a simple Kummer extension of the function field of X. Thus our theorem for line bundles simply asserts that the characters of the etale fundamental group of X (which is the profinite completion of the topological fundamental group of X are in one-to-one correspondence with line bundles of finite order on X. This is, of course, a well-known fact, and a very useful one because the structure of the abelian group of all such line bundles is determined very easily by the topology of the Jacobian. Whereas it is not clear how to go about determining the finite bundles from the variety of stable bundles on X ; consequently our theorem has met with no utility.

If X is a complete connected reduced scheme over a field k, finite vector bundles still make sense. An essentially finite bundle is just a sub-quotient of W, remaining in the semi-stable category. If G is a finite group-scheme and P is a principal G-bundle on X, the representations of G give rise to essentially finite bundles on X and in fact all essentially finite bundles are obtained in this manner. In characteristic zero, finite = essentially finite.

This is the content of Chapter I.

* Ph.D. thesis submitted to University of Bombay.

While proving this, we show that there is an affine group-scheme $\pi(X, \chi_0)$ which is an inverse limit of finite group-schemes, a principal $\pi(X, \chi_0)$-bundle P on X, a base-point $*$ of P sitting above χ_0 which is a k-rational point of X with the following universal property : given a principal G-bundle Q on X with G being a finite group-scheme and V a base-point of Q above χ_0, there is a unique pair (f, ρ) such that

(i) $\rho : \pi(X, \chi_0) \rightarrow G$ is a homomorphism. (ii) $f : P \rightarrow Q$ interwines the actions of $\pi(X, \chi_0)$ and G, and (iii) $f(*) = V$.

Naturally we call $\pi(X, \chi_0)$ the fundamental group-scheme of X at χ_0.

This leads us to the questions : when does such a $(P, \pi(X, \chi_0), *)$ exist with the above universal property ? In characteristic zero, there is no problem at all : this is just the etale fundamental group.

In Chapter II, we show that $\pi(X, \chi_0)$ exists if X is connected and reduced (the completeness is not necessary). That some conditions on X are necessary was suggested by Milne who showed (in our language) that $\pi(X, \chi_0)_{ab}$ exists if and only if all members of $\Gamma(X, \mathbf{O}_X)$ integral over k belong to k (in particular, $\Gamma(X, \mathbf{O}_X)$ has no nilpotents). It seems unlikely that this $\pi(X, \chi_0)$ has the decent properties enjoyed by the usual fundamental group, e.g.,

A†. If $X \rightarrow S$ is a smooth proper morphism and S is not equi-characteristic then the fundamental group-schemes of the fibres certainly do not vary in a flat manner and this destroys some of the interest in this concept.

B. If $P \rightarrow X$ is a principal G-bundle on X with G a finite group-scheme, then P may not have a fundamental group-scheme at all !

On the positive side, we have :

A. A proper smooth morphism with connected fibres induces a surjection of fundamental group-schemes.

B. $\pi(X, \chi_0)$ is a birational invariant for smooth complete varieties.

C. It remains unaffected by the removal of a closed subset of codimension $\geqslant 2$ if the ambient space is regular.

D. $\pi(X, \chi_0)$ is trivial for normal rational varieties.

E. It remains invariant under base-change by separable extensions.

The existence of $\pi(X, \chi_0)$ and the proofs of the above statements are deal with in Chapter II.

In Chapter III we show that all the results of Chapter I are valid for parabolic bundles (which are a slight modification of the parabolic bundles defined and used by C S Seshadri). Thus we show that for a smooth projective connected curve X and a finite set $S \rightarrow X$, the representations of $\pi(X-S, \chi_0)$ are in one-to-one correspondence with essentially finite parabolic bundles on $X-S$.

In the final chapter we consider principal bundles on X with nilpotent structure-groups. In this context there is again a nilpotent affine group-scheme

† This was shown by M. Artin.

$U(X, \chi_0)$ and a principal bundle P with this structure group and a base-point having the obvious universal property. In characteristic zero, $U(X, \chi_0)$ is determined completely by its Lie algebra. In positive characteristic, however, $U(X, \chi_0)$ is an inverse limit of finite group-schemes and therefore a quotient of $\pi(X, \chi_0)$. We show that

A. $U(X, \chi_0)_{ab} = \varprojlim_{G \to \operatorname{Pic} X} \hat{G}$ where the G run through all local group-schemes embedded in Pic X (assuming that Pic X exists).

B. If X is an abelian variety, $U(X, 0)$ is abelian.

C. If X is an elliptic curve, $\pi(X, 0) \to \varprojlim_{G \to \hat{X}} \hat{G}$ is an isomorphism, where the G run through all finite sub-group-schemes of X.

Equivalently, if P is a principal G-bundle on X with a base-point v above the zero of X and G is a finite group-scheme, then there is a homomorphism $\rho : X_n \to G$ for some n and a commutative diagram :

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "n"'] & & P \arrow[dl] \\ & X & \end{tikzcd}$$

such that f intertwines the X_n-action on X and the action of G on P.

We fail to prove however that this holds for abelian varieties.

D. Invariance under arbitrary field extensions.

The remaining part of the chapter is devoted to a preliminary study of $U(X, \chi_0)$ for curves X in positive characteristic. We find that the $U(X, \chi_0)$ are determined by "non-commutative formal groups" which are defined there. A classification of such objects presents an interesting problem. We then compute $U(X, \chi_0)$ for rational curves with rather simple singularities, and also prove an old result of Safarevich.

The appendix gives an easy proof for the results about Tannaka Categories stated in Chapter I, § 1.

Literature referred to is mentioned at the end of each chapter.

Chapter I is a reproduction of "Representations of the Fundamental Group" which appeared in *Compositio Math.*, 1976, Vol. 33. It has been included here for the sake of completeness. Several conventions introduced in Chapter I have been adhered to throughout.

* A new proof of the theorem on Tannaka categories has also appeared in Springer Verlag Lecture Notes 900.

PART I

CHAPTER 1

2. On the Representations of the Fundamental Group

2.1. *Tannaka categories*

Let G be an affine group-scheme defined over a field k, R its coordinate ring, and G-mod the category of finite-dimensional left representations of G. Let k-mod be the category of finite-dimensional k-vector spaces, and $T_k : G\text{-mod} \to k\text{-mod}$ the forgetful functor. Let $\hat{\otimes}$ ($\otimes$ resp.) denote the usual tensor product functor on G-mod (k-mod resp.). Let L_0 be the trivial representation of G.

Putting $(G\text{-mod}, \hat{\otimes}, T_k, L_0) = (\mathcal{C}, \hat{\otimes}, T, L_0)$, we note that the following statements are true :

$\mathcal{C}1$: $\mathcal{C}$ is an abelian k-category (existence of direct sums of finite object of $\mathcal{C}$ included).

$\mathcal{C}2$: Obj $\mathcal{C}$ is a set.

$\mathcal{C}3$: $T : \mathcal{C} \to k\text{-mod}$ is a k-additive faithful exact functor.

$\mathcal{C}4$: $\hat{\otimes} : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ is a functor which is k-linear in each variable, and $T \circ \hat{\otimes} = \otimes \circ (T \times T)$.

$\mathcal{C}5$: $\hat{\otimes}$ is associative, preserving T, in the following sense : Let $H : \hat{\otimes} \circ (I_{\mathcal{C}} \times \hat{\otimes}) \to \hat{\otimes} \circ (\hat{\otimes} \times I_{\mathcal{C}})$ be the equivalence of functors that give the associativity of $\hat{\otimes}$. For objects V_1, V_2, V_3 of $\mathcal{C}$, $T(H(V_1, V_2, V_3))$ gives an isomorphism of $TV_1 \otimes (TV_2 \otimes TV_3)$ with $(TV_1 \otimes TV_2) \otimes TV_3$. We ask that this isomorphism coincides with the usual one that gives the associativity of the tensor product for vector spaces.

$\mathcal{C}6$: $\hat{\otimes}$ is commutative, preserving T, in the above sense.

$\mathcal{C}7$: There is an object L_0 of $\mathcal{C}$, and an isomorphism $\varphi : k \to TL_0$, such that L_0 is an identity object of $\hat{\otimes}$, preserving T.

$\mathcal{C}8$: For every object L of $\mathcal{C}$ such that TL has dimension equal to one, there is an object L^{-1} such that $L \hat{\otimes} L^{-1}$ is isomorphic to L_0.

Any $(\mathcal{C}, \hat{\otimes}, T, L_0)$ shall be called a Tannaka category.

Definition : Let $\mathcal{C}$ be any category where $\mathcal{C}1$ and $\mathcal{C}2$ hold. Let S be a subset of Obj $\mathcal{C}$. Then

$$\bar{S} = \{W \in \operatorname{Obj} \mathcal{C} : \exists\, P_i \in S,\ 1 \leqslant i \leqslant t, \text{ and } V_1, V_2 \in \operatorname{Obj} \mathcal{C} \text{ such that } V_1 \subseteq V_2 \subseteq \bigoplus_{i=1}^{t} P_i, \text{ and } W \text{ is isomorphic to } V_2/V_1\}.$$

By $\mathcal{C}(S)$, we mean the full subcategory of $\mathcal{C}$ with Obj $\mathcal{C}(S) = \bar{S}$. Note that $\mathcal{C}(S)$ is also an abelian category. Finally, S will be said to generate $\mathcal{C}$ if obj $\mathcal{C} = \bar{S}$. The following theorems are due to Saavedra (see Theorem 1 of Saavedra [4]).

Theorem (1.1) : Any Tannaka category is the category of finite-dimensional left representations of an affine group-scheme G, and this sets up a bijective correspondence between affine group-schemes and Tannaka categories.

Theorem (1.2) : A group-scheme G is finite if and only if there exists a finite collection S of G-representations which generates G-mod (in the sense of the above definition).

Theorem (1.3) : Any homomorphism of Tannaka categories from (G-mod, $\hat{\otimes}$ T_k, L_0) to (H-mod, $\hat{\otimes}$, T_k, L_0) is induced by a unique homomorphism (of affine algebraic group schemes) from H to G.

2.2. *Principal bundles*

Let X be a nonempty k-prescheme, $S(X)$ the category of quasi-coherent sheaves on X, $\otimes : S(X) \times S(X) \to S(X)$ the tensor product functor on sheaves.

Let G be an affine group scheme defined over k.

Recall that $j : P \to X$ is said to be a principal G-bundle on X if

(a) j is a surjective flat affine morphism.

(b) $\Phi : P \;\, G \to P$ defines an action of G on P such that $j \cdot \bar{\phi} = j \cdot p_1$.

(c) $\Psi : P \times G \to P \times_X P$ by $\Psi = (p, \Phi)$ is an isomorphism.

In this case, $\mathscr{F} \to j^* (\mathscr{F})$ gives an isomorphism of $S(X)$ with the category of G-sheaves on P, by the method of flat descent (see Grothendieck [2]). Every left representation V of G gives rise to a G-sheaf on P in a natural way, and by taking G-invariants, one gets a sheaf on X, denoted by $F(P)V$. This gives rise to a functor $F(P) : G\text{-mod} \to S(X)$, and putting $F = F(P)$, we note that the following are true :

F_1 : F is a k-additive exact functor ; $F_2 : F \circ \hat{\otimes} = \otimes \circ (F \times F)$; F_3 : The obvious statements parallel to $\mathscr{C}5$, $\mathscr{C}6$, $\mathscr{C}7$; in particular, $FL_0 = \mathbf{O}_X$, where L_0 is the trivial representation, and finally ; F_4 : If rank $V = n$, then FV is locally free of rank n ; in particular, F is faithful.

From now on, F will denote a functor where $F1$ to $F4$ held.

Let G-mod be the category of all (possibly infinite-dimensional) left representations of G.

Lemma (2.1) : There is a unique functor $\overline{F} : G\text{-mod} \to \mathscr{S}(X)$, such that :

(i) The statements $F1$, $F2$, $F3$ hold good for $\overline{F}$, (ii) $\overline{F} \mid G\text{-mod} = \overline{F}$, (iii) $\overline{F}V$ is flat for all V, and faithfully flat if $V \neq 0$, and (iv) $\overline{F}$ preserves direct limits.

Proof : Define $\overline{F}V$ to be the direct limit of FW, where W runs through the collection of finite-dimensional G-invariant sub-spaces of V, and the lemma is then easily checked. We will put $\overline{F} = F$ from now on.

Lemma (2.2) : F induces a functor from affine G-schemes to affine X-preschemes.

Proof : Let $Y = \operatorname{spec} A$ be a scheme on which G operates, and let $m : A \otimes A \to A$ be the multiplication map on A. Since A is a commutative, associative k-algebra with identity, by $F2$ and $F3$, we deduce that FA is a commutative, associative sheaf of $\mathbf{O}_X$-algebras with identity. This is enough to conclude that there is an affine morphism $j : Z \to X$ such that $j_* (\mathbf{O}_Z)$ is isomorphic to FA as a sheaf of $\mathbf{O}_X$-algebras. We shall denote Z by FY from now on.

Definition : Let G operate on itself by the left. Put $P(F) = FG$, and let $j : P(F) \to X$ be the canonical morphism. Since no confusion is likely to arise, we shall denote $P(F)$ simply by P.

Lemma (2·3) : P is a principal G-bundle on X.
Proof : By definition, j is an affine morphism. That j is flat and surjective follows from the fact that $j_* (\mathbf{O}_P)$ is faithfully flat. ((iii) of Lemma 2·1). Properties (*b*) and (*c*) will be checked later.
Lemma (2·4) : If Y and Z are schemes on which G operates, $F(Y \times Z) = FY \times_X FZ$. Furthermore, if G acts trivially on Y, then $FY = X \times Y$.
Proof : Obvious.

Proof of Lemma (2·3) : We denote by G' the same scheme as G, equipped with the trivial action of G. Let $\varphi : G \times G' \to G$ be the multiplication map of G, and $\psi : G \times G' \to G \times G$ be given by $\psi(x, y) = (x, \varphi(x, y))$. Note that φ and ψ are both G-morphisms ; consequently there are X-morphisms

$$\Phi = F \quad : P \times G \to P, \text{ and}$$

$$\Psi = F\psi : P \times G \to P \times_X P.$$

Since φ defines an action of G' on G, Φ defines an action of G on P, and $j \circ p_1 = j \circ \bar{\Phi}$ simply because Φ is an X-morphism.

Also, ψ is an isomorphism, from which it follows that Ψ is an isomorphism too, thus concluding the proof of the lemma.

Now that we have constructed a principal bundle P, given a functor F, the next step is to show that F is the functor naturally associated with P, that is:

Proposition (2·5) : $F = F(P)$.

We introduce some notation first. Let Z be a scheme on which G operates on the right, and let V be any left representation of G. We denote by V_Z the sheaf $V \otimes \mathbf{O}_Z$ equipped with the following action of $G : g(v \otimes f) = gv \otimes f \circ \rho(g)$, where $v \in V$, $g \in G$, and $f \in \Gamma(U, \mathbf{O}_Z)$, for some open U in Z. This is the natural construction of a G-sheaf on Z, given a representation V, mentioned in the beginning of the section.

To show that two sheaves are isomorphic on X, it suffices to prove that the inverse images are isomorphic as G-sheaves on P, and hence the above proposition is reduced to the following :

Lemma (2·6) : There is a functorial isomorphism (of G-sheaves) of $j^* (FV)$ with V_P.

We require the aid of

Lemma (2·7) : Let Y be an affine scheme on which G operates on the left, H operates on the right. Assuming the actions of G and H on Y commute with each other, let $Z = FY$. Then Z is a H-scheme, and $j : Z \to X$ is a H-morphism, where X has the trivial action of H. Furthermore, F induces a functor F

from the category of sheaves on Y with commuting G and H action to the category of H sheaves on Z.

The proof of Lemma 2·7 is trivial, and we omit it. To apply the Lemma, put $G = H = Y$, with the actions of G ard H on Y being given by left and right translations respectively.

Let V be a representation of G and V' its underlying vector space equipped with the trivial action of G. Therefore, there are G-sheaves, V_G and V'_G (corresponding to the right action of G) on G. We shall define left actions of G on V_G and V'_G as follows :

(a) $g(v \otimes f) = v \otimes f \circ L_g^{-1}$, for $v \in V, g \in G$, and $f \circ \Gamma(U, O_G)$,

(b) $g(v \otimes f) = gv \otimes f \circ L_g^{-1}$, for $v \in V', g \in G$, and $f \circ \Gamma(U, O_G)$.

With F as in Lemma 2·7, it is trivial to check that $F(V_G) = V_P$ and $F(V'_G) = j^*(FV)$. To prove Lemma 2·6, it therefore suffices to prove

Lemma (2·8) : There is a functorial isomorphism of V with V'_G as sheaves on G, with G acting both on the left and the right.

Proof : Let W be any vector space. We denote the scheme spec $(S(W^*))$ again by W. Then the sheaf $W \otimes O_G$ can be identified canonically with the sheaf of morphisms from G to the scheme W.

Using this identification, define $\lambda : V'_G \to V_G$ by $\lambda(f)(g) = g^{-1}f(g)$, where $g \in G, f : G \to V'$. The map furnishes the required isomorphism, thus concluding the proof of Prop. 2·5.

Proposition (2·9) : There is a bijective correspondence between principal G-bundles on X and functors $F : G\text{-mod} \to \mathcal{S}(X)$ such that $F1$ to $F4$ hold. Furthermore,

(a) Let $f : Y \to X$ be a morphism, and assume that $F = G\text{-mod} \to S(X)$ satisfies $F1$ to $F4$. Then $F1$ to $F4$ hold good for $f^* \circ F$ also, and $P(f^* \circ F) = f^*(P(F))$; (b) Let $X = \text{spec } k$, and $F : G\text{-mod} \to k\text{-mod}$ the forgetful functor. Then $P(F) = G$; (c) Let $\rho : H \to G$ be a morphism of affine group schemes. Let P be a principal H-bundle on X, and P' the quotient of $P \times G$ by H. Let R : $G\text{-mod} \to H\text{-mod}$ be the restriction functor. Then $F(P) \circ R = F(P')$.

Proof : (b) is trivial, and (a) and (c) are proved by chasing the construction of $P(F)$.

Remark : The condition $F4$, which is crucial in proving that $j : P \to X$ is flat and surjective, is actually a consequence of $F1$, $F2$ and $F3$. However, we do not need this fact.

2·3. *Essentially finite vector bundles*

Let X be a complete connected reduced k-scheme, where k is a perfect field. Let vect(X) denote the set of isomorphism classes, $[V]$, of vector bundles V, on X. Then vect(X) has the operations :

(a) $[V] + [V'] = [V \otimes V']$, and

(b) $[V] \cdot [V'] = [V \times V']$.

In particular, for any vector bundle V on X, given a polynomial f with non-negative integer coefficients, $f(V)$ is naturally defined.

Let $K(X)$ be the Grothendieck group associated to the additive monoid Vect (X) ; this is not the usual Grothendieck ring of vector bundles on X, since $0 \to V' \to V \to V'' \to 0$ exact does not imply that $[V'] + [V''] = [V]$.

The Krull–Schmidt–Remak theorem holds, since $H^\circ(X, \text{end } V)$ is finite-dimensional. In particular, $[W]$, where W runs through all indecomposable vector bundles on X, form a free basis for $K(X)$.

Definition : For a vector bundle V, $S(V)$ is the collection of all the indecomposable components of $V^{\otimes n}$, for all non-negative integers n.

Lemma (3.1) : Let V be a vector bundle on X. The following are equivalent :
(a) $[V]$ is integral over Z in $K(X)$; (b) $[V] \otimes 1$ is integral over Q in $K(X) \otimes Q$; (c) There are polynomials f and g with non-negative integer coefficients such that $f(V)$ is isomorphic to $g(V)$ and $f \neq g$.
(d) $S(V)$ is finite.

Proof :

(a) $\Leftrightarrow$ (b) holds merely because $K(X)$ is additively a free abelian group.

(c) $\Rightarrow$ (b) is obvious.

(b) $\Rightarrow$ (c) : Let $h \in Z[t]$ such that $h([V]) = 0$, and $h \neq 0$. Choose $f, g \in Z[t]$ such that f and g have non-negative coefficients, and $h = f - g$. Then $[f(V)] = [g(V)]$ in $K(X)$, but vect (X), as a monoid, has the cancellation property, so it follows that $f(V)$ is actually isomorphic to $g(V)$.

(d) $\Rightarrow$ (a) : The abelian subgroup of $K(X)$ with basis as $S(V)$ is certainly stable under multiplication by $[V]$.

(a) $\Rightarrow$ (d) : Simply note that if m is the degree of a monic polynomial h such that $h([V]) = 0$, then any member of $S(V)$ is actually an indecomposable component of $V^{\otimes r}$ for some r lying between 0 and $m - 1$.

Definition : A vector bundle V on X is said to be finite if it satisfies any of the equivalent hypothesis of Lemma 3·1.

Lemma (3.2) :
(i) V_1, V_2 finite $\Rightarrow$ $V_1 \oplus V_2$, $V_1 \otimes V_2$, V_1^* finite.
(ii) $V_1 \oplus V_2$ finite $\Rightarrow$ V_1 finite.
(iii) A line bundle L is finite $\Leftrightarrow$ $L^{\otimes m}$ is isomorphic to $\mathbf{O}_X$ for some positive integer m.

Proof :
(1) is obvious.
(2) follows from the fact that $S(V_1)$ is contained in $S(V_1 \oplus V_2)$.
(3) follows from the fact that $S(L) = \{L^{\otimes m} : m \geqslant 0\}$.

Lemma (3.3) : Let X be a smooth projective curve. For a vector bundle V, let $C(V) = \sup\{\mu(W) = \deg W/rkW,\ 0 \neq W \subseteq V\}$.
Then, (a) $C(V)$ is finite, and
(b) if $0 \to V' \to V \to V'' \to 0$ is an exact sequence of vector bundles on X, $C(V) \leqslant \max(C(V'), C(V''))$.

Proof : That $D(V) = \sup\{\deg L : L \subset V,\ L \text{ a line bundle}\}$ is finite is well-known. Since $C(V) \leqslant \max\{D(\Lambda^r(V))/r : 1 \leqslant r \leqslant rk\, V\}$, (a) follows.

Given an injection $j : W \to V$ and an exact sequence $0 \to V' \to V \to V'' \to 0$, there is a canonical factoring :

$$\begin{tikzcd}
0 \arrow[r] & W' \arrow[r] \arrow[d, dash, "j'"'] & W \arrow[r] \arrow[d, dash, "j"'] & W'' \arrow[r] \arrow[d, dash, "j''"'] & 0 \\
0 \arrow[r] & V' \arrow[r] & V \arrow[r] & V'' \arrow[r] & 0
\end{tikzcd}$$

such that the horizontal rows are exact, and j', j'' are generic injections. Let U', U'' be the sub-bundles of V', V'' respectively, such that $j'(W') \subseteq U'$ and $j''(W'') \subseteq U''$, and $rkW' = rkU'$ and $rk\, W'' = rk\, U''$. Then $\deg W' \leqslant \deg U'$ and $\deg W'' \leqslant \deg U''$.

Now,

$$\begin{aligned}
\mu(W) &= \deg W' + \deg W''/rk\, W' + rk\, W'' \\
&\leqslant \deg U' + \deg U''/rk\, U' + rk\, U'' \\
&\leqslant \max(\deg U'/rk\, U', \deg U''/rk\, U'') \\
&\leqslant \max (C V'), C(V''),
\end{aligned}$$

which proves (b).

Proposition (3·4) : Any finite vector bundle V on a smooth projective curve X is semistable of degree zero.

Proof : By Lemma 3·3, $C(V^{\otimes m}) \leqslant \sup\{C(W) : W \in S(V)\} = T(V)$, which is finite, since $S(V)$ is a finite collection. Consequently, for any sub-bundle W of V, $W \neq 0$, since $W^{\otimes m}$ is a sub-bundle of $V^{\otimes m}$, $\mu(W^{\otimes m}) \leqslant T(V)$, for all non-negative integers m. But a simple calculation shows that $\mu(W^{\otimes m}) = m\mu(W)$ which obviously implies that $\mu(W) \leqslant 0$.

In particular, since both V and V^* are finite, $\mu(V) \leqslant 0$ and $\mu(V^*) = -\mu(V) \leqslant 0$. Therefore we have shown that

(a) $\mu(V) = 0$, and

(b) for all sub-bundles W of V, $W \neq 0$, $\mu(W) \leqslant 0$.

For the rest of this section, X will be a complete, connected, reduced scheme and the phrase "a curve Y in X" is to be interpreted as a morphism $f : Y \to X$, where Y is a smooth, connccted, projective curve, and f is a birational morphism onto its image.

Definition : A vector bundle on X is semistable if and only if it is semistable of degree zero restricted to each curve in X.

Since the restriction of a finite vector burdle is also finite, we have the following obvious corollary :

Corollary (3·5) : A finite vector bundle on X is semistable.

Lemma : (3·6) :

(a) If V is a semistable vector bundle on X and W is either a sub-bundle or a quotient bundle of V, such that W/Y has degree zero for each curve Y in X, then W is semistable.

(b) The full subcategory of $\mathcal{S}(X)$ with objects as semistable vcctor bundles on X is an abelian category.

Proof :

(a) Under the given hypothesis, it follows that $W \mid Y$ is semistable of degree zero, and therefore W is semistable.

(b) Let V and W be semistable vector bundles on X, and let $f : V \rightarrow W$ be a morphism. For a geometric point x : spec $\bar{k} \rightarrow X$, let $r(x)$ be the rank of the morphism $x^*(f) : x^*(V) \rightarrow x^*(W)$. Then, by elementary degree considerations $r(x)$ is a constant restricted to each curve, and since X is connected, $r(x)$ is constant globally. Now, since X is reduced, it follows that ker f and coker are locally free, and moreover, (ker f)$\mid Y$ = ker ($f \mid Y$) and (coker f)$\mid Y$ = coker (f / Y), and both these bundles are semistable of degree zero on Y ; the lemma follows.

Definition : We shall denote by $SS(X)$ the full subcategory of $S(X)$ with semistable vecor bundles as objects. Let F be the collection of finite vector bundles, regarded as a subset of obj $SS(X)$, and let $EF(X)$ be the full subcategory of $SS(X)$ with obj $EF(X) = \bar{F}$, where the meaning of $\bar{F}$ is to be taken in the sense of § 1. The objects of $EF(X)$ will be essentially called finite vcctor bundles.

Proposition (3·7) :

(a) If V is an essentially finite vector bundle on X, and W is either a subbundle or a quotient bundle of V such that $W \mid Y$ has degree zero for each curve Y in X, then W is essentially finite. (b) $EF(X)$ is an abelian category. (c) If V_1 and V_2 are essentially finite, so are $V_1 \otimes V_2$ and V^*.

Proof : (a) and (b) are obvious consequences of Lemma 3·6. To prove (c), choose W_i and P_i such that

(i) W_i is finite, (ii) P_i is a sub-bundle of W_i and P_i is semistable, and (iii) V_i a quotient of P_i, for $i = 1, 2$.

Then

(i) $W_1 \otimes W_2$ is finite by Lemma 3.2, (ii) $P_1 \otimes P_2$ is a sub-bundle of $W_1 \otimes W_2$, and (iii) $V_1 \otimes V_2$ is a quotient of $P_1 \otimes P_2$.

Both $P_1 \otimes P_2$ and $V_1 \otimes V_2$ are of degree zero restricted to each curve in X ; consequently, by (a), both $P_1 \otimes P_2$ and $V_1 \otimes V_2$ are essentially finite.

In a similar fashion, one proves that the dual of an essentially finite vector bundle is essentially finite.

Proposition (3·8) : Let G be a finite group scheme, and $j : X' \rightarrow X$ a principal G-bundle. Then, for the functor $F(X')$: G mod $\rightarrow S(X)$, $F(X')$ V is always an essentially finite vector bundle.

Proof : We shall show that $F(X').V$ is of degree zero restricted to each curve. For this, we assume that X itself is a smooth projective curve. Let R be the coordinate ring of G, and n the vector space dimension of R. Then, n deg $(F(X')\, V)$ = deg $(j^*(F(X')\, V)$; but $j^*(F(X')\, V)$ is, by definition, a trivial vector bundle on X', and therefore deg $(F(X')\, V)$ is equal to zero. Note that " degree " makes sense even if X' is ot reduced, by looking at Hilbert polynomials.

Now, any representation V of G can be embedded (injectively) in $R \oplus R \cdots \oplus R$, and therefore $F(X')\,V$ is contained in a direct sum of several copies of $F(X')\,R$. To prove that $F(X')\,V$ is essentially finite, it would surffice to show that $F(X')\,R$ is finite, by (a) of Prop. 3·7. But $R \otimes R$ is isomorphic to $R \oplus R \oplus \ldots \oplus R$ n times, from which, if $W = F(X')\,R$, $[W]^2 = n\,[W]$, concluding the proof of the proposition.

For the rest of this section, we shall fix a k-rational point x of X and denote by $x^* : S(X) \to |\,k\,|$ the functor which associates to a sheaf on X its fibre at the point x. Note that x^* is faithful and exact when restricted to the category of semistable bundles. It is now obvious that $(EF(X), \otimes, x^*, O_X)$ is a Tannaka category. By Theorem 1·1, this determines an affine groups scheme G such that $|\,G\,|$ can be identified with $EF(X)$ in such a way that x^* becomes the forgetful functor. We shall call the group-scheme G above the fundamental group-scheme of X at x, and denote it by $\pi(X, x)$.

For a subset S of obj $EF(X)$, let $S^* = \{V^* : V \epsilon S\}$. Let $S_1 = S \cup S^*$ and $S_2 = \{V_1 \otimes V_2 \otimes \cdots \otimes V_m : V_i \in S_1\}$. Let obj $EF(X, S) = \bar{S}_2$. As before, this determines an affine group scheme which we call $\pi(X, S, x)$, such that

$$G_S : EF(X, S) \to |\,\pi(X, S, x)\,|^*$$

is an equivalence of categories. Let F_S be the inverse of G_S ; then F_S can be regarded as a functor from $|\,\pi(X, S, x)\,|$ to $S(X)$ such that the composite x^*. F_S is the forgetful functor. In particular, by Prop. 2.9, there is a principal $\pi(X, S, x)$-bundle $\tilde{X}_S$ such that $F_S = F(\tilde{X}_S)$. By Prop. 2·9 (a), the functors $x^* \cdot F_S$ and $F(\tilde{X}_S \mid x)$ coincide, and by Prop. 2.9 (b), there is a natural isomorphism of $\tilde{X}_S \mid x$ with G (as G-spaces), which is equivalent to specifying a k-rational base point $\tilde{x}_s$ of $X_S \mid x$.

Now, if S is a subset of Q, there is a natural homomorphism of Tannaka categories from $EF(X, S)$ to $EF(X, Q)$, which by Theorem 1.3, determines a natural homomorphism ρ^Q_S from $\pi(X, Q, x)$ to $\pi(X, S, x)$, and by Prop. 2.9 (c), it follows that X_S is induced from X_Q by the homomorphism ρ^Q_S.

Lemma (3·9) : Let S be a finite collection of finite vector bundles. Then $\pi(X, S, x)$ is a finite group scheme.

Proof : Let W be the direct sum of all the members of S and their duals. Then W is a finite vector bundle, and by Lemma 3.1, $S(W)$ is finite. Note that $S(W)$ generates the abelian category $EF\,(X, S)$ in the sense of § 1, and therefore, by Theorem 1.2, $\pi(X, S, x)$ is a finite group-scheme.

Proposition (3 .10) : Let S be any finite collectior of essentially finite vector bundles. Then, there is a principal G-bundle X' on X, with G a finite groud scheme, such that the image of $F(X')$: G and $\to S(X)$ contains the given collection S.

Proof : For each $W \in S$, choose V such that W is a quotient of a semistable sub-bundle of V and V a finite vector bundle. Let Q be the collection of V as constructed, and note that S is a subset of obj $EF(X, Q)$.

Put $G = \pi\,(X, Q, x)$, and $X' = \tilde{X}_Q$. By Lemma 3.9, G is a finite group-scheme. Let G_Q, as above, be the equivalence of categories, from $EF(X, Q)$ to $|\,\pi(X, Q, x)\,|$, and then, we know that $F(X')$. $G_Q(V) = V$, for all objects V of $EF(X, Q)$, thus proving the proposition.

[*] $|\,\pi(X, S, x)\,|$ denote the cotegory of $\pi\,(X, S, x)$-modules.

For $S =$ obj $EF(X)$, we shall denote $\tilde{X}_S$, G_S, F_S, $\tilde{x}_S$ by $\tilde{X}$, G, $\tilde{F}$, $\tilde{x}$ respectively.

Definition : The principal $\pi(X, x)$-bundle $\tilde{X}$ is the universal covering scheme of X.

The universal property possessed by $\pi(X, x)$ and $\tilde{X}$ is given by the following :

Proposition (3.11) : Let (X', G, u) be a triple, such that X' is a principal G-bundle on X, u a k-rational point in the fibre of X' over X, and G is a firite group scheme.

Then there is a unique homomorphism $\rho : \pi(X, x) \to G$, such that

(a) X' is induced from $\tilde{X}$ by the homomorphism ρ, and

(b) the image of $\tilde{x}$ ir X' is u.

Consequently, there is a bijective correspondence of the above triples with homomorphisms $\rho : \pi(X, x) \to G$.

Proof : By Prop. 3.8, $F(X')$ is a functor from mod-G to $EF(X)$. Now $EF(X)$ is identified with $|\pi(X, x)|$ in such a way that the forgetful functor T_k on $|\pi(X, x)$ is equivalent to the functor x^* from $EF(X)$ to $|k|$. Thus, the composite $T_k \cdot F(X')$ is simply $x^* \cdot F(X') = F(X' \mid x)$, by Prop. 2·9 (a). Now, the k-rational point u of $X' \mid x$ gives a unique isomorphism $\varphi : G \to X' \mid x$ of principal homogeneous spaces such that $\varphi(1) = u$. By Prop. 2·9 (b), φ determines a ratural equivalence of the functor $F(X' \mid x)$ with the forgetful functor from mod-G $\to$ mod-k. This information yields a morphism (of Tannaka categories) from mod-G to $\pi(X, x)\,|$, which, by Theorem 1·3, is induced by a homomorphism $\rho : \pi(X, x) \to G$. We now appeal to Prop. 2·9 (c) to settle the fact that X' isindeed induced from $\tilde{X}$ by ρ, and that the image of $\tilde{x}$ ir X' is u. The uniqueness of ρ is easily checked.

3. Conclusion

(1) With S as in Lemma 3·9, assume that $|\pi(X, S, x)|$ is a semi-simple category. Then, for any representation W of $\pi(S, X, x)$, there exist polynomials f and g, with $f \neq g$, the coefficients of f and g being non-negative integers, such that $f(W)$ and $g(W)$ are isomorphic. This follows from the fact that there are only finitely indecomposable representations of $\pi(X, S, x)$ up to isomorphism. Putting $V = F(X_S)\, W$, it follows that V-is a finite vector bundle.

In characteristic zero, any finite group scheme is reduced, and its representations certainly form a semi-simple category. By Prop. 3·10, it follows therefore that in characteristic zero, any essentially finite vector bundle is finite.

(2) The structure of the fundamental group-scheme :

(a) For $S \subseteq Q \subseteq$ obj $EF(X)$,

$$\rho^Q_S : \pi(X, Q, x) \to \pi(X, S, x) \text{ is surjective.}$$

(b) $\pi(X, x)$ is the inverse limit of $\pi(X, S, x)$, where S runs through all finite collections of finite bundles on X ; consequently $\pi(X, x)$ is the inverse limit of finite group schemes.

Both (a) and (b) follow from standard facts about Tannaka categories (Saavedra Rivano 1972).

CHAPTER II

The fundamental group-scheme

We shall always assume that the base-field k has characteristic $p > 0$.

Propositions 1 and 2 examine the existence of the fundamental group-scheme of a k-scheme $\mathscr{X}$ with a k-rational base-point χ_0. The results of Chapter I are re-interpreted in Proposition 3. Proposition 4 studies the dependence of $\pi(\mathscr{X}, \chi_0)$ on the base-point χ_0. Proposition 5 shows that $\pi(\mathscr{X}, \chi_0)$ is well behaved under base-change by separable algebraic extensions of the ground field.

This is the content of § 1.

In § 2 we show that the fundamental group-scheme is a birational invariant for smooth complete varieties. This involves a "purity of branch-locus" theorem (see Proposition 7). Finally we show that $\pi(X, \chi_0)$ is trivial for normal complete rational varieties.

§ 1. $\mathscr{X}$ is a k-scheme and χ_0 : spec $k \to \mathscr{X}$ is a morphism.

Consider the following category $\mathcal{C}$: the objects are triples (Q, G, V) where Q is a principal G-bundle on $\mathscr{X}$, G is a finite group-scheme and V is a k-rational point of Q sitting above χ_0.

A morphism $(f, g) : (Q, G, V) \to (Q', G', V')$ is a homomorphism $g : G \to G'$ and a morphism $f : Q \to Q'$ that intertwines the G and G' actions on Q and Q' and in addition, $f(V) = V'$.

By $\mathcal{C}^1$ we shall denote the category of all triples (Q, G, V) as above, except that G is now an inverse limit of finite group-schemes.

Definition 1 : $\mathscr{X}$ has a fundamental group-scheme $\pi(\mathscr{X}, \chi_0)$ if there is a triple $(P, \pi(\mathscr{X}, \chi_0), *)$ in the category $\mathcal{C}'$ such that for each object (Q, G, V) of $\mathcal{C}'$, there is a unique morphism from $(P, \pi(\mathscr{X}, \chi_0), *)$ to (Q, G, V).

Remark : Clearly it suffices to check the above for all (Q, G, V) in $\mathcal{C}$ to ensure that it holds for all (Q, G, V) in $\mathcal{C}^1$.

Definition 2 : $\mathscr{X}$ has $\mathscr{P}$ if whenever $(f_i, \rho_i) : (Q_i, G_j, V_i) \to (Q, G, V)$ for $i = 1, 2$ are morphisms in $\mathcal{C}$, then

$$(Q_1 \times_Q Q_2\ G_1 \times_G G_2,\ v_1 \times v_2) = (Z, H, w) \text{ is an object of } \mathcal{C}.$$

We have :

Proposition 1 : $\mathscr{X}$ has a fundamental group-scheme if and only if X has $\mathscr{P}$.

Proposition 2 : If $\mathscr{X}$ is reduced, and connected, then $\mathscr{X}$ has a fundamental group-scheme.

First we need

Lemma 1 : With $Q_i, G_i, V_i, \rho_i, Z, H, w$ as in Definition 2, Z is a principal H-bundle on a closed sub-scheme R of $\mathscr{X}$ containing x_0.

Proof of Lemma 1

$Z = Q_1 \text{x}_Q Q_2$ is a closed sub-scheme of $T = Q_1 \text{x}_X Q_2$ which is a principal $(G_1 \times G_2)$-bundle on $\mathscr{X}$. Let q_i be the composite $T \xrightarrow{f_i} Q_i \to Q$ for $i = 1, 2$. Because Q is a principal G-bundle on $\mathscr{X}$, there is a unique $z : T \to G$ such that $q_1 = q_2\, z$. If $e \to G$ represents the identity of G, clearly $Z = z^{-1}(e)$.

Also theie is a commutative diagram :

$$\begin{tikzcd}
T \times G_1 \times G_2 \arrow[r] \arrow[d, "z \times 1_{G_1} \times 1_{G_2}"'] & T \times_X T \arrow[d, "z \times z"] \\
G \times G_1 \times G_2 \arrow[r, "h"] & G \times G
\end{tikzcd}$$

where the first horizontal arrow induces $(p, g) \to (p, pg)$ for $p \in \operatorname{Mor}(S, T)$, $g \in \operatorname{Mor}(S, G_1 \times G_2)$, and h induces $(g, g_1, g_2) \to (g, \rho_2 (g_2)^{-1} g \rho_1 (g))$ for all $g_1 \in \operatorname{Mor}(S, G_1)$, $g_2 \in \operatorname{Mor}(S, G_2)$ and $g \in \operatorname{Mor}(S, G)$.

Now $h^{-1} (e \times e) = e \times H$, and taking inverse images in the vertical arrows, we see that the first horizontal arrow restricts to an isomorphism $Z \times H \to Z \times_x Z$. In particular Z is stable under the H-action on T; this action, being free, makes Z a principal H-bundle on $R = Z/H$ which is a closed sub-scheme of T/H. only remains to show that $R \to X$ is a closed immersion.

Consider the commutative diagram :

$$\begin{tikzcd}
Z \times H \arrow[r, "\cong"] \arrow[d, "j \circ \rho_1"'] & Z \times_X Z \arrow[d, "j \times j"] \\
R \arrow[r, "\Delta"] & R \times_X R
\end{tikzcd}$$

where $j : Z \to R$ is the given morphism and $\rho_1 : Z \times H \to Z$ is the projection. The morphism $j \times j$ makes $zx_X Z$ a principal bundle on $Rx_X R$ with the obvious action of $H \times H$ on the right. The right action of $H \times H$ on $Z \times H$ given by $(p, h) \cdot (h_1, h_2) = (ph_1, h_1^{-1} h h_2)$ for all $p \in \operatorname{Mor}(S, Z)$, h, h_1 and $h_2 \in \operatorname{Mor}(S, H)$ clearly makes $Z \times H$ a principal bundle on R. Moreover $Z \times H \to Z x_X Z$ preserves the $H \times H$ action. It follows that Δ is an isomorphism.

It is a trivial matter to check that a finite morphism $A \to B$ is a closed immersion if and only if the diagonal $A \overset{\Delta}{\to} A \times_B A$ in an isomorphism. So this proves that $R \to X$ is a closed immersion, finishing the proof of the lemma.

With z as above $W = Z^{-1} (G_{\mathrm{loc}})$ is an open and closed sub-scheme of T. But $\pi : T \to X$ is flat implying that $\pi (W) = X$ if X is connected. We have seen that $z^{-1} (e) = Z$, from which it follows that $\pi (Z)_{\mathrm{red}} = X_{\mathrm{red}}$, and therefore $\pi (Z) = X$ if X is assumed to be reduced. Consequently $R = X$ and this shows that Z is a principal H-bundle on X. Thus any connected and reduced X has $\mathscr{P}$.

Next we show that if X has a fundamental group-scheme, then X has $\mathscr{P}$. By definition there exist $(r_i, s_i) : (P, \pi (X, X_0), *) \to (Q_i, G_i, V_i)$ for $i = 1, 2$, and by uniqueness $(f_1 r_1, \rho_1 \circ s_1) = (f_2 r_2, \rho_2 \circ s_2)$. Therefore $r_1 \times r_2 : P \to T$ has $(r_1 \times r_2) P \subseteq Z$. This shows that $R = \pi (Z) = X$ and therefore Z is a principal H-bundle on X, as was to be shown.

Finally we show that if X has $\mathscr{P}$, then X has a fundamental group-scheme. First some generalities :

A small category $\mathscr{D}$ is an inverse system if given $f_i : A_i \to B$ for $i = 1, 2$, there is an object C of $\mathscr{D}$ and morphisms $g_i : C \to A_i$ for $i = 1, 2$ that $f_1 \circ g_1 = f_2 \circ g_2$.

Given such a category and a functor $F : \mathscr{D} \to \mathscr{C}'$, there is a canonically associated object of $\mathscr{C}'$.

For any object A of $\mathscr{D}$, if $FA = (Q, G, V)$, put $QFA = Q$, $GFA = G$ and $VFA = V$. The triple $(\tilde{Q}, \tilde{G}, \tilde{V})$ is an object of $\mathcal{C}'$:

$$\tilde{Q} = \lim_{\substack{\longleftarrow \\ A\in\mathscr{D}}} QFA, \quad \tilde{G} = \lim_{\substack{\longleftarrow \\ A\in\mathscr{D}}} GFA, \quad \tilde{V} = \lim_{\substack{\longleftarrow \\ A\in\mathscr{D}}} VFA.$$

Let us check that these constructions make sense :

If $R(G)$ denotes the coordinate ring of an affine group-scheme G, then $R = \lim_{\substack{\longrightarrow \\ A\in\mathscr{D}}} R(GFA)$ is a Hopf algebra which is the union of its finite dimensional Hopf sub-algebras. Therefore $\tilde{G} = \operatorname{spec} R$ is an inverse limit of finite group-schemes.

Similarly, if $R(Q) = j_*(\mathbf{O}_Q)$ for a morphism $j : Q \to \mathfrak{X}$, put $R' = \lim_{\substack{\longrightarrow \\ A\in\mathscr{D}}} R(QFA)$ is a locally free sheaf of $\mathbf{O}_X$-algebras on $\mathfrak{X}$; thus there is a flat affine morphism $j : \tilde{Q} \to \mathfrak{X}$ such that $R(\tilde{Q}) = R'$.

The isomorphisms $QFA \otimes_k GFA \to QFA \otimes_X QFA$ give isomorphisms $R(QFA) \otimes_X R(QFA) \to R(QFA) \otimes_k R(GFA)$, and in the direct limit ar isomorphism $R' \otimes_X R' \to R' \otimes_k R$. Thus $Q \times G \to Q \, x_X \, Q$ is an isomorphism. $\tilde{V}$ is constructed similarly.

If we assume that $\mathfrak{X}$ has $\mathscr{P}$, then $\mathcal{C}$ itself is an inverse system and the $(\tilde{Q}, \tilde{G}, \tilde{V})$ associated to the identity functor of $\mathcal{C}$ is easily seen to satisfy all the required properties of $(P, \pi(\mathfrak{X}, x_0), *)$.

This completes the proofs of Propositions 1 and 2.

In Chapter I, we constructed $\pi(\mathfrak{X}, x_0)$ directly using the Tannaka category of all essentially finite vector bundles. The essential content of Proposition 3·11 is contained in Proposition 3 given below.

Definition 3 : A triple (Q, G, V) in $\mathcal{C}$ is reduced if for any morphism $(Q', G', V') \to (Q, G, V)$ in $\mathcal{C}$, $G' \to G$ is a surjection (i.e., it is a surjection in the flat topology : more directly $R(G) \to R(G')$ is an injection).

If $\mathfrak{X}$ has a fundamental group-scheme, a triple (Q, G, V) is reduced if and only if the homomorphism $\pi(\mathfrak{X}, \chi_0) \to G$ is surjective. This is trivial.

Proposition 3 : Let $\mathfrak{X}$ be a complete, connected and reduced k-scheme with χ_0 as usual. Let (Q, G, V) be a triple in $\mathcal{C}$. Then the following are equivalent :

(a) (Q, G, V) is reduced.

(b) The functor $F(Q)$: mod-$G \to S(\mathfrak{X})$ is fully faithful (see § 2, Chapter I for the definition of $F(Q)$).

(c) $\Gamma(Q, \mathbf{O}_Q) = k$.

This is the only case where we have a criterion for determining whether (Q, G, V) is reduced or not. In characteristic zero, (Q, G, V) is reduced if and only if Q is connected, as is well-known.

Proof: $B \Rightarrow C$. Let $j : Q \to \mathscr{X}$ be the given morphism. Then $\Gamma(Q, O_Q) = \Gamma(\mathscr{X}, j_* O_Q) = \Gamma(\mathscr{X}, F(Q)\, R(G))$ = the fixed subspace of $R(G)$ under the G-action (because $F(Q)$ is fully faithful) $= k$.

$C \Rightarrow A$. There is a morphism $(f, \rho) = (P, \pi(\mathscr{X}, \chi_0), *) \to (Q, G, V)$. If ρ is not surjective, its image is a proper closed subgroup-scheme H of G and the fixed subspace of $R(G)$ under the $\pi(\mathscr{X}, \chi_0)$-action is clearly the coordinate ring of G/H which contains k properly. Therefore $\Gamma(Q, O_Q) = \Gamma(\mathscr{X}, F(P)\, R(G))$ contains k properly.

$A \Rightarrow B$. We are given that $\rho : \pi(\mathscr{X}, \chi_0) \to G$ is a surjective. Therefore G-mod $\to$ $\pi(\mathscr{X}, \chi_0)$-mod is fully faithful. But from the construction of $\pi(\mathscr{X}, \chi_0)$ in chapter I, $\pi(\mathscr{X}, \chi_0)$-mod $\to S(\mathscr{X})$ is fully faithful. Thus mod-G $\to S(\mathscr{X})$ is fully faithful.

Next we deal with the relation between $\pi(\mathscr{X}, \chi_0)$ and $\pi(\mathscr{X}, \chi_1)$ where χ_1 : spec $k \to \mathscr{X}$ is another k-rational point of $\mathscr{X}$, assuming that $\pi(\mathscr{X}, x_0)$ does indeed exist

Let R be a principal homogeneous G-space with G acting on the left. Then there is a group-scheme G' acting on R on the right such that

(a) the actions of G and G' on R commute, and

(b) R is a principal homogeneous G'-space.

This determines G' uniquely. In the literature, G' is often called an inner twist of G, especially when G is an affine algebraic group. If G is commutative, then $G = G'$.

Let $\mathscr{C}_1$ be the same category as $\mathscr{C}$ except that the base-point V of Q sits above χ_1.

Take an object (Q, G, V) of $\mathscr{C}$. Let R and G' be as above. Then $Q \times R$ has an action of $G \times G'$: G' acts trivially on Q and on R in the given manner, and $Q \times R$ gets the diagonal action of G. The quotient $Q' = Q \times R/G$ is thus a principal G'-bundle on $\mathscr{X}$.

In particular, $j^{-1}(\chi_1)$ in $j : Q \to \mathscr{X}$ is a principal homogeneous G-space, so we may put $R = j^{-1}(\chi_1)$. In this case the fibre over χ_1 in Q' is $R \times R/G$ which contains $\Delta R/G$. This $\Delta R/G$ gives a base point V' of Q' sitting above χ_1. Thus (Q', G', V') is an object of $\mathscr{C}_1$.

It is clear that this induces an isomorphism of the categories $\mathscr{C}$ and $\mathscr{C}_1$. This gives in the inverse limit :

Proposition 4 : Assume that $\mathscr{X}$ has a fundamental group-scheme at χ_0. Let $R = j^{-1}(\chi_1)$ in $j : P \to \mathscr{X}$. Then $\pi(\mathscr{X}, \chi_1)$ also exists, and

(a) R is a principal homogeneous space for both $\pi(\mathscr{X}, \chi_0)$ and $\pi(\mathscr{X}, \chi_1)$ and the actions of both on R commute, i.e.,

(b) $\pi(\mathscr{X}, \chi_1)$ is an inner twist of $\pi(\mathscr{X}, x_0)$; consequently,

(c) $\pi(\mathscr{X}, \chi_0)$ and $\pi(\mathscr{X}, \chi_1)$ are isomorphic after a base-change to $\bar{k}$, and

(d) $\pi(\mathscr{X}, \chi_0)_{ab}$ and $\pi(\mathscr{X}, \chi_1)_{ab}$ are isomorphic.

Now we examine the effect of base-change on fundamental group-schemes. It will be freely asumed that all schemes encountered have $\mathscr{P}$.

Let L be an arbitrary field extension of k. The base-change of a k-scheme Y to L will be denoted by $\bar{Y}$.

If $\mathscr{X}$ is a k-scheme and χ_0 a k-rational point, we can base-change the universal triple $(P, \pi(\mathscr{X}, \chi_0), *)$ to L. If $(R, \pi(\bar{\mathscr{X}}, \bar{\chi}_0), \bar{*})$ is the univesal triple for $(\bar{\mathscr{X}}, \bar{\chi}_0)$

by definition there is a unique morphism $(R, \pi(\bar{\mathscr{X}}, \bar{\chi}_0), \tilde{*}) \to (\bar{P}, \overline{\pi(\mathscr{X}, \chi_0)}, \bar{*})$, and in particular, a natural homomorphism $\pi(\bar{\mathscr{X}}, \bar{\chi}_0) \to \overline{\pi(\mathscr{X}, \chi_0)}$.

If τ is an automorphism of L fixing k, again invoking the universal property, we see that there is a unique A_τ with a commutative diagram as below :

$$\begin{tikzcd}
(R, \pi(\bar{X}, \bar{x}_0), \tilde{*}) \arrow[r, "A_\tau"] \arrow[d, dash] & (R, \pi(\bar{X}, \bar{x}_0), \tilde{*}) \arrow[d, dash] \\
\operatorname{Spec} L \arrow[r, "\tau"] & \operatorname{Spec} L
\end{tikzcd}$$

It follows that $A_\sigma A_\tau = A_{\sigma\tau}$, and if L is a finite galois extension of k, this gives descent data for the above triple showing that there is a triple (Q, G, V) for the pair $(\mathscr{X}, \chi_0)$ such that $(\bar{Q}, \bar{G}, \bar{V}) = (R, \pi(\bar{\mathscr{X}}, \bar{\chi}_0), *)$. Using the unique morphism $(P, \pi(\mathscr{X}, \chi_0), *) \to (Q, G, V)$, we get a homomorphism $\pi(\mathscr{X}, \chi_0) \to G$ and therefore (after base-change) a homomorphism $\overline{\pi(\mathscr{X}, \chi_0)} \to \pi(\bar{\mathscr{X}}, \bar{x}_0)$. It is easy to see that these homomorphisms are inverses of each other : therefore $\pi(\bar{\mathscr{X}}, \bar{\chi}_0) \to \overline{\pi(\mathscr{X}, \chi_0)}$ is an isomorphisms.

If L is a finite separable extension of k, then there is a finite galois extension E if k containing L. Applying the above to E/k and E/L we see once again that $\pi(\bar{\mathscr{X}}, \bar{\chi}_0) \to \overline{\pi(\mathscr{X}, \chi_0)}$ is an isomorphism. This immediately gives

Proposition 5 : If L is an arbitrary separable algebraic extension of k, then $\pi(\bar{\mathscr{X}}, \bar{\chi}_0)$ and $\overline{\pi(\mathscr{X}, \chi_0)}$ are isomorphic.

Remark : If $\mathscr{X} = A^1$ and $L = k(t)$, then $\pi(\bar{\mathscr{X}}, \bar{\chi}_0)$ and $\overline{\pi(X, \chi_0)}$ are certainly not isomorphic (even if k is algebraically closed) as is easily seen by considering the Artin-coverings $Z - Z^p = f(T)$.

Here $L = \bar{K}$ = an algebraic closure of k. If $\mathscr{X} = A^1$ and k are not perfect, then $\pi(\bar{\mathscr{X}}, \bar{\chi}_0)$ and $\overline{\pi(X, \chi_0)}$ are not isomorphic ; this is seen by comparing the α_p-quotients on either side.

However we believe that the following is true :

Conjecture : If $\mathscr{X}$ is complete, geometrically connected and reduced, and L is an arbitrary field extension of k, then $\pi(\bar{\mathscr{X}}, \bar{\chi}_0) \to \overline{\pi(\mathscr{X}, \chi_0)}$ is an isomorphism.

§ 2. All schemes considered are connected, reduced and of finite type over k, unless explicitly mentioned.

Proposition 6 : U is an open dense subset of $\mathscr{X}$ such that $\mathbf{O}_{X,x}$ is an integrally closed local domain for all $x \in \mathscr{X} - U$, and $f : Y \to \mathscr{X}$ is a morphism such that $\mathbf{O}_X \to f_*(\mathbf{O}_Y)$ when restricted to U is an isomorphism.

A. Let Q be a principal G-bundle on $\mathscr{X}$ (with G a finite group-scheme) such that the structure group of f^*Q can be reduced to a closed subgroup-scheme H. Then the structure group of Q itself can be reduced to H.

B. If y_0 is a k-ratlonal point of $f^{-1}(U)$ and $f(y_0) = x_0$, then $\pi(Y, y_0) \to \pi(\mathscr{X}, x_0)$ is a surjection.

Proof: Factor $j : Q \to \mathscr{X}$ by $j' : Q \to Z = Q/H$ and $j'' : Z \to \mathscr{X}$. By assumption, there is a $s : Y \to Z$ such that $j''. s = f$ with the principal H-bundle Q' on Y being $Y x_Z Q$.

Now s induces $j''_*(\mathbf{O}_Z) \to f_*(\mathbf{O}_Y)$, and by restricting to U, $j''_*(\mathbf{O}_Z) \mid U \to \mathbf{O}_X \mid U \overset{\cong}{\to} f_*(\mathbf{O}_Y) \mid U$. Because j'' is an affine morphism, there is a $t : U \to Z$ such that $t \circ (f \mid f^{-1} U) = s \mid f^{-1} U$.

Let T be the closure of the image of t. Then, for all $x \in \mathscr{X} - U$, Tx_X spec $\mathbf{O}_{X,\bullet} \to$ spec $\mathbf{O}_{X,\bullet}$ is a finite birational morphism, and therefore an isomorphism. Therefore $T \to \mathscr{X}$ is itself an isomorphism, thus giving a section $t : \mathscr{X} \to Z$ such that $t \mid U = t$. Then $Q'' = j'^{-1}(t(\mathscr{X}))$ is the required H-bundle on $\mathscr{X}$. This finishes the proof of A.

To show that $\pi(Y, y_0) \to \pi(\mathscr{X}, x_0)$ is a surjection, it suffices to show that the composite $\pi(Y, y_0) \to \pi(\mathscr{X}, x_0) \to G$ is a surjection for all finite quotients G of $\pi(\mathscr{X}, x_0)$.

Let G be one such, and let H be the image of $\pi(Y, y_0)$ in G. Then, there is a triple (Q, G, V) for the pair $(\mathscr{X}, x_0)$ and a triple (Q', H, V') for (Y, y_0) and a morphism $(Q', H, \mathrm{V}') \to (f^*, Q, G, \mathrm{V}\, xy_0)$.

By A there is a principal H-bundle Q'' on $\mathscr{X}$ and a diagram :

$$\begin{tikzcd}
Q' \mid f^{-1} U \arrow[r] \arrow[d] & Q' \arrow[d] \\
Q'' \mid U \arrow[r] & Q
\end{tikzcd}$$

thus showing that V is a k-rational point of $Q'' \mid U$. The inclusion (Q'', H, V), $\to (Q, G, v)$ shows that there is a factoring : $\pi(\mathscr{X}, x_0) \to H \to G$. Consequently $H = G$ and B has also been proved.

Corollary: If $f : Y \to \mathscr{X}$ is an open immersion and $\mathscr{X}$ is normal, then $\pi(Y, y_0) \to \pi(\mathscr{X}, x_0)$ is a surjection.

Corollary : If $f : Y \to \mathscr{X}$ is smooth and proper with connected fibres, then $\pi(Y, y_0) \to \pi(X, x_0)$ is a surjection.

Proposition 7 : Let U be open dense in X such that $\mathbf{O}_{X,x}$ is a regular local ring of dimension $\geqslant 2$, for all $x \in X - U$. Then any principal G-bundle on U (where G is a finite group-scheme) extends to one such on X.

If x_0 is a k-rational point of U, then $\pi(U, x_0) \to \pi(X, x_0)$ is an isomorphism.

Proof: The second assertion follows trivially from Proposition 6 and the first assertion.

Let $j : Q \to U$ be a principal G-bundle on U and $i : U \to X$ the inclusion morphism. Then $i_* j_* (\mathbf{O}_Q)$ is a coherent sheaf of $\mathbf{O}_X$-algebras and therefore there is a finite morphism $j' : P \to X$ such that $j'_*(\mathbf{O}_P) = i_* j_* (\mathbf{O}_Q)$. It is clear that there is a G-action on P such that j' is G-equivariant (with the trivial action of G on $\mathscr{X}$), and that $j'^{-1}(U) = Q$.

Assume that $j'_*(\mathbf{O}_P)$ is locally free. Then the standard morphism $P \times G \to P \times_X P$ is an isomorphism if and only if it induces an isomorphism $j'_*(\mathbf{O}_P) \otimes j'_*(\mathbf{O}_P) \to j'_* \mathbf{O}_P \otimes R(G)$. But these are locally free and of the same rank and therefore if V is the largest open subset of $\mathscr{X}$ restricted to which it is an isomorphism, then the complement of V is of pure codimension one. However, V contains U ; consequently $V = \mathscr{X}$ and P is a principal G-bundle on X.

Thus it suffices to show that $j'_*(O_P)$ is locally free ; equivalently, $j' : P \to X$ is a flat morphism. For this purpose, we may clearly assume that $\mathscr{X} = \operatorname{spec} R$, where R is a regular ring.

For a scheme Y in characteristic p, let $\pi_Y : Y \to Y$ be the Frobenius. If $Y =$ spec A, π_Y will also be noted by π_A and $(\pi_Y^m)_* O_Y = \tilde{A}_m$. If A is an integral domain, $A_m = A^{1/p^m}$.

The commutative diagram

$$\begin{tikzcd}
G \arrow[r, "\pi_G^m"] \arrow[d] & G \arrow[d] \\
\operatorname{Spec} k \arrow[r, "\pi_k^m"] & \operatorname{Spec} k
\end{tikzcd}$$

induces a homomorphism $G \to (\pi_k^m)^* G$.

Similarly, the diagram

$$\begin{tikzcd}
Q \arrow[r, "\pi_Q^m"] \arrow[d] & Q \arrow[d] \\
U \arrow[r, "\pi_U^m"] & U
\end{tikzcd}$$

induces $Q \to (\pi_U^m)^* Q$. Also $(\pi_U^m)^* Q$ is easily seen to be a principal $(\pi_k^m)^* G$-bundle on U and the morphism $Q \to (\pi_U^m)^* Q$ intertwines the actions of G and $(\pi_k^m)^* G$.

The direct image of the structure sheaf under $(\pi_U^m)^* Q \to U \xrightarrow{\pi_U^m} U \to \mathscr{X}$ is precisely $\widetilde{R_m \otimes_R B}$, where $\tilde{B} = i_* j_* (O_Q)$, because R_m is R-flat. And the morphism $Q \to (\pi_U^m)^* Q$ induces the usual R-algebra homomorphism $R_m \otimes_R B \to B_m$ by taking direct images of structure sheaves.

Case 1 : If G is a local group-scheme, $G \to (\pi_k^m)^* G$ is the trivial homomorphism for a suitably large m. The morphism $Q \to (\pi_U^m)^* Q$ thus makes $(\pi_U^m)^* Q$ the trivial bundle on U. Therefore $R_m \otimes_R B$ is a free R_m-module, and because R_m is R-faithfully flat, B is a locally free R-module.

Case 2 : If G is geometrically reduced, then $G \to \pi_k^* G$ is an isomorphism ; it follows that $Q \to \pi_U^* Q$ and $R_1 \otimes_R B \to B_1$ are isomorphisms too. In particular, B_1 is B-flat. By a theorem of Kunze, this proves that B is regular. That B is R-flat follows from the fact that it is a finitely generated Cohen-Macaulay R-module,

In both cases we have shown that $j' : P \to \mathscr{X}$ is flat.

Now for the general case : there is an exact sequence :

$$1 \to G_{\text{loc}} \to G \to H \to 1$$

where G_{loc} is a local group-scheme and H is geometrically reduced. In fact this sequence is split if k is assumed to be perfect.

In any case Q/G_{loc} is a principal H-bundle on U, and by case 2, Q/G_{loc} is the inverse image of U in a principal H-bundle $Z \to X$. The pair $(Z, Q/G_{\text{loc}})$ have the same properties as (X, U) and $Q \to Q/G_{\text{loc}}$ is a principal G_{loc}-bundle: by case 1, Q is the inverse image of Q/G_{loc} in a principal G_{loc}-bundle $W \to Z$. Thus Q is the inverse image of U in the flat morphism $W \to X$ showing that $i_* j_* (\mathbf{O}_Q)$ is locally free.

This completes the proof of Proposition 7.

Proposition 8: If X and Y are smooth complete birationally isomorphic varieties over k, and x_0, y_0 are geometric points of X and Y respectively, then $\pi(X, x_0)$ an $\pi(Y, y_0)$ are inner twists of each other.

If Y is assumed only to be normal and complete instead, and k is algebraically closed, then $\pi(Y, y_0)$ is a quotient of $\pi(X, x_0)$.

Proof: For the sake of simplicity, we shall prove the first statement only for separably closed field k. In this case, there is a complete normal variety Z, morphisms $f : Z \to X$ and $g : Z \to Y$, open subsets $U \to X$ and $V \to Y$ such that $f^{-1}(U) \to U$ and $g^{-1}(V) \to V$ are isomorphisms and a k-rational point z_0 in $f^{-1}(U) \cap g^{-1}(V)$. Put $x_0 = f(z_0)$ and $y_0 = g(z_0)$. Then we have :

$$\begin{tikzcd}
\pi(f^{-1}(U), z_0) \arrow[r, "\text{onto}"] \arrow[d, "\cong"'] & \pi(Z, z_0) \arrow[d] \\
\pi(U, x_0) \arrow[r, "\cong"] & \pi(X, x_0)
\end{tikzcd}$$

The above horizontal arrow is surjective by Proposition 6, and the one below is an isomorphism by Proposition 7. Therefore $\pi(Z, z_0) \to \pi(X, x_0)$ is an isomorphism. Similarly $\pi(Z, z_0) \to \pi(Y, y_0)$ is an isomorphism, and the general statement follows from Proposition 4.

If Y is only normal, then $\pi(Z, z_0) \to \pi(Y, y_0)$ is only a surjection, proving the second statement.

Lemma : If k is any field, $\pi(\mathbf{P}^1, x_0)$ is trivial.

Proof : The representations of $\pi(\mathbf{P}^1, x_0)$ are essentially finite bundles on $\mathbf{P}^1$. But any semi-stable bundle on $\mathbf{P}^1$ of degree zero is trivial, and therefore all repiesentations of $\pi(\mathbf{P}^1, x_0)$ are trivial. Thus $\pi(\mathbf{P}^1, x_0)$ is itself trivial.

Proposition 9 : Let $f : Z \to X$ be a smooth proper morphism with connected fibres. Assume that X is reduced. Also, for every t : spec $\bar{k} \to X$, the fibre Z_t has the trivial fundamentalgroup-scheme. Let z_0 be a k-rational point of Z and $f(z_0) = x_0$. Then $\pi(Z, z_0) \to \pi(X, x_0)$ is an isomorphism.

Proof : The surjectivity follows from the corollaries to Proposition 6. To prove the injectivity we have to show that any $j : P \to Z$ which is a principal G-bundle on Z is the pull-back of a principal G-bundle on X. Here G is a finite group-scheme.

For any t : spec $\bar{k} \to X$, $P \mid Z_t$ is the trivial bundle. Thus the semi-continuity theorem applied to the sheaf $j_*(\mathbf{O}_P)$ and the morphism $f : Z \to X$ shows that $f_* j_* (\mathbf{O}_P)$ is locally free, and, the natural homomorphism $f^* f_* j_* (\mathbf{O}_P) \to j_* (\mathbf{O}_P)$ is an isomorphism of $\mathbf{O}_Z$-algebras.

Thus, if $h : W \to X$ is defined by $h_* (O_W) = f_* j_* (O_P)$, i.e., $P \to W \xrightarrow{h} X$ is the Stein factorisation of $f \circ j$, then the natural map $P \to W x_X Z$ is an isomorphism.

The Stein factorisation applied to the vertical arrows of

$$\begin{tikzcd}
P \times G \arrow[rr] \arrow[dr] & & P \arrow[dl] \\
& X &
\end{tikzcd}$$

gives

$$\begin{tikzcd}
P \times G \arrow[rr] \arrow[d] & & P \arrow[d] \\
W \times G \arrow[rr] \arrow[dr] & & W \arrow[dl] \\
& X &
\end{tikzcd}$$

Therefore there is a G-action on W, and $P \to W$ and $W \to X$ are G-equivariant (with the trivial action on X).

Also the standard $W \times G \to W x_X W$ is an isomorphism because its base-change to Z is $P \times G \to P x_Z P$ (which is by very assumption an isomorphism) and $Z \to X$ is flat and surjective.

This shows that W is a principal G-bundle on X and that $P = f^* W$, Q.E.D.

Corollary : Any complete normal rational variety has a trivial fundamental group-scheme.

Proof: By the above proposition, $\mathbf{P}^1 \times \mathbf{P}^1 \times \cdots \mathbf{P}^1$ has a trivial fundamental group-scheme. The corollary now follows from Proposition 8. No assumption on k is neessary; that k is algebraically closed was required in the proof of Proposition 8 only to get hold of a k-rational point in any non-empty open subset.

Corollary: If $f : Z \to X$ is smooth and proper with Z_t rational for all t : spec $\bar{k} \to X$, then $\pi(Z, z_0) \to (\pi(X, x_0)$ is an isomorphism.

This follows immediately from the above corollary and Proposition 9.

Chapter III

Parabolic bundles and ramified coverings

Let X be a smooth connected projective curve over an algebraically closed field k with a base-point x_0 and a finite subset S of X such that $x_0 \notin S$. We want to identify the representations of $\pi(X - S, x_0)$ with certain bundles on $X - S$ wih some additional structure (denoted by parabolic bundles) and show that the main theorems of Chapter I hold in this modified situation

First some generalities : denote by T the diagram

$$\begin{tikzcd} & Y_1 \\ Z \arrow[ur, "f_1"] \arrow[dr, "f_2"'] & \\ & Y_2 \end{tikzcd}$$

where Z, Y_1 and Y_2 are schemes over k and f_1 and f_2 are morphisms.

A vector bundle W on T is a $W = (V, V_1, V_2, \varphi_1, \varphi_2)$ where V, V_1 and V_2 are vector bundles on Z, Y_1 and Y_2 respectively and $\varphi_i : V \to f_i^* V_i$ are isomorphisms for $i = 1, 2$. It is clear what a homomorphism of vector bundles on T is, and what is meant by exactness of a sequence of vector bundles on T. The category of vector bundles on T shall be denoted by Vect T.

A principal G-bundle P on T is $P = (Q, Q_1, Q_2, \psi_1, \psi_2)$ where Q, Q_1 and Q_2 are principal G-bundles on Z, Y_1 and Y_2 respectively and $\psi_i : Q \to f_i^* Q_i$ are isomorphisms for $i = 1$ and 2. If Y_1 has a base point x_0, a base-point for P is a point of Q_1 sitting above x_0. Thus we can form the category of triples (P, G, v) where P is a principal G-bundle on T, G is a finite group-scheme, as in chapter II ; this category we shall denote by $\mathcal{C}(T)$.

An immediate extension of Proposition 2·9, Chapter I is :

Lemma 1 : There is a bijective correspondence between principal G-bundles P on T and functors $F : G$-mod $\to$ Vect T satisfying $F1$ to $F4$, where G is any affine group-scheme. The functor F associated to a principal G-bundle P on T will be denoted by $F(P)$ as usual.

In applications Z, Y_1 and Y_2 are going to be very special : $Y_1 = X - S$ with base-point x_0. For each $x \in S$, let K_x = quotient field of $\hat{O}_{X,x}$ and E_x an arbitrary algebraic extension of K_x. Let R_x be the integral closure of $\hat{O}_{X,x}$ in E_x. Put $Z = \operatorname{spec}(\bigoplus_{x \in S} E_x)$ and $Y_2 = \operatorname{spec}(\bigoplus_{x \in S} R_x)$, with the obvious morphisms f_1 and f_2.

With this choice of T, a parabolic bundle on $X - S$ is just a vector bundle on T, and homomorphisms of parabolic bundles are just vector bundles homomorphisms on T.

2 : For each $x \in S$ choose an isomorphism of K_x with $k(t)$ and put $E_x = \bigcup_{n \geqslant 1} k(t^{1/n})$. Then parabolic bundles on $X - S$ are precisely "parabolic bundles with fractional weights" in the sense of Seshadri.

3 : However, most frequently we shall put $E_x = \bar{K}_x$, the algebraic closure of K_x. One good reason is the following :

Lemma 2 : $\mathcal{C}(X - S, x_0)$ be the category of triples (Q, G, v) associated to the pair $(X - S, x_0)$. If $E_x = \bar{K}_x$ for all $x \in S$, then $\mathcal{C}(T) \to \mathcal{C}(X - S, x_0)$ is an isomorphism.

Proof : A principal G-bundle on spec E_x can be regarded as a principal homogeneous space for spec $E_x \times_{\operatorname{spec} k} G$, but E_x being algebraically closed, this always admits a E_x-rational point. Thus any principal G-bundle on spec E_x is trivial. By Proposition 6, Chapter II, it follows that any principal G-bundle on spec R_x is trivial, where G is a finite k-group-scheme.

Let P be a principal G-bundle on T. Then $P = (Q, Q_1, Q_2, \psi_1, \psi_2)$, and we may assume that $Q = Z \times G$, $Q_2 = Y_2 \times G$ and ψ_2 is the obvious isomorphism from Q to $f_2^* Q_2$. Thus, such a P is completely determined by a principal G-bundle Q_1 on $Y_1 = X - S$, and an isomorphism $\psi_1 : Z \times G \to f_1^* Q_1$.

It follows that the objects of $\mathcal{C}(T)$ can be identified with (Q_1, G, ψ_1, v) where Q_1 is principal G-bundle on $X - S$, G a finite group-scheme, v a base-point of Q_1 above x_0, and $\psi_1 : Z \times G \xrightarrow{\cong} f_1^* Q_1$.

Given (Q_1, G, v) an object of $\mathcal{C}(X - S, x_0)$, such a ψ_1 always exists because all G-bundles on Z are trivial. This shows that $\mathcal{C}(T) \to \mathcal{C}(X - S, x_0)$ is a "surjection".

A morphism from (Q_1', G', ψ_1', v') to $(Q_1'', G'', \psi_1'', v'')$ in $\mathcal{C}(T)$ is by definition a (h, h_1, h_2, ρ) such that $A : (h_1, \rho) : (Q_1', G', v') \to (Q_1'', G'', v'')$ is a morphism in $\mathcal{C}(X - S, x_0)$ and a commutative diagram

$$\begin{tikzcd}
\mathrm{B} & Y_2 \times G' \arrow[d, "h_2"'] & Z \times G' \arrow[l] \arrow[r] \arrow[d, "h"] & f_1^* Q_1' \arrow[d, "f_1^* h_1"] \\
 & Y_2 \times G'' & Z \times G'' \arrow[l] \arrow[r] & f_1^* Q_1''
\end{tikzcd}$$

where h and h_2 intertwine the right actions of G' and G'' *via* $\rho : G' \to G''$.

Given a (h_1, ρ) satisfying A, we shall show that there is a unique (h, h_1, h_2, ρ) satisfying both A and B. The right side of the diagram determines h. Now h is equivalent to giving a morphism $Z \to G''$ and this necessarily factors : $Z \to \operatorname{spec} k \xrightarrow{\iota} G''$. Using the morphism $Y_2 \to \operatorname{spec} k \xrightarrow{\iota} G''$, one gets the required h_2.

This is exactly the same as saying that $\mathcal{C}(T) \to \mathcal{C}(X - S, x_0)$ is fully faithful. The lemma is now proved.

We now define the degree of a parabolic vector bundle.

Let $v_x : E_x \to Q \cup \infty$ be the unique valuation such that $v_x(K_x) = \mathbf{Z} \cup \infty$. If L is a line bundle on Y_2 and s is a section of $f_2^* L$ on Z, then $(\bigoplus_{x \in S} R_x) s = \bigoplus_{x \in S} h_x L_x$ for some $h_x \in E_x$, where L_x is the stalk of the sheaf of sections of L at x. Define $v_x(s)$ to be $v_x(h_x)$.

If $W = (L, L_1, L_2)$ is a line bundle on T, and s is a section of L_1 on $Y_1 = X - S$, put $\deg s = \sum_{x \in X} v_x(s)$. For $x \in X - S$, $v_x(s)$ is as usual the order of vanshing of s at x, and if $x \in S$, then $v_x(s)$ makes sense as above, as a rational number. Then deg s is easily seen to be independent of the choice of s and we define $\deg W = \deg s$.

If W is a parabolic vector bundle of rank r, then we define $\deg W = \deg \Lambda^r W$. Clearly we have :

Lemma 3 : A. For an exact sequence $0 \to V' \to V \to V'' \to 0$ of parabolic bundles, $\deg V' + \deg V'' = \deg V$.

B. If $f : V \to W$ is a homomorphism of parabolic bundles and $f \mid U$ is an isomorphism for some open subset U of $X - S$, then $\deg V \leqslant \deg W$.

C. If $\mu(V) = \deg V / rk\, V$, then $\mu(V \otimes W) = \mu(V) + \mu(W)$.

A homomorphism $h : W \to V$ of parabolic bundles is a generic injection if $h|U$ is an injection for some nonempty open subset U of $X - S$.

A parabolic bundle V of degree zero is semi-stable if for all $h : W \to V$ which are generic injections, $\deg W \leqslant 0$.

Lemma 4 : A. Parabolic semi-stable bundles of degree zero form an abelian category.

B. If V is a parabolic bundle of rank $r > 1$, there is an exact sequence $0 \to V' \to V \to V'' \to 0$ with $rkV' = 1$.

C. If $0 \to V' \to V \to V'' \to 0$ is an exact sequence of parabolic bundles and $h : W \to V$ is a generic injection, there is a diagram :

$$\begin{tikzcd}
0 \arrow[r] & W' \arrow[r] \arrow[d, "h'"'] & W \arrow[r] \arrow[d, "h"'] & W'' \arrow[r] \arrow[d, "h''"'] & 0 \\
0 \arrow[r] & V' \arrow[r] & V \arrow[r] & V'' \arrow[r] & 0
\end{tikzcd}$$

with the horizontal arrows exact, and h' and h'' are generic injections.

The proofs are simple enough. For example C is proved by showing that such a diagram exists on Z, Y_1 and Y_2 separately (because torsion-free modules are locally free) and patching up.

A finite bundle is a parabolic bundle V such that $f(V) \cong g(V)$ for some $f \neq g$ which are polynomials with non-negative integer coefficients. An essentially finite bundle is defined exactly as in Chapter I.

Lemma 5 : The global sections of a parabolic bundle are finite dimensional.

Proof : Let (V, V_1, V_2) be a parabolic bundle. Let W be any vector bundle on X such that $W | X - S = V_1$. Then it is easy to see that there is a $\mathcal{N}$ such that the global sections of this parabolic bundle are contained in $\Gamma(X, W(ND))$ where $D = \sum_{x \in S} x$. This proves the lemma.

Lemmas 3, 4 and 5 immediately show that all the results of § 3, Chapter I up to Proposition 3·7 are valid for finite and essentially finite parabolic bundles.

Proposition 1 : Let P be a principal G-bundle on T, and G a finite group-scheme. Then, for all representations W of G, $F(P)\,W$ is an essentially finite parabolic bundle.

Proof : Let R be the co-ordinate ring of G, and if $n = rkR$, then $R \otimes R = R^n$ as G-representations. Consequently, if $V = F(P)\,R$, then $V \otimes V = V^n$, i.e., $[V]$ satisfies the polynomial $x^2 = nx$.

If W is a representation of G, then $W \to R^m$ for some m, and therefore $F(P)\,W \hookrightarrow V^m$. It suffices to show that $F(P)\,W$ has degree zero to prove that it is essentially finite. But if $r = rkW$, $L = \Lambda^r W$, $E = F(P)\,L$, then $\Lambda^r(F(P)\,W) = E$ and E is a parabolic line bundle of finite order and therefore has degree zero.

Exactly as in Chapter I, we see that all essentially finite bundles on T form a Tannaka category. Let $\pi(T)$ be the associated group-scheme. Then

Proposition 2 : Objects of $\mathcal{C}(T)$ are in one-to-one correspondence with homomorphisms from $\pi(T) \to G$.

Combining this with Lemma 2, we have :

Proposition 3 : If $E_x = \bar{K}_x$ for all $x \in S$, $\pi(T) = \pi(X - S, x_0)$ and its category of representations is precisely all essentially finite parabolic bundles on $X - S$.

If Char $k = 0$, note that $E_x = \bar{K}_x$ is the same as example 2, so that we have a good description of parabolic bundles in this case.

PART II

CHAPTER IV

1. Nilpotent bundles and formal groups for curves

An affine group-scheme G is nilpotent if every G-representation $V \neq 0$ has a $v \neq 0$ which is fixed by G.

Let X be a k-scheme of finite type with $\Gamma(X, O_X) = k$. We shall be concerned with principal G-burdles P on X.

Lemma 1 : If P and G are as above, and V is a finite dimensional representation of G, then $W = F(P)\,V$ has a filtration $W = W_0 \supseteq W_1 \supseteq \cdots \supseteq W_n = 0$ such that W_i/W_{i+1} is a trivial vector bundle on X.

Proof : By induction, we see that V has a filtration $V = V_0 \supseteq V_1 \supseteq \cdots \supseteq V_n = 0$ such that V_i/V_{i+1} is a trivial representation of G. Simply put $W_i = F(P)\,V_i$.

The full subcategory of all vector bundles on X with objects as those vector bundles on X that admit a filtration as in Lemma 1 will be denoted by $N(X)$.

Lemma 2 : $N(X)$ is an abelian category and is closed with respect to tensor products and duals.

Proof : Let $f : V \to W$ be a homomorphism with V and W in $N(X)$. For convenience, we identify vector bundles with their sheaves of sections. We have to show that Ker (f) and Coker (f) are locally free, and moreover, belong to $N(X)$. We shall do so by induction on $rk\,V + rk\,W$.

If $V = 0$ or $W = 0$, or if $rk\,V = rk\,W = 1$, then the statement is obvious because $\Gamma(X, O_X) = k$.

Also, the statement for f is equivalent for the statement for $f^* : W^* \to V^*$. Therefore, replacing f by f^* if necessary, we may assume that $rk\,W > 1$. There is an exact sequence $0 \xrightarrow{i} W' \xrightarrow{j} W \to O \to 0$ with W' in $N(X)$. Also $rk\,V + rk\,O_x < rk\,V + rk\,W$, so the statement holds for $j \circ f$. Thus $j \circ f = 0$ or $j \circ f$ is an isomorphism.

In the first case, we have $g : V \to W'$ such that $i \circ g = f$, and by the induction hypothesis ker (g) and coker (g) are locally free and in $N(X)$. But clearly, ker (f) = ker (g) and $0 \to$ coker $(g) \to$ coker $(f) \to O_x \to 0$ is exact, so that ker (f) and coker (f) have the required property.

The category of modules over a ring is denoted both by A-mod and | A | in the text.

In the second case, $V' = f^{-1}(W') = \ker(j \circ f)$ is in $N(X)$ and $h : V' \to W$ defined by

$$\begin{tikzcd} V' \arrow[r, "h"] \arrow[d] & W' \arrow[d] \\ V \arrow[r, "f"] & W \end{tikzcd}$$

has the required property by the induction hypothesis, and here h and f have the same kernels and cokernels.

That $V \otimes W$ is in $N(X)$ if both V and W are in $N(X)$ is obvious.

Let x_0 be a k-rational point of X and let $T : N(X) \to k$-mod be given by $T(V)$ = fibre of V at x_0. Then $N(X)$ becomes a Tannaka category and by Chapter I, § 1, there is an affine group-scheme $U(X, x_0)$ such that $U(X, x_0)$-mod is isomorphic to $N(X)$.

Every non-zero vector bundle in $N(X)$ has a trivial sub-bundle ; consequently every non-zero representation of $U(X, x_0)$ contains a non-zero fixed subspace. In other words $U(X, x_0)$ is a nilpotent group-scheme. By § 2, Chapter I, we see that there is a principal $U(X, x_0)$-bundle P on X with a k-rational point $*$ above x_0 with the following universal property :

Proposition 1: For every principal G-bundle Q on X with a k-rational point v of Q above x_0 (and G nilpotent), there is a unique homomorphism $\rho : U(X, x_0) \to G, f : P \to Q$ intertwining the actions of $U(X, x_0)$ and G, such that $f(*) = ve$.

Proposition 2: $\mathrm{Hom}(U(X, x_0), G_a) = H^1(X, O_X)$. In particular, if characteristic $k = 0$, then $U(X, x_0)_{ab} = H^1(X, O_X)^*$.

Proof : The second assertion follows immediately from the first.

The first follows from the well-known fact: isomorphism classes of principal G_a-bundles are in one-to-one correspondence with members of $H^1(X, O_X)$.

We recall some basic facts about affine group-schemes : if $\mu : R \to R \otimes R$ is the co-multiplication of R, the coordinate ring of $U(X, x_0)$, and if $A = R^* =$ the vector space dual of R, then A is an algebra. The collection of $V^{\perp}$, where the V range through all finite dimensional subspaces of R such that $\mu V \subseteq V \otimes V$, give a system of neighdourhoods of zero under which A is complete : $A = \lim\limits_{\overleftarrow{V}} A/V^{\perp}$. Note that $A/V^{\perp}$ is a finite-dimensional k-algebra.

In fact any open two-sided ideal is of the form $V^{\perp}$ where V is of the above type.

Also, $U(X, x_0)$-mod is the category A-mod of left A-modules M such that each member of M is annihilated by some V. Because $U(X, x_0)$ is nilpotent, it follows that each $A/V^{\perp}$ is an Artin-local ring (with maximal ideal $\mathbf{m}/V^{\perp}$ where $\mathbf{m} = k^{\perp}$ and $A/\mathbf{m} = k$).

Let $J_n = \bigcap\limits_{V} (\mathbf{m}^n + V^{\perp})$, i.e., J_n is the closure of $\mathbf{m}^n$ in A.

Lemma 3 : Assume that $H^1(X, \mathbf{O})_X$ is finite dimensional. Then

(a) J_n is open for all n,

(b) Every open two-sided ideal contains J_n for some n. Therefore $A = \varprojlim_{n} A/J_n$.

(c) $(J_1/J_2)^* = H^1(\mathcal{X}, \mathrm{O}_X)$.

(d) $J_n = \mathbf{m}^n$ for all n.

Proof ; We shall have no occasion to use D, so we omit its proof. Let J be any open two-sided ideal. Let $\bar{\mathbf{m}} = \mathbf{m}/J$ be the maximal ideal of the Artin-local ring A/J. Then $(\bar{m}/\bar{m}^2)^* = (m/m^2 + J)^* = \mathrm{Der}\,(A/J, k) =$ all derivations $D : A \to k$ that vanish on J. If $J = W^{\perp}$, all such derivations are in 1-1 correspondence with $x \in W$ such that $\mu\mathcal{X} = X \otimes 1 + 1 \otimes \mathcal{X}$. This in turn is a subspace of $\mathrm{Hom}\,(U(\mathcal{X}, x_0), G_a) = L = \{x \in R \mid \mu\mathcal{X} = \mathcal{X} \otimes 1 + 1 \otimes x\} = H^1(\mathcal{X}, \mathrm{O}_X)$.
Let $rk\, L = g$. By assumption, g is finite. Then

$$rk\,(A/\mathbf{m}^n + J) \leqslant 1 + rk\,(\bar{\mathbf{m}}^2/\bar{\mathbf{m}}^3) + rk\,(\bar{\mathbf{m}}^2/\bar{\mathbf{m}}^3) + \cdots + rk + (\bar{\mathbf{m}}^{n-1}/\bar{\mathbf{m}}^n)$$
$$\leqslant 1 + g + g^2 + \cdots + g^{n-1}.$$

From this it follows that there is an open two-sided ideal E such that for all open two-sided J contained in E, $A/\mathbf{m}^n + J \to A/\mathbf{m}^n + E$ is an isomorphism. This shows clearly that $J_n = \mathbf{m}^n + E$. This proves (a).

By the above remarks, if $J = W^{\perp}$, then $J + \mathbf{m}^2 = (k + W \cap L)^{\perp}$. It follows that $J_2 = (k + L)^{\perp}$. Thus $(J_1/J_2)^* = k + L/k = L$. This proves (c).

If J is any open two-sided ideal, then some power of the maximal ideal of A/J is zero. In other words, J contains some power of the maximal ideal, and therefore contains its closure, which is J_n for some n. This proves (b).

Let $R_n \subseteq R$ be defined by $R_n^{\perp} = J_n$. Then

Lemma 4 :

(a) $\mu(R_n) \subseteq R_n \otimes R_n$.

(b) R_n is finite dimensional.

(c) the R_n span R.

Proof : (a) and (b) follow from the fact that J_n is an open two-sided ideal (c) follows from dualising (b) of the above lemma.

We shall now get an explicit definition of the R_n. Let $R^{\otimes n}$ be the n-fold tensor product of R and $\mu_n : R \to R^{\otimes n}$ the iterated co-multiplication map. In fact it is induced by the multiplication morphism $G \times G \times \cdots \times G \to G$ where $G = U(\mathcal{X}, x_0)$. Let i_t: $R^{\otimes(n-1)} \to R^{\otimes n}$ be the inclusion by tensoring with 1 in the t-th factor, for $1 \geqslant t \geqslant n$. Let S_n = span of the images of $i_1, i_2, \cdots, i_n$.

Clearly, $(R^{\otimes n})^* = A \hat{\otimes} A \hat{\otimes} \cdots \hat{\otimes} A$ where $\hat{\otimes}$ denotes the completed tensor product, and $S_n = (m \hat{\otimes} m \hat{\otimes} \cdots \hat{\otimes} m)^{\perp}$. Then J_n is the closure of the image of S_n in $A \hat{\otimes} A \hat{\otimes} \cdots \hat{\otimes} A \to A$, and therefore $J_n = R_n^{\perp}$, where $R_n = \{x \in R \mid \mu_n x \in S_n\}$.

The following completely distinguishes the situation in characteristic zero and positive characteristic (assuming as always that $rk\, H^1(X, O_X) < \infty$).

Proposition 3 : If characteristic $k = p > 0$, then $U(X, x_0)$ is an inverse limit of finite group-schemes.

If X has a fundamental group-scheme, by the universal properties enjoyed by both $\pi(X, x_0)$ and $U(X, x_0)$, it follows that $U(X, x_0)$ is a quotient of $\pi(X, x_0)$.

Proof: Let H_n be the k-subalgebra of R generated by R_n. By lemma 4 (a), H_n is a Hopf sub-algebra of R.

If $\theta \in R_n$, then $\mu_n \theta \in S_n$. We have : $\mu_n(\theta^p) = (\mu_n \theta)^p \in S_n^p \subseteq S_n$. Therefore θ^p also belongs to R_n.

Let $x_1, x_2, \cdots, x_l$ span R_n. Then $x_1^{a_1} x_2^{a_2} \cdots x_l^{a_l}$ for $0 \leqslant a_i \leqslant p-1$ span H_n. because R_n is closed with respect to p-th powers. Therefore H_n is finite dimensional.

By lemma 4 (c), R is the union of its finite dimensional Hopf subalgebras, i.e, $U(X, x_0)$ is an inverse limit of finite group-schemes.

For simplicity, we assume that X is complete from now on.

Definition: An exact sequence $0 \to O_X^m \to U(V) \to V \to 0$ is a universal extension of V, if for every exact sequence $0 \to O_X^n \to W' \to V \to 0$ there is a diagram :

$$\begin{tikzcd}
0 \arrow[r] & O_X^m \arrow[r] \arrow[d, "f"'] & U(V) \arrow[r] \arrow[d] & V \arrow[r] \arrow[d, "1"] & 0 \\
0 \arrow[r] & O_X^n \arrow[r] & W' \arrow[r] & V \arrow[r] & 0
\end{tikzcd}$$

and while this diagram is not necessarily unique, the $f : O_X^m \to O_X^n$ is unique.

Every vector bundle V on X has a universal extension : Choose a basis $\xi_1, \xi_2, \cdots, \xi_m$ of $H^1(X, V^*)$. Then $\theta = (\xi_1, \xi_2, \cdots, \xi_m) \in H^1(X, V^*) = H^1(X, \mathrm{Hom}(V, O_X^m))$ defines the required extension :

$$0 \to O_X^m \to U(V) \to V \to 0.$$

More canonically, the O_X^m should be replaced by $j^*(H^1(X, V^*))^*$ where $j : X \to \operatorname{Spec} k$.

An immediate consequence of the definition is :

Lemma 5 : The natural map $H^1(X, V^*) \to H^1(X, U(V)^*)$ is identically zero,

Similarly, for A-modulus M, a universal extension of M is an exact sequence : $0 \to k^m \to U(M) \to M \to 0$ of A-modules with an identical universal property.

Denote by F the natural equivalence from $|U(X, x_0)| = |A| \to N(X)$. The next lemma is obvious.

Lemma 6 : $U(FM) = F(U(M))$ for all A-modules M.

Lemma 7 : If $V_1 = O_X$ and $V_{n+1} = U(V_n)$ for all n, then $F(A/J_n) = V_n$ for all n.

Proof: By Lemma 6, it suffices to show that $U(A/J_n) = A/J_{n+1}$ for all $n \geqslant 1$. Let $0 \to k^m \to M \to A/J_n \to 0$ be an exact sequence of A-modules annihilated by some open two-sided ideal E. But M is clearly annihilated by m^{n+1} ; therefore its annihilator contains $m^{n+1} + E \supset J_{n+1}$. Commutative diagrams below are clearly in one-to-one correspondence with elements $\xi \in M$ which go to $\bar{1}$ in A/J_n :

$$\begin{tikzcd}
0 \arrow[r] & J_n/J_{n+1} \arrow[r] \arrow[d, "h"] & A/J_{n+1} \arrow[r] \arrow[d] & A/J_n \arrow[r] \arrow[d, "1"] & 0 \\
& k^m \arrow[r] & M \arrow[r] & A/J_n \arrow[r] & 0
\end{tikzcd}$$

But any two choices of ξ differ by an element of k^m which is annihilated by J_1, showing that h does not depend on the choice of ξ. Q.E.D.

Proposition 4 : If $\dim X = 1$, then $A \cong k\{\{X_1, X_2, \cdots, X\}\}$ which is the non-commutative formal power series ring in g variables, and $g = rk\, H^1(X, \mathbf{O}_X)$.

Proof : $A = \varprojlim_n A/J_n$. Choose $x_1, x_2, \cdots, x_g \in J_1$ so that they form a basis for J_1/J_2. Putting $B = k\{\{X_1, X_2 \cdots, X_g\}\}$ and sending X_j to the x_j for all j, there is a natural surjection $B \to A$. This is an isomorphism if and only if $B/m^n \to A/J_n$ is an isomorphism for all n. For this it suffices to show that

$$rk\,(A/J_n) = rk\,(B/m^n) = 1 + g + g^2 + \cdots + g^{n-1}.$$

But $rk\,(A/J_n) = rk\,(V_n)$ where the V_n are as in Lemma 7.

If $0 \to \mathbf{O}_X^l \to U(V_n) = V_{n+1} \to V_n \to 0$ is the universal extension of V_n, then $H^1(X, V_n^*) \xrightarrow{0} H^1(X, V_{n+1}^*) \to H^1(X, \mathbf{O}_X^l) \to H^2(X, V_n^*) = 0$ is exact and therefore $rk\, H^1(X, V_{n+1}^*) = lg$

$$= g\, rk\, H^1(X, V_n^*).$$

Therefore $rk\, H^1(X, V_n^*) = g^n$ for all n and $rk\, V_n = 1 + g + \cdots + g^{n-1}$ for all n. This proves the Proposition.

We shall use this Proposition a little later.

We know what $U(X, x_0)_{ab}$ is in characteristic zero. We attempt below to understand this in the general case.

First we need :

Definition : Pic X is the following functor from k-schemes to abelian groups for a k-scheme S, a member of Mor $(S, \text{Pic } X)$ is a line bundle on $X \times S$ with a chosen trivialisation on $x_0 \times S$.

Proposition 5 : Let B be a commutative local finite-dimensional (Artin) k-algebra with $B/m = k$.

The following data are equivalent :

1. A k-algebra homomorphism $A \to B$ that vanishes on some J_n ;
2. An element of Mor (Spec B, Pic X) which vanishes when restricted to Mor (Spec k, Pic X).

Proof : We are given a line bundle L on $Y = X \times \text{Spec } B$ with a trivialisation on $x_0 \times \text{Spec } B$ and $X \times \text{Spec } k$. Let p_1 and p_2 be the projections. For a B-module M, let $GM = (p_1)_* (L \otimes p_2^* \tilde{M})$.

This is a functor from $|B|$ to $N(X)$ such that there is a natural equivalence of the functors $T \circ G$ and the forgetful functor from $|B|$ to $|A|$. Recall that $T : N(X) \to |k|$ is defined by $T(V)$ = fibre of V at x_0. This gives

$$\begin{tikzcd}
B\text{-mod} \arrow[r, "G"] \arrow[dr] & N(X) \arrow[d, "T"] & A\text{-mod} \arrow[l] \arrow[dl] \\
& k\text{-mod} &
\end{tikzcd}$$

and therefore a functor from $|B|$ to $|A|$ which respects the forgetful functors from both to $|k|$. Applying this functor to B itself, we see that B becomes an A-module such that R_α = right multiplication by α for $\alpha \in B$ is a A-module homomorphism for all $\alpha \in B$. Consequently there is a k-algebra homomorphism from A to B.

Conversely, given $j : A \to B$, define G to be the composite : $|B| \to |A| \xrightarrow{F} N(X)$. Because $B = \mathrm{End}_{|B|}(B, B)$, it follows that $G(B)$ has an action of B ; equivalently, $G(B) = (p_1)_* L$ where L is a sheaf on $Y = X \times \operatorname{Spec} B$. We omit the checking that L is an invertible sheaf on Y.

As a consequence, we have :

Proposition 6 : Assume Pic X is representable. Then

1. A_{ab} = the completion of the local ring of Pic X at zero.

2. The natural homomorphism $A_{ab} \to A_{ab} \hat{\otimes} A_{ab}$ is induced by taking completions at zero of Pic $X \times$ Pic $X \to$ Pic X.

3. If char $k = p > 0$, then $U(X, x_0)_{ab} = \varprojlim_{G} \hat{G}$ where the inverse limit is taken over all local group-schemes G embedded in Pic X.

Proof ; 1 and 2 follows immediately from the previous Proposition. For 3, observe that

(a) The dual of the co-ordinate ring of $U(X, x_0)_{ab}$ is just A_{ab}.

(b) if $G_n \hookrightarrow$ Pic X is the local group-scheme defined by the ideal J_n generated by p^nth powers of all elements of the maximal ideal, then $A_{ab} = \varprojlim_{n} R(G_n)$, where $R(G_n)$ is the co-ordinate ring of G_n, and

(c) $R(\hat{G}_n) = R(G_n)^*$.

A morphism $(Y, y_0) \to (X, x_0)$ clearly induces a homomorphism $U(Y, y_0) \to U(X, x_0)$. Tne projections $X \times Y \to X$ and $X \times Y \to Y$ thus induce a homomorphism

$$U(X \times Y, x_0 \times y_0) \to U(X, x_0) \times U(Y, y_0).$$

Lemma 8 : The above homomorphism is an isomorphism.

Corollary : If X is an abelian variety, then $U(X, 0)$ is abelian.

Proof: The multiplication $X \times X \to X$ clearly induces $U(X \times X, 0 \times 0) = U(X, 0) \times U(X, 0) \to U(X, 0)$ which is just the multiplication in the group-scheme $(U(X, x_0)$. Because this is a homomorphism, $U(X, 0)$ is commutative.

Proof of Lemma : $i : X \to X \times Y$ defined by $X \to X \times y_0 \to X \times Y$ induces $U(X, x_0) \to U(X \times Y, x_0 \times y_0)$. Because $p_1 \circ i = 1_X$ and $p_2 \circ i =$ constant, it follows that the composite $U(X, x_0) \to U(X \times Y, x_0 \times y_0) \to U(X, x_0) \times U(Y, y_0)$ is just $a \mapsto (a, 0)$.

Thus we see that $U(X \times Y, x_0 \times y_0) \to U(X, x_0) \times U(Y, y_0)$ is surjective. To show that it is injective also, it suffices to show that any representation V of $U(X \times Y, x_0 \times y_0)$ is a quotient of $P \otimes Q$ where P and Q are representations of $U(X, x_0)$ and $U(Y, y_0)$ respectively. Or, what is the same, to show that any V in $N(X \times Y)$ is a quotient of $P \otimes Q$ where P and Q are in $N(X)$ and $N(Y)$ respectively.

Sublemma : If V and W are in $N(X)$ and $N(Y)$ respectively, then $U(V \otimes W)$ is a quotient of $U(V) \otimes U(W)$.

Proof: Let $0 \to H^1(X, V^*)^* \otimes_k \mathbf{O}_X \to U(V) \to V \to 0$ and $0 \to H^1(Y, W^*)^* \otimes_k \mathbf{O}_Y \to U(W) \to W \to 0$ be the universal extensions. The quotient of $U(V) \otimes U(W)$ by $H^1(X, V^*)^* \otimes H^1(Y, W^*)^* \otimes \mathbf{O}_{X \times Y}$ gives an exact sequence :

$$0 \to H^1(X, V^*)^* \otimes_k \mathbf{O}_X \otimes W \oplus H^1(Y, W^*)^* \otimes_k V \otimes \mathbf{O}_Y \to Z \to V \otimes W \to 0.$$

Also there are canonical surjections $V \to H^\circ(X, V^*)^* \otimes_k \mathbf{O}_X$ and $W \to H^\circ(Y, W^*)^* \otimes_k \mathbf{O}_Y$. This gives a surjection from Z to Z' with :

$$0 \to (H^1(X, V^*)^* \otimes H^\circ(Y, W^*)^* \oplus H^1(Y, W^*)^* \otimes H^\circ(X, V^*)^*) \otimes \mathbf{O}_{X \times Y} \to Z' \to V \otimes W \to 0$$

which by the Kunneth formula is easily seen to be the universal extension of $V \otimes W$. Q.E.D.

Let V_n be as in Lemma 7 and let W_n be the same sequence for Y. Using this sublemma, we shall show that any T in $N(X \times Y)$ of rank n is a quotient of $(V_n \otimes W_n)^n$ by induction on n.

If $n = 1$, this is obvious.

If $rk\, T = n + 1$, $0 \to \mathbf{O}_{X \times Y} \to T \to T' \to 0$ is exact with T' in $N(X \times Y)$. There is a surjection $(V_n \otimes W_n)^n \to T'$ by which one pulls back this extension by $\mathbf{O}_{X \times Y}$ to get the following diagram :

$$\begin{tikzcd}
 & & (V_{n+1} \otimes W_{n+1})^n \arrow[r] \arrow[d] & (V_n \otimes W_n)^n \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \Theta^l_{X \times Y} \arrow[r] \arrow[d] & U(V_n \otimes W_n)^n \arrow[r] \arrow[d] & (V_n \otimes W_n)^n \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \Theta_{X \times Y} \arrow[r] \arrow[d, "1"] & H \arrow[r] \arrow[d] & (V_n \; W_n)^n \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \Theta_{X \times Y} \arrow[r] & T \arrow[r] & T' \arrow[r] & 0
\end{tikzcd}$$

If $(V_{n+1} \otimes W_{n+1})^{n} \rightarrow T$ is not surjective, its image is a sub-bundle N of T such that $\mathbf{O}_{X \times Y} \oplus N = T$. In either case, it is clear that T is a quotient of $(V_{n+1} \otimes W_{n+1})^{n+1}$.

This finishes the proof of Lemma 8.

We come back to curves. Fix a $g \geqslant 1$.

We denote by $k\{\{X ; Y ; Z ; \cdots\}\}$ the non-commutative formal power series ring in $X_1, X_2, \cdot\ \cdot, X_g, Y_1, Y_2, \cdots, Y_g, Z_1, Z_2, \cdots Z_g, \cdots$, modulo the relations : $X_i \cdot Y_j = Y_j \cdot X_i$ for all i and j, $X_i \cdot Z_j = Z_j \cdot X_i$ for all i and j, $Y_i \cdot Z_j = Z_j \cdot Y_i$ for all i and j, etc.

A non-commutative formal group is a $F(X ; Y) = (F_1 (X ; Y), F_2 (X ; Y), \cdots F_g (X; Y))$ with the $F_i (X, Y) \in k\{\{X ; Y\}\}$ such that

(a) $F_i (X, 0) = F_i (0 ; X) = X_i$ for $1 \leqslant i \leqslant g$.

(b) $F(X ; Y) = F(Y ; X)$.

(c) $F(F(X : Y) ; Z) = F(X ; F(Y ; Z))$. This is an identity in $k\{\{X ; Y ; Z\}\}$.

Every complete curve X with $\Gamma(X, \mathbf{O}_X) = k$ gives rise to such a formal group: with A as usual, there is an isomorphism $A \cong k\{\{X\}\}$ and the homomorphism $k\{\{X\}\} \rightarrow A \cong A \hat{\otimes} A \cong k\{\{X ; Y\}\}$ provides the $F_i (X ; Y)$: put $F_i (X ; Y) =$ the image of X_i.

Given a non-commutative formal group, put $R =$ continuous linear functionals on $k\{\{X\}\}$. Then R is a Hopf algebra and $G =$ Spec R is an affine nilpotent group-scheme with $R^* = k\{\{X\}\}$.

In characteristic zero, after a change of co-ordinates, $F_i (X ; Y) = X_i + Y_i$. The lie algebra of the affine nilpotent group-scheme G is canonically identified to the completion of the lie sub-algebra of $k\{\{X\}\}$ generated by $X_1, X_2, \cdots, X_g$. This is an inverse limit of finite dimensional nilpotent lie algebras and the inverse limit of the corresponding nilpotent algebraic groups is precisely G.

In positive characteristic, the situation is more difficult. Even in the commutative case, a complete classification of such objects is given by Deindorne modules. We do not know as yet the non-commutative analogue of this. Essentially it amounts to a classification of finite nilpotent group-schemes.

Here are some elementary examples :

Example 1 : Take disjoint sets $S_1, S_2, \cdots, S_t$ of k-rational points of $\mathbf{P}'$ such that the sum of the cardinalities of the S_i is $g + t$. Let X be the "semi-normal" curve obtained by identifying all points of S_i to a single point y_i for $i = 1, 2, \cdots, t$.

Then $H^1 (X, \mathbf{O}_X)$ has rank g and the associated formal group is given by $F_i (X ; Y) = X_i + Y_i + X_i Y_i$.

X is semi-normal if the local ring completions of X are isomorphic to $k[[x_1, x_2, \cdots, x_n]]/(x_i x_j$ for all $i < j)$, for some n.

Proof : For simplicity assume that $S = S_1$ and $t = 1$, and $x_0, x_1, \cdots, x_g$ are the points of S. The image of x_0 in X will still be denoted by x_0.

If $f : \mathbf{P}^1 \rightarrow X$ is the normalisation map and W is in $N(X)$, then $f^* (W)$ is in $N(\mathbf{P}^1)$ and is therefore trivial. Thus $f^* W = V \otimes_k \mathbf{O}_{\mathbf{P}'}$ canonically, where V is the fibre of $f^* (W)$ at x_0. The diagram

$$\begin{tikzcd}
 & P^1 \arrow[dr, "f"] & \\
\mathrm{Spec}\, k \arrow[ur, "x_i"] \arrow[dr, "x_0"'] & & X \\
 & P^1 \arrow[ur, "f"'] &
\end{tikzcd}$$

gives an isomorphism of the fibres of $f^*(W)$ at x_0 and x_i for $1 \leqslant i \leqslant g$, *i.e.*, an automorphism ϕ_i of V for $1 \leqslant i \leqslant g$.

Using the filtration that W possesses, we see that there is a flag $V = V_0 \supseteq V_1 \supseteq V_2 \cdots \supseteq V_m = 0$ so that $\phi_i X - X \in V_{j+1}$ for all $x \in V_j$. Consequently $\phi_j - I_v = \psi_i$ has the property that $\psi_{i_0} \psi_{i_1} \cdots \psi_{i_m} = 0$ for all possible choices of $i_0, i_1, \cdots, i_m \in \{1, 2, \cdots, g\}$. This makes V a $k\{\{X\}\}$-module by letting the X_i act by ψ_i. This immediately gives :

$$\begin{tikzcd}
k\{\{X\}\}-\mathrm{mod} \arrow[rr, leftrightarrow, "\cong"] \arrow[dr] & & N(X) \arrow[dl, "T"] \\
 & k\text{-}\mathrm{mod} &
\end{tikzcd}$$

where the vertical arrows are the forgetful functor and evaluation at x_0 respectively. We have a natural isomorphism of A with $k\{\{X\}\}$ in this case (unlike the necessarily arbitrary isomorphism of Proposition 4).

If W' and W'' are in $N(X)$ with the corresponding ϕ_i' and ϕ_i'', then $W' \otimes W''$ is defined by $\phi_i' \otimes \phi_i''$. Putting $\phi_i' = 1 + \psi_i'$ and $\phi_i'' = 1 + \psi_i''$, this gives $\phi_i{}' \otimes \phi_i'' = 1 + \psi_i' \otimes 1 + 1 \otimes \psi_i'' + \psi_i' \times \psi_i''$, and therefore the homomorphism $k\{\{X\}\} \to k\{\{X\}\} \hat{\otimes} k\{\{X\}\}$ is given by $X_i \to X_i \otimes 1 + 1 \otimes X_i + X_i \otimes X_i$.

In our language, $F_i(X ; Y) = X_i + Y_i + X_i Y_i$. Q.E.D.

Example 2 : If $y_1, y_2, \cdots, y_g$ are k-rational points of P' and X is obtained from P' by introducing a simple cusp at $y_1, y_2, \cdots, y_g$ then $rk\, H^1(X, O_X) = g$, and $F(X ; Y) = X_i + Y_i$ in this case.

This means that $f : P^1 \to X$ is set—theoretically injective and if $f(y_i) = x_i$, then $O_{X, x_i} = k + m_i^2$ where m_i is the maximal ideal of O_{P^1, y_i}.

Proof : Choose a point $x_0 \in P^1$. Let W be in $N(X)$. As before $f^*W = V \otimes_P$ where V is the fibre of f^*W at x_0. Thus all fibres can be canonically identified to V. The diagram :

$$\begin{tikzcd}
\mathrm{Spec}\, k[q/q^2] \arrow[r] \arrow[d] & P' \arrow[d, "f"] \\
\mathrm{Spec}\, k \arrow[r, "x_i"] & X
\end{tikzcd}$$

gives an automorphism of $V \otimes k[q/q^2]$ which is the identity modulo q. Thus this automorphism ϕ_i is of the form $1 + q\psi_i$ where $\psi_i \in \mathrm{End}(V)$. Using the filtration of W, the ψ_i preserve a flag as in example 1, showing that V becomes a $k\{\{X\}\}$-module.

If W' and W'' are in $N(X)$ with the ϕ_i' and ϕ_i'', then $\phi_i' \otimes \phi_i'' = 1 + q(\psi_i' \otimes 1 + 1 \otimes \psi_i'')$ and this shows that

$$F(X\,;\,Y) = X_i + Y_i.$$

Example 3 : What is the affine group-scheme G associated to $F(X\,;\,Y) = X_i + Y_i + X_i Y_i$? In characteristic zero, we have already seen the answer, so we restrict ourselves to characteristic p with $p > 0$. Here the answer is : G is isomorphic to a free pro-p-group on g letters. In particular, G is reduced.

Proof : Let π be a free group on $u_1, u_2, \cdots, u_g$ and let P be its pro-p-completion.

Let $A(H)$ be the group algebra of a finite group H. Then $A(P) =$ dual of its co-ordinate ring $= \varprojlim_H A(H)$ where H runs through all finite p-quotients H of π.

Let $\rho : k\{X_1, X_2, \cdots, X_g\} \to A(P)$ be the homomorphism defined by $\rho(X_i) = u_i - 1$. For any finite p-quotient H of π, the composite $k\{X_1, X_2, \cdots, X_g\} \to A(P) \to A(H)$ is clearly surjective, andits kernel contains $(X_1, X_2, \cdots, X_g)^h$ where h is the cardinality of H. This is seen as usal by showing that $A(H)$ has a flag such that u_i acts by the identity on successive quotients. Therefore there is an induced diagram :

$$\begin{tikzcd}
k\{X_1, X_2, \ldots\ldots, X_g\} \arrow[r, "\rho"] \arrow[d] & A(P) \\
k\{\{X\}\} = k\{\{X_1, \ldots\ldots, X_g\}\} \arrow[ur, "\bar{\rho}"'] &
\end{tikzcd}$$

and $\bar{\rho}$ is a surjection.

Now consider $B_n = |\, k\{\{X\}\} \,|$ the n-th power of its maximal ideal. The image of the homomorphism $\pi \mid\!\to B_n^*$ given by $u_i \mid\!\to 1 + X_i$ is denoted by H_n. We shall show below (lemma 9) that H_n is a finite p-group. This induces $A(P) \to A(H_n) \to B_n$ for all n, and therefore a continuous homomorphism $A(P) \to \varprojlim_n B_n = k\{\{X\}\}$. This is seen to be the inverse of $\bar{\rho}$ quite easily.

The diagonal homomorphism $A(P) \to A(P) \hat{\otimes} A(P)$ is given by $u_i \to u_i \otimes u_i$. Under $\rho : k\{\{X\}\} \overset{\cong}{\to} A(P)$, this becomes $X_i \to X_i \otimes 1 \oplus 1 \otimes X_i \oplus X_i \otimes X_i$. This finishes the proof modulo the following well-known.

Lemma 9 : Any finitely generated subgroup of a nilpotent affine algebraic group in characteristic p is a finite p-group.

Proof : By induction on the dimension of the algebraic group N : there is an exact sequence $1 \to N_1 \to N \to G_a \to 1$. If H is the finitely generated subgroup, then $1 \to N_1 \cap H \to H \to G_a$ is exact. The image of H in G_a is a finite abelian p-group. Consequently $N_1 \cap H$ is of finite index in H and is therefore finitely generated. By induction, $N_1 \cap H$ is a finite p-group and therefore H itself is a finite p-group.

We need the following :

Lemma 10 : The letters A and B stand for inverse limits of finite dimensional local k-algebras with residue field k. It will also be assumed that they have finite dimensional m/m^2. Any such algebra will be called free if it is isomorphic to $k\{\{X_1, X_2, \cdots, X_g\}\}$ for some g.

A. If $f : A \to B$ is a homomorphism inducing a surjection on the m/m^2-level, then f is a surjection.

B. A homomorphism $f: A \to B$ inducing an isomorphic on the m/m^2-level is an isomorphism if there is a $g : B \to A$ such that $fg(X) = X$ for all $X \in B$.

C. If $f : A \to B$ induces an isomorphism on the m/m^2-level and B is free, then f is an isomorphism.

D. If A is free and $h_1, h_2, \cdots, h_r \in m$ are such that their images in m/m^2 are inearly independent, then $A/(h_1, h_2, \cdots, h_r)$ is free.

Proof; A. The hypothesis implies that there is a surjection on the m^n/m^{n+1} level for all n and this is enough.

B. Clearly g is injective. But g induces an isomorphism on the m/m^2-level implying by A that it is also surjective.

C. By Part A of the lemma, $f : A \to B$ is surjective. But B is free ; therefore there is a $g : B \to A$ such that $fg(x) = x$ for all $x \in B$. By Part B of the lemma, f is an isomorphism.

D. Choose $g_1, g_2, \cdots g_s$ in the maximal ideal so that the h_i an1 the g_j form a basis for m/m^2. Let B be a free algebra on $r+s$ generators and define $f : B \to A$ by sending the generators to the h_i and the g_j. By Part C, f is an isomorphism, therefore

$$A/(h_1,h_2, \cdots, h_r) \cong k\{\{X_1, X_2, \cdots, X_{r+s}\}\}/(X_1, X_2, \cdots, X_r) \cong k\{\{Y_1, Y_2, \cdots, Y_s\}\}.$$

This proves the lemma completely.

Lemma 11 : Let G be the affine group-scheme associated to a non-commutative formal group. Assume that k is perfect. Then G_{red} is also a group-scheme associated to a non-commutative formal group. If k is algebraically close then, G_{red} is a free pro-p-group.

Proof: Let A and B be the duals of the co-ordinate rings of G and G_{red} respectively. By assumption A is free, and the first assertion of the lemma is equivalent to the assertion that B is free.

The exact sequence $1 \to G_{\text{loc}} \to G \to G_{\text{red}} \to 1$ is split by the natural inclusion of G_{red} in G. This gives $j : A \to B$ and $i : B \to A$ so that $ji(x) = x$ for all $x \in B$. Choose $h_1, h_2, \cdots, h_r$ in the kernel of j so that their images in ker $(j) + m^2/m^2$ form a basis. Let $p : A \to A/(h_1, h_2, \cdots, h_r) = C$ be the projection. If $f \circ p = j$ and $p \circ i = g$, then $fg(x) = x$ for all $x \in B$. Also C is free by Lemma 10·D. By 10·B, f is an isomorphism, showing that B is free.

If k is algebraically closed, there is a surjection $h : F \to G_{\text{red}}$ where F is a free pro-p-group such that Hom $(G_{\text{red}}, Z/p) \to$ Hom $(F, Z/p)$ is an isomorphism. Consequently, $A(F) \to B$ induces an isomorphism on the m/m^2-level. But B is free and by 10·C it follows that $A(F) \to B$ is an isomorphism. Therefore $F \to G_{\text{red}}$ is an isomorphism.

Corollary (due to Safarevich) : Let X be a complete curve with $\Gamma(X, O_x) = k$. The maximal p-quotient of the etale fundamental group is a free pro-p-group in characteristic p.

If $f : Y \to X$ is a Galois etale covering of degree N where N is a power of p, and $r(Y)$ and $r(X)$ are the ranks of the Hasse-Witt matrices of Y and X respectively, then

$$r(Y) - 1 = N(r(X) - 1).$$

We first remark that Safarevich's proof is much shorter than ours.

Proof : In this set-up the maximal p-quotient of the etale fundamental group is just $U(X, x_0)_{\text{red}}$. By Lemma 11 and Proposition 4, this is a free pro-p-group. The second assertion is an immediate consequence.

We state without proof the following proposition which shows that $U(X, x_0)$ has flat variation at least in a special case :

Proposition 7 : Let $f : X \to S$ be a flat proper morphism with fibres of dimension one with $S = \operatorname{Spec} R$. Let $j : S \to X$ be a section. There is an affine group-scheme $U(X, j)$ which is S-flat such that for all $t : \operatorname{Spec} k \to S$, $U(X, j)_t = U(X_t, x_0)$ where x_0 is the base-point of X_t induced by j.

We assume that $f_* \mathbf{O}_s = \mathbf{O}_s$ and $R^1 f_* \mathbf{O}_s$ is locally free. If we assume further that $R^1 f_* \mathbf{O}_s = \mathbf{O}_s^g$, then this gives a non-commutative formal group $F(X : Y)$ with coefficients in R.

The proof is not difficult ; one has to construct the V_n as in Lemma 7 for this situation and construct the A/J_n as $\operatorname{End}(V_n)^\circ$.

We proved that $U(X, x_0) \times U(Y, y_0) = U(X \times Y, x_0 \times y_0)$. We conjecture that the same holds for the fundamental group-scheme. This would show that $\pi(X, 0)$ is abelian for an abelian variety X and this shows in fact that $\pi(X, 0) = \varprojlim_{G \hookrightarrow \hat{X}} \hat{G}$ where G ranges through all finite subgroup-schemes of $\hat{X}$. The best we can manage now is :

Proposition 8 : If k is perfect and X is an elliptic curve, then $\pi(X, 0) = \varprojlim_{G \to \hat{X}} \hat{G}$.

Proof : By Proposition 5, Chapter II, k may be replaced by any separable extension and therefore we may assume it is algebraically closed.

With the V_n as in Lemma 7, a theorem of Atiyah asserts that any semi-stable bundle of degree zero is a direct sum of bundles of the type $L \otimes V_n$ where L is a line bundle on X.

This gives us an easy classification of all essentially finite bundles on X : direct sums of $L \otimes V_n$ with L ranging through all line bundles of finite order.

There is a natural surjection $\pi(X, 0) \to \varprojlim_{G \to \hat{X}} \hat{G}$ and the representations of the group on the right already give all essentially finite bundles : if L is a line bundle of order m, this gives a $Z/m \to \hat{X}$, and the V_n come from representations of $U(X, 0)$ which by the Corollary to Lemma 8 is a quotient of $\varprojlim_{G \to \hat{X}} \hat{G}$.

∴ Therefore any representation of $\pi(X, 0)$ is already a representation of $\varprojlim_{G \to \hat{X}} \hat{G}$ showing that the homomorphism is indeed an isomorphism.

We examine finally the behaviour of $U(X, x_0)$ under base-change. Let L be any field extension of k and $(\bar{X}, \bar{x}_0)$ and $\overline{U(X, x_0)}$ be the base-change of (X, x_0) and $U(X, x_0)$ to L respectively. The universal properties show that there is a natural homomorphism $U(\bar{X}, \bar{x}_0) \to \overline{U(X, x_0)}$ with a commutative diagram :

$$\begin{tikzcd}
U(X, x_0)-\mathrm{mod} \arrow[r] \arrow[d, "F", "="'] & U(\bar{X}, \bar{x}_0)-\mathrm{mod} \arrow[d, "\bar{F}", "="'] \\
N(X) \arrow[r] & N(\bar{X})
\end{tikzcd}$$

where the horizontal arrows are the obvious ones and F is the given natural equivalence of categories.

Let B be the dual of the co-ordinate ring of $U(X, x_0)$ and let I_n be the closure of the n-th power of its maximal ideal. The arrow $U(\bar{X}, \bar{x}_0) \to \overline{U(X, x_0)}$ induces a continuous homomorphism $f : B \to A = A \otimes_k L$, and the first horizontal arrow in the above commutative diagram is induced by this homomorphism.

If W_n is defined inductively by $W_{n+1} = U(W_n)$ and $W_1 = \mathbf{O}_{\bar{x}}$, then $W_n = \bar{F}(B/I_n)$. But, by induction, it follows that $\bar{V}_n$ (which is the base-change of V_n to $\bar{X}$) is isomorphic to W_n, because $H^1(X, \bar{V}_n^*) = H^1(X, V_n^*) \otimes_k L$.

By the above commutative diagram, it follows that $(A/J_n) \otimes_k L$ considered as a B-module is isomorphic B/I_n, i.e., $f^{-1}(J_n \otimes L) = I_n$ and $B/I_n \to A \otimes_k L/J_n \otimes_k L$ is subjective for all n. From this, $f : B \to A$ is itself an isomorphism, showing that

Proposition 9 : With notation as above, $U(\bar{X}, \bar{x}_0) \to \overline{U(X, x_0)}$ is an isomorphism. In other words, $U(X, x_0)$ is invariant under base-change.

Appendix

Tannaka categories

Section 2 of this appendix contains the proofs of all the results about Tannaka categories that have been used freely (see chapter I, § 1). These follow easily enough from the results of § 1.

Section 1. Let k be a field. The only algebras considered here are k-algebras A equipped with a topology such that

(a) A/J is a finite dimensional k-vector space for all open two-sided ideals J, and

(b) $A \to \varprojlim_{J} A/J$ is an isomorphism where the J run through all open two-sided ideals in A.

In particular any finite dimensional k-algebra with the discrete topology will do

All k-algebra homomorphisms under consideration will be assumed to be continuous.

If A and B are such algebras, $A \otimes B$ has a topology by taking $\{ I \otimes B + A \otimes J :$ I and J are open two-sided ideals of A and B respectively$\}$ to be a basis of

The category of modules over a ring is denoted both by A-mod and | A | in the text.

neighbourhoods of zero. The completion $\varprojlim_{I,J} A \otimes B/I \otimes B + A \otimes J = \varprojlim_{I,J} A/I \otimes B/J$ will be denoted by $A \hat{\otimes} B$. Here a neighbourhood-basis consists of the kernels of $A \hat{\otimes} B \to A/I \otimes B/J$ with I and J as usual.

By $|A|$ we shall mean the category of left A-modules M which are finite-dimensional k-vector spaces and whose annihilators are open.

A homomorphism $f : A \to B$ induces a functor $H(f) : |B| \to |A|$. If $i_A : k \to A$ is the canonical inclusion, we put $H(i_A) = T_K$.

More generally, if $f : A \to B_1 \hat{\otimes} B_2 \hat{\otimes} \cdots \hat{\otimes} B_n$ is a homomorphism, then there is a functor $H(f) : |B_1| \times |B_2| \times \cdots \times |B_n|$.

The main result of this section is :

Proposition 1 : Let $\mathcal{C}$ be an abelian category with finite directsums. Assume that $\mathcal{C}(V, W) = \mathcal{C}$-morphisms from V to W, where V and W are objects of $\mathcal{C}$ has the structure of a k-vector space and that for objects V, W, P of $\mathcal{C}$, the composition $\mathcal{C}(V, W) \times \mathcal{C}(W, P) \to \mathcal{C}(V, P)$ is k-bilinear, Such a $\mathcal{C}$ will be called an abelian k-category.

Assume further that $\mathrm{Obj}\,\mathcal{C}$ is a set, and that $T : \mathcal{C} \to |k|$ is a faithful exact k-linear functor. The phrase " k-linear " in this context means that $T(V, W) : \mathcal{C}(V, W) \to \mathrm{Hom}_k(TV, TW)$ is k-linear for all objects V and W of $\mathcal{C}$.

There is then an algebra $A(\mathcal{C})$ and an equivalence $F : \mathcal{C} \to |A(\mathrm{C})|$ with the commutative diagram :

$$\begin{tikzcd}
\mathcal{C} \arrow[rr, "F"] \arrow[dr, "T"'] & & A(\mathcal{C})\text{-mod} \arrow[dl, "T_k"] \\
& k\text{-mod} &
\end{tikzcd}$$

The proof of this Proposition will take up the rest of this section.

The construction of $A(\mathcal{C})$:

This is forced on us. Suppose we are given a commutative diagram ;

$$\begin{tikzcd}
\mathcal{C} \arrow[rr, "R"] \arrow[dr, "T"'] & & B\text{-mod} \arrow[dl, "T_k"] \\
& k\text{-mod} &
\end{tikzcd}$$

Then, for all objects V of $\mathcal{C}$, TV becomes a B-module in a natural way and therefore there is a homomorphism $\rho_V : B \to \mathrm{End}(TV)$ vanishing on some open two-sided ideal.

If $f \in \mathcal{C}(V, W)$, then $Tf : TV \to TW$ is B-linear showing $Tf \circ \rho_V(b) = \rho_W(\mathrm{b}) \circ Tf$ for all $b \in B$.

Put $\rho = \prod_V \rho_V : B \to \prod_{V \in \mathrm{Obj}\,\mathcal{C}} \mathrm{End}(TV)$ and let $\pi_W : \prod_{V \in \mathrm{Obj}\,\mathcal{C}} \mathrm{End}(TV) \to \mathrm{End}(TW)$ be the projection for each $W \in \mathrm{Obj}\,\mathcal{C}$.

Then $Tf \circ \pi_V(\rho(b)) = \pi_W(\rho(b)) \circ Tf$.

Therefore, if $A(\mathcal{C}) = \{a \in \prod_{V \in \mathrm{Obj}\,\mathcal{C}} \mathrm{End}\, TV \mid \forall f \in \mathcal{C}(V, W), \forall V \in \mathrm{Obj}\,\mathcal{C}, \forall W \in \mathrm{Obj}\,\mathcal{C}, Tf \circ \pi_V(a) = \pi_W(a) \circ Tf\}$, the image of ρ is contained in $A(\mathcal{C})$, Furthermore, if $\prod_{V \in \mathrm{Obj}\, C} \mathrm{End}\ TV$ is given the product topology (with all finite dimensional spaces having the discrete topology), clearly $B \to A(\mathcal{C})$ is continuous.

Finally, for all $V \in \mathrm{Obj}\, \mathcal{C}$, $A(\mathcal{C}) \to \prod_{V \in \mathrm{Obj}\, C} \mathrm{End}\ TV \xrightarrow{\pi_V} \mathrm{End}\ TV$ makes TV an object of $|A(\mathcal{C})|$which we shall denote by FV. All this goes to show that we have a commutative diagram :

$$\begin{tikzcd}
\mathcal{C} \arrow[rr, "F"] \arrow[dr, "T"'] & & A(\mathcal{C})\text{-mod} \arrow[dl, "T_k"] \\
& k\text{-mod} &
\end{tikzcd}$$

and that any other commutative diagram

$$\begin{tikzcd}
\mathcal{C} \arrow[rr, "R"] \arrow[dr, "T"'] & & B\text{-mod} \arrow[dl, "T_k"] \\
& k\text{-mod} &
\end{tikzcd}$$

is induced by a unique $\rho : B \to A(\mathcal{C})$; in other words, $R = H(\rho) \circ F$.

If $(\mathcal{C}, T) = (|A|, T_k)$ it is easy to see that $A = A(\mathcal{C})$ canonically. This proves:

Corollary : a $F : |A| \to |B|$ such that $T_k \circ F = T_k$ is equal to $H(\rho)$ for a unique $\rho : B \to A$. However we need the following slightly stronger statement for §2.

Proposition 2 : Let $\otimes^n : |k| \times |k| \times \cdots \times |k| \to |k|$ be the usual tensoring functor. The functors $F : |B_1| x \times |B_2| \times \cdots \times |B_n| \to |A|$ such that $T_k \circ F = \otimes^n \circ (T_k \times T_k \times \cdots \times T_k)$ are in one-one correspondence with $f : A \to B_1 \hat{\otimes} B_2 \hat{\otimes} \cdots \hat{\otimes} B_n$.

Proof : For ease of writing, we take $n = 2$.

We may ignore T_k if we agree to identify modules with their underlying vector spaces. What F does is the following :

A. For objects M_1 and M_2 of $|B_1|$ and $|B_2|$, there is an A-module structure on $M_1 \otimes M_2$. For $a \in A$ and $m \in M_1 \otimes M_2$, the multiple of m by a will be denoted by $a \cdot m$.

B. If $f_1 : M_1 \to N_1$ and $f_2 : M_2 \to N_2$ are module homomorphisms for B_1 and B_2 respectively, then $f_1 \otimes f_2$ is a A-module homomorphism.

In particular, putting $B_1/J_1 = M_1 = N_1$ and $B_2/J_2 = M_2 = N_2$ for two-sided open ideals J_1 and J_2, and f_i = right multiplication by $b_i \in B_i/J_i$ for $i = 1$ and 2, we see that the A-action on $B_1/J_1 \otimes B_2 J_2$ commutes with all right multiplications. Consequently there is a homomorphism $h(J_1, J_2) : A \to B_1/J_1 \otimes B_2/J_2$ such that $a \cdot m = (h(J_1, J_2)\, a)m$ for all $a \in A, m \in B_1/J_1 \otimes B_2/J_2$.

It is easy enough to see that the $h(J_1, J_2)$ form an inverse system giving rise to $h : A \to B_1 \hat{\otimes} B_2$, such that the composite

$$\begin{tikzcd}
A \arrow[r, "h"] \arrow[rr, bend right, "h(J_1, J_2)"'] & B_1 \hat{\otimes} B_2 \arrow[r] & B_1/J_1 \otimes B_2/J_2
\end{tikzcd}$$

We shall show that $F = H(h)$, *i.e.*, for all $m \in M_1 \otimes M_2$, $a \in A$, $a \cdot m = h(a)\, m$. If M_1 and M_2 are annhilated by J_1 and J_2 respectively, define $f_i : B_i/J_i \to M$ by $f_i(b) = bm_i$ for $i = 1, 2$, Then $a \cdot (m_1 \otimes m_2) = a \cdot ((f_1 \otimes f_2 (1 \otimes 1)) = (f_1 \otimes f_2)(a \cdot (1 \otimes 1)) = (f_1 \otimes f_2)(h(a)) = h(a)(m_1 \otimes m_2)$.

But the $m_1 \otimes m_2$ generate all of M so that $a \cdot m = h(a)\, m$ always. Therefore $F = H(h)$.

Given $f : A \to B_1 \otimes B_2$ and $F = H(f)$ it is easy to see that the h constructed above equals f. This establishes the one-to-one correspondence and completes the proof of Proposition 2.

We have already constructed $F : \mathcal{C} \to |A(\mathcal{C})|$. To show that this is an equivalence, we must prove :

*F*1. For all V and W in $\mathcal{C}$, $\mathcal{C}(V, W) \to \mathrm{Hom}_{A(\mathcal{C})}(FV, FW)$ is an isomorphism. Note that it is already a monomorphism because $T = T_k \circ F$ is faithful.

*F*2. For every M in $|A(\mathcal{C})|$ there is a V in $\mathcal{C}$ such that $FV = M$.

What we need is functors going the other way :

Lemma 1 : Let B be finite dimensional k-algebra. Diagrams

$$\begin{tikzcd}
B\text{-mod} \arrow[r, "G"] \arrow[dr] & \mathcal{C} \arrow[d] \\
 & k\text{-mod}
\end{tikzcd}$$

are in one-one correspondence with the data :

1. An object N of $\mathcal{C}$ and an isomorphism $TN \cong B$,
2. a k-linear $\rho : B \to \mathcal{C}(N, N)$ such that under the above isomorphism $T_\rho(b)$ = right multiplication by $b \in B$.

Proof : Given G, put $GB = N$. Then $B = T_k GB = TN$, and if $R_b : B \to B$ is right multiplication by $b \in B$, put $\rho(b) = G(R_b)$.

Conversely given N, the isomorphism $TN \cong B$, and $\rho : B \to \mathcal{C}(N, N)$. First note that $\rho(a) \circ \rho(b) = \rho(ba)$ for all $a, b \in B$. This is so because T is faithful and $T(\rho(a)\rho(b)) = R_a R_b = R_{ba} = T(\rho(ba))$.

Let P be any object of $|B|$. Fix a presentation :

$$B^p \xrightarrow{h} B^q \to P \to 0.$$

If h is given by the matrix (h_{ij}), define GP by an exact sequence in $\mathcal{C}$:

$$N^p \xrightarrow{\rho(h)} N^q \to GP \to 0$$

where $\rho(h)$ is the matrix with entries $\rho(h_{ij})$.

If $f : P \to Q$ is a B-module homomorphism and $B^s \overset{h'}{\to} B^q \to Q \to 0$ is the chosen presentation of Q, then there is a diagram :

$$\begin{tikzcd}
B^p \arrow[r, "h"] \arrow[d, "r'"'] & B^q \arrow[r] \arrow[d, "r"] & P \arrow[r] \arrow[d, "f"] & 0 \\
B^r \arrow[r] & B^s \arrow[r] & Q \arrow[r] & 0
\end{tikzcd}$$

which in turn induces a unique diagram :

$$\begin{tikzcd}
N^p \arrow[r, "\rho(h)"] \arrow[d, "\rho(r')"'] & N^q \arrow[r] \arrow[d, "\rho(r)"] & GP \arrow[r] \arrow[d, "l"'] & 0 \\
N^r \arrow[r, "\rho(h')"] & N^s \arrow[r] & GQ \arrow[r] & 0
\end{tikzcd}$$

Now $l : GP \to GQ$ does not depend on the choice of r and r' because Tl : $TGP \to TGQ$ is just $T_k f : T_k P \to T_k Q$ and T is faithful. Put $Gf = l$.

This defines G. We omit to check that G is a k-linear functor and the fact that this establishes a one-to one correspondence with the G and the N with the above data.

Lemma 2 : With N and G as above, there is a unique $f : A(\mathcal{C}) \to B$ such that $F \circ G = H(f)$. Thus if P and Q are B-modules, $V = GP$ and $W = GQ$, then $FV = H(f)P$ and $FW = H(f)\,Q$ and the image of $F : \mathcal{C}(V, W) \to \mathrm{Hom}_{A(\mathcal{C})}$ (FV, FW) contains the image of $\mathrm{Hom}_B(P, Q) \to \mathrm{Hom}_{A(\mathcal{C})}(FV, FW)$.

Proof : The existence and uniqueness of f follows from Proposition 2. The next assertion follows from the diagram :

$$\begin{tikzcd}
\mathrm{Hom}_B(P, Q) \arrow[r, "G(P,Q)"] \arrow[rr, bend right, "H(f)(P,Q)"'] & \mathcal{C}(V, W) \arrow[r, "F(V,W)"] & \mathrm{Hom}_{A(\mathcal{C})}(FV, FW)
\end{tikzcd}$$

We shall use this lemma while proving $F1$.

Lemma 3 : With N and G and B as in Lemma 1, we shall characterise GP for P in $|B|$.

Given (a) $V \in \mathrm{Obj}\,\mathcal{C}$

(b) $h : P \to \mathcal{C}(N, V)$

a k-linear map such that $h(ap) = h(p) \circ \rho(a)$ for all $a \in B$, so that

(c) $\tilde{h} : P \to TV$ defined by $\tilde{h}(p) =$ the value at 1 of $T(h(p)) : TN \cong B \to TV$ for all $p \in P$, is an isomorphism, then $V = GP$. In future, GP will be denoted by $N \otimes_B P$.

This is fairly obvious so we skip the proof.

Lemma 4 : Let N and B be as in Lemma 1. Let $\phi : B \to C$ be an algebra homomorphism with C finite dimensional. Let Q be a left C-module. Then

(a) there is an anti-homomorphism $\tilde{\rho} : C \to \mathcal{C}(N \otimes_B C, N \otimes_B C)$ and an isomorphism $\mathcal{C} \cong T(N \otimes_B C)$ so that $T(c)$ is right multiplication by c for all $c \in C$ under this isomorphism.

(b) $(N \otimes_B C) \otimes_C Q \cong N \otimes_B Q$ with Q considered as a B-module in an obvious manner.

Proof (a) : With G as in Lemma 1, the anti-homomorphism $C \to \mathrm{End}_C(C, C) \to \mathrm{End}_B(C, C)$ induces the anti-homomorphism $\tilde{\rho} : C \to \mathcal{C}(GC, GC)$. The rest of (a) follows from the fact that $T_k = T \circ G$.

(b) Let $V = (N \otimes_B C) \otimes_C Q$. Then there is a k-linear $h : Q \to (N \otimes_B C, V)$ such that $h(cq) = h(q) \circ \tilde{\rho}(c)$ for all $c \in C$, $q \in Q$. Using $G\varphi : GB = N \to GC = N \otimes_B C$, we define $h'(q) = h(q) \circ G\phi$. This gives $h' : Q \to \mathcal{C}(N, V)$. We check that h' has the desired properties :

1. $$\begin{aligned} h'(q) \circ \rho(b) &= h(q) \circ G\phi \circ G(R_b) \\ &= h(q) \circ \tilde{\rho}(\varphi b) \circ G\phi \\ &= h(\phi(b)\, q) \circ G\phi \\ &= h'(\phi(b)\, q). \end{aligned}$$

2. We need to show that $q \mapsto (T h'(q))(1)$ is an isomorphism from Q to $T((N \otimes_B C) \otimes Q)$. But this is the same as $q \mapsto (T h(q))(1)$ because there is a commutative diagram

$$\begin{tikzcd} TGB \arrow[r, "T\phi"] \arrow[d] & TGC \arrow[d] \\ B \arrow[r, "\phi"] & C \end{tikzcd}$$

which takes 1 to 1. This finishes the proof of the lemma.

Definition : A pair (B, N) with the data as in Lemma 1 will be called a ring object in $\mathcal{C}$. For a P in $|B|$, GP will be denoted by $N \otimes_B P$.

We shall now construct plenty of ring objects in $\mathcal{C}$. For any subset S of Obj $\mathcal{C}$, let $C(S) = \prod_{V \in S} \mathrm{End}(TV)$ and let $\pi_V : C(S) \to \mathrm{End}(TV)$ be the projection for $V \in S$.

Let $A(S) = \{a \in C(S) \mid \forall V \in S, \forall W \in S, \forall f \in \mathcal{C}(V, W), Tf \circ \pi_V(a) = \pi_W(a) \circ Tf\}$

There is a natural homomorphism $A(\mathcal{C}) \to A(S)$.

All subsets of Obj $\mathcal{C}$ considered from now on will be assumed to be finite.

Lemma 5 : $A(\mathcal{C}) \to \varprojlim_{S} A(S)$ is an isomorphism.

This is obvious.

Lemma 6 : For each finite $S \in \operatorname{Obj} \mathcal{C}$, let $\tilde{A}(S)$ be the image of $A(\mathcal{C})$ in $A(S)$. Then

(a) there is a finite T containing S such that $A(T) \to A(S)$ has its image equal to $\tilde{A}(S)$, and

(b) $A(\mathcal{C}) = \varprojlim\limits_{S} \tilde{A}(S)$.

Proof : (b) is clear so we need to prove only (a).

Let $A_T(S)$ be the image of $A(T) \to A(S)$ for all T containing S. There is some T containing S for which $\dim A_T(S)$ is the least possible. Consequently for all $T' \supseteq T$, $A_{T'}(S) \to A_T(S)$ is an isomorphism. Put $A_T(S) = X(S)$.

If $S_1 \subseteq S_2$, choose T_1 and T_2 containing S_1 and S_2 respectively with the above property. If $T = T_1 \cup T_2$, the diagram

$$\begin{tikzcd}
 & A(T_1) \arrow[rr] & & A(S_1) \\
A(T) \arrow[ur] \arrow[dr] & & & \\
 & A(T_2) \arrow[r] & A(S_2) \arrow[uur] &
\end{tikzcd}$$

shows that the image of $X(S_2)$ in $A(S_2) \to A(S_1)$ is precisely $X(S_1)$. Clearly, $\varprojlim\limits_{S} X(S) \to \varprojlim\limits_{S} A(S)$ is an isomorphism. But $\{X(S)\}$ is an inverse system of surjections showing that the image of $A(\mathcal{C}) \to A(S)$ is precisely $X(S)$. Therefore $X(S) = \tilde{A}(S)$ and this proves the lemma.

For every (finite) subset S of $\operatorname{Obj} \mathcal{C}$ we shall construct ring objects $(A(S), B(S)$ and $(C(S), D(S))$.

We need first to make some trivial remarks: there is a unique functor $\operatorname{Hom} |k| \times \mathcal{C} \to \mathcal{C}$ which is k-linear in each variable, contravariant in the first and covariant in the second variable, and which satisfies : $\mathcal{C} \to \mathcal{C}$ defined by $W \to \operatorname{Hom}(k, W)$ is the identity functor.

Moreover there is a commutative diagram :

$$\begin{tikzcd}
k\text{-mod} \times \mathcal{C} \arrow[r, "\text{Hom}"] \arrow[d, "1 \times T"] & \mathcal{C} \arrow[d, "T"'] \\
k\text{-mod} \times k\text{-mod} \arrow[r, "\text{Hom}"] & k\text{-mod}
\end{tikzcd}$$

where the Hom in the second row is the usual one.

The category $|k|$ can be assumed to have objects k^n for $n = 0, 1, 2, \cdots$. Define $\operatorname{Hom}(k^n, W) = W^n$ for all $W \in \operatorname{Obj} \mathcal{C}$.

Given $f : k^n \to k^m$ and $g : W_1 \to W_2$ with W_1 and W_2 in $\mathcal{C}$, the corresponding homomorphism from $\operatorname{Hom}(k^m, W_1) \to \operatorname{Hom}(k^n, W_2)$, *i.e.*, from $W_1^m \to W_2^n$ is given by $\sum\limits_{r,s} f_{rs}\, i_r \circ g \circ p_s$ where $i_r : W_2 \to W_2^n$ is the r-th inclusion,

$p_s : W_1^m \to W_1$ the s-th projection and the f_{rs} are the coefficients of the matrix f.

We have stated the Hom functor in basis-free language to avoid choosing bases for plenty of vector spaces which could be very cumbersome.

Definition : If $f : W_1 \to W_2$ is a linear transformation and $V \in \text{Obj } \mathcal{C}$, the $\mathcal{C}$ morphism from $\text{Hom}(W_2, V)$ to $\text{Hom}(W_1, V)$ will be denoted simply by R_f.

If $f \in \mathcal{C}(V_1, V_2)$ and W is a vector space, the $\mathcal{C}$-morphism from $\text{Hom}(W, V_1) \to \text{Hom}(W, V_2)$ will be denoted by L_f.

We now define the $D(S)$ and $B(S)$:

$D(S) = \bigoplus_{V \in S} \text{Hom}(TV, V)$. Clearly $TD(S) = C(S)$ canonically. For $V, W \in S$ and $f \in \mathcal{C}(V, W)$ we define $\alpha(f) \in \mathcal{C}(D(S), \text{Hom}(TV, W))$ by $\alpha(f) = L_f \circ p_V - R_{Tf} \circ p_W$ where the p_V and p_W are projections from $D(S)$ to $\text{Hom}(TV, V)$ and $\text{Hom}(TW, W)$ respectively.

Clearly $T(\alpha(f)) : C(S) \to \text{Hom}(TV, TW)$ is given by $T(\alpha(f))\, a = Tf \circ \pi_V(a) - \pi_W(a) \circ Tf$.

Define $B(S) = \bigcap_{f \in C(V, W);\, V,\, W S} \ker(\alpha(f))$. This makes sense because it is a finite intersection : any collection of f that span all the $\mathcal{C}(V, W)$ with V and W in S will do.

Clearly $TB(S) = A(S)$.

Lemma 7 : $(A(S), B(S))$ and $(C(S), D(S))$ are ring objects for all finite sets S. In addition,

1. $B(S) \otimes_{A(S)} C(S) = D(S)$
2. if $S_1 \subseteq S_2$, then $B(S_2) \otimes_{A(S_2)} A(S_1) = B(S_1)$
3. if $S_1 \subseteq S_2$, then $D(S_2) \otimes_{C(S_2)} C(S_1) = D(S_1)$.

Lemma 8 : If $S = \{V\}$ is a singleton, then TV is a $C(V) = \text{End}(TV)$-module for which $D(V) \otimes_{C(V)} TV = V$.

We first show that these lemmas together imply that F is an equivalarce of functors. We first check $F2$.

Let M be an $A(\mathcal{C})$-module. Then M is an $\tilde{A}(S)$-module for some finite S and by lemma 6, $A(T) \to \tilde{A}(S)$ is a surjection for a suitable T containing S. Consequently M may be regarded as a $A(T)$-module. By lemma 2, $F(B(T) \otimes_{A(T)} M)$ is isomorphic to M. Therefore F induces a surjection from Obj $\mathcal{C}$ to $|\text{Obj}(A(\mathcal{C})|$,

Now we come to $F1$. For V and W in $\mathcal{C}$, we have to prove that $\mathcal{C}(V, W) \to \text{Hom}_{A(C)}(FV, FW)$ is a surjection. Let $S = \{V, W\} \subseteq \text{Obj } \mathcal{C}$. Then TV and TW are $A(S)$-modules in a natural manner and the corresponding $A(\mathcal{C})$-module structures induced by $A(\mathcal{C}) \to A(S)$ are precisely FV and FW respectively. Choose any $R \subset \text{Obj } \mathcal{C}$ which contains S. Let $S_1 = \{V\}$ and $S_2 = \{W\}$.

By Lemma 4 and Lemma 7, we have :

$$B(R) \otimes_{A(R)} TV = (B(R) \otimes_{A(R)} A(S_1)) \otimes_{A(S_1)} TV = B(S_1) \otimes_{A(S_1)} TV, \text{ and}$$

$$B(S_1) \otimes_{A(S_1)} TV = (B(S_1) \otimes_{A(S_1)} C(S_1)) \otimes_{C(S_1)} TV = D(S_1) \otimes_{C(S_1)} TV.$$

By Lemma 8, $D(S_1) \otimes_{C(S_1)} TV = V$. Thus we have : $B(R) \otimes_{A(R)} TV = V$ and $B(R) \otimes_{A(R)} TW = W$. By Lemma 2, the image of $\mathcal{C}(V, W) \to \text{Hom}_{A(C)}(FV, FW)$

contains all the $A(R)$-module homomorphisms from FV to FW. By choosing R large enough (by lemma 6), $A(R) \to A(S)$ has its image equal to $\tilde{A}(S)$, and for such R the $A(R)$-module homomorphisms and $A(\mathcal{C})$-module homomorphism are the same. This finishes the proof of Proposition 1 modulo Lemmas 7 and 8.

We retain the use of R_f and L_f defined by the Hom functor.

To define $\rho : C(S) \to \mathcal{C}(D(S), D(S))$, first consider the $\mathcal{C}$-morphism $R_{\pi_v(a)}$; $\mathrm{Hom}(TV, V) \to \mathrm{Hom}(TV, V)$ for all $V \in S$ and put $\rho(a) = \bigoplus\limits_{V} R_{\pi_v(a)}$. With the natural identification of $TD(S)$ with $C(S)$ clearly $T\rho(a)$ is right multiplication by a.

This proves that $(C(S), D(S))$ is a ring object.

To show that $(A(S), B(S))$ is a ring object, it suffices to show that $\rho(a)B(S) \subseteq B(S)$ for all $a \in A(S)$.

Take any $a \in C(S)$. Then

$$\begin{aligned} &\rho(a)B(S) \subseteq B(S) \\ &\Leftrightarrow 0 = \rho(a)B(S) + B(S)/B(S) \\ &\Leftrightarrow 0 = T(\rho(a)B(S) + B(S)/B(S)) \text{ by the faithfulness of } T \\ &\qquad = A(S)a + A(S)/A(S) \text{ by the exactness of } T \\ &\Leftrightarrow a \in A(S). \end{aligned}$$

Therefore $(A(S), B(S))$ is a ring object.

The k-linear map : $C(S) \to \mathcal{C}(D(S), D(S)) \to \mathcal{C}(B(S), D(S))$ after an application of T becomes $D(S) \to \mathrm{Hom}_k(A(S), C(S))$ which is just $a \mapsto$ the restriction of the right multiplication by a to $A(S)$, for all $a \in C(S)$. This proves 7·1 :

$$B(S) \otimes_{A(S)} C(S) = D(S).$$

7·2 and 7·3 are equally clear : look at

$$C(S_2) \to \mathcal{C}(D(S_2), D(S_2)) \to \mathcal{C}(D(S_2), D(S_1)) \text{ and}$$

$$A(S_2) \to \mathcal{C}(B(S_2), B(S_2)) \to \mathcal{C}(B(S_2), B(S_1)) \text{ given by}$$

composing with the projections $D(S_2) \to D(S_1)$ and $B(S_2) \to B(S_1)$ respectively.

It only remains to prove Lemma 8. Here the ring object is $(C, N) = (\mathrm{End}\ TV, \mathrm{Hom}(TV, V))$, and $\rho : \mathcal{C}(N, N)$ is given by $\rho(f) = R_f$. To show that $N \otimes_C TV = V$, we need to :

1. define $h : TV \to \mathcal{C}(C, V)$

2. check that $h(ap) = h(p) \circ \rho(a)$ for all $p \in TV$, $a \in C$, and

3. check that $\tilde{h} : TV \to TV$ is an isomorphism.

Every $p \in TV$ gives $A(p) : k \to TV$ and induces therefore a $\mathcal{C}$-morphism $R_{A(P)}$ $\mathrm{Hom}(TV, V) = C \to \mathrm{Hom}(k, V) = V$. We define $h(p) = R_{A(p)}$.

This takes care of condition 1.

To see 2, we must show that $h(ap) = h(p) \circ \rho(a)$, for all $a \in \mathrm{End}(TV)$, for all $p \in TV$. The composite $k \xrightarrow{A(p)} TV \xrightarrow{a} TV$ is piecisely $A(ap)$, so $h(ap) = R_{A(ap)} = R_{a \circ A(p)} = R_{A(p)} \circ R_a = h(p) \circ \rho(a)$.

Next we show that $\bar{h}$ is the identity. Note that $T(h(p)) : \mathrm{End}(TV) \to TV$ is just $a \to a(p)$ for all $a \in \mathrm{End}(TV)$. Therefore $\bar{h}(p) = T(h(p))\,1 = p$. Q.E.D.

Proposition 3 : $f : A \to B$ is surjective if and only if $H(f) : |B| \to |A|$ is fully faithful and any exact sequence : $0 \to W' \to H(f)\,V \to W'' \to 0$ is isomorphic to the $H(f)$-image of an exact sequence

$$0 \to V' \to V \to V'' \to 0 \text{ in } |B|.$$

Proof : If f is indeed surjective, that these properties are enjoyed by $H(f)$ is absolutely clear.

Conversely, we have to show that $A \to B/J$ is surjective for all open two-sided ideals J of B given the hypothesis on $H(f)$. Let I be the kernel of $A \to B/J$. Then $0 \to A/I \to H(f)(B/J) \to H \to 0$ shows that there is $N \hookrightarrow B/J$ and a commutative diagram :

$$\begin{tikzcd}
H(f)N \arrow[rr] \arrow[dr, "\cong"'] & & H(f)(B/J) \\
& A/I \arrow[ur] &
\end{tikzcd}$$

In other words the image of A/I and B/J is a B-module, *i.e.*, it is an ideal on B/J. But 1 is in this image : Therefore $A/I \to B/J$ is an isomorphism. Q.E.D.

Remarks : 1. We have been purposely careless by identifying functors when in truth there is only a natural equivalence between them.

2. We could have extended the G of Lemma 1 to a $G : |A(\mathcal{C})| \to \mathcal{C}$ such that $F \circ G =$ identity. But this would have been much more tedious to write out. To check $F1$ and $F2$, defining G at a finite stage, *i.e.*, from $|A(S)| \to \mathcal{C}$ suffices as we have already seen.

§2. *Tannaka categories*

If $G = \mathrm{Spec}\, R$ is an affine group-scheme over k, let $|G|$ be the category of finite dimensional G-representations. If $A = R^*$, then A becomes an algebra in the sense of § 1 and it is easy to see that $|A| = |G|$ canonically. Let $T_k : |G| \to |k|$ be the "forgetful functor" as usual. The multiplication homomorphism $a \otimes b \mapsto ab$ from $R \otimes R \to R$ induces $\triangle : A \to A \hat{\otimes} A$. Given representations V and W of A, $V \otimes W$ becomes an $A \hat{\otimes} A$-module and by using $\triangle$ it becomes a A-module again. This is just the tensor product of representations V and W; it will be denoted by $V \hat{\otimes} W$. Let L_0 be the trivial representation.

Putting $|G| = \mathcal{C}$, $T_k = T$, the $(\mathcal{C}, T, \hat{\otimes}, L_0)$ has the following properties :
$\mathcal{C}1$, $\mathcal{C}2$, $\mathcal{C}3$: the pair $(\mathcal{C}, T)$ satisfies the hypothesis of Proposition 1,
$\mathcal{C}4$, $\hat{\otimes} : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ is a covariant functor which is k-linear in each variable, and

$$\begin{tikzcd}
\mathcal{C} \times \mathcal{C} \arrow[r, "\hat{\otimes}"] \arrow[d, "T \times T"] & \mathcal{C} \arrow[d, "T"] \\
k\text{-mod} \times k\text{-mod} \arrow[r, "\otimes"] & k\text{-mod}
\end{tikzcd}$$

commutes, where $\otimes$ is the usual tensoring functor.

$\mathcal{C}$ 5 : $\hat{\otimes}$ is associative preserving T : there is a natural equivalence of the functors from $\mathcal{C} \times \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ given by $\hat{\otimes} \circ (l_C \times \hat{\otimes})$ and $\hat{\otimes} \circ (\hat{\otimes} \times l_C)$ such that for all objects P, Q, R of $\mathcal{C}$, the isomorphism $H(P, Q, R)$ from $P \hat{\otimes} (Q \hat{\otimes} R)$ to $(P \hat{\otimes} Q) \hat{\otimes} R$ after an application of T gives the standard isomorphism $TP \otimes (TQ \otimes TR) \to (TP \otimes TQ) \otimes TR$ which gives the associativity of the tensor product for k-modules.

$\mathcal{C}$ 6 : $\hat{\otimes}$ is commutative preserving T (in the above sense).

$\mathcal{C}$7 : the functor $\mathcal{C} \to \mathcal{C}$ given by $P \mapsto L_0 \hat{\otimes} P$ is naturally equivalent to the identity functor, and there is an isomorphism $k \cong T_{L_0}$ so that for all $P \in$ Obj $\mathcal{C}$. $L_0 \hat{\otimes} P \overset{\cong}{\to}$ P yields after T an isomorphism :
$k \otimes TP \to TL_0 \otimes TP \to TP$ which is the standard isomorphism $a \otimes P \to a p$.

8 : If $L \in$ Obj $\mathcal{C}$ and TL has dimension one, there is a L^{-1} such that $L \hat{\otimes} L^{-1} \cong L_0$

$A(\mathcal{C}, T, \hat{\otimes}, L_0)$ satisfying all the above properties is called Tannaka category, The aim here is to prove :

Proposition 4 : Any Tannaka category is $| G |$ for a unique affine group-scheme G, and homomorphisms of Tannaka categories are induced by a homomorphism of affine group-schemes.

Proof: By Proposition 1, if $A = A(\mathcal{C})$, the pair $(\mathcal{C}, T)$ may be identified to $(| A |, T_k)$.

By Proposition 2, the axiom $\mathcal{C}$ 4 shows that $\hat{\otimes}$ is induced by a unique homomorphism $\triangle : A \to A \hat{\otimes} A$.

$\mathcal{C}$ 5 and $\mathcal{C}$ 6 show that

$(l_A \otimes \triangle) \circ \triangle = (\triangle \otimes l_A) \circ \triangle$ and $\triangle = \theta \circ \triangle$ where $\theta : A \hat{\otimes} A \to A \hat{\otimes} A$ is defied by $\theta' (a \otimes b) = b \otimes a$.

$\mathcal{C}$ 7 shows that there is a homomorphism $\varphi : A \to k$ such that $A \xrightarrow{\triangle} A \hat{\otimes} A \xrightarrow{\varphi \otimes 1} k \otimes A = A$ is the identity.

Now let R be the vector space of continuous linear functionals on A, *i.e.* all linear functionals that vanish on some neighbourhood of zero.

$\triangle : A \to A \hat{\otimes} A$ gives a linear transformation $\triangle^* : R \otimes R \to R$. Then $\mathcal{C}$ 5 and $\mathcal{C}$ 6 show that $\triangle^*$ defines an associative commutative algebra-structure on R. And $\mathcal{C}$ 7 shows that this algebra R has an identity. Put $G =$ Spec R.

Now A is itself an algebra : thus $A \hat{\otimes} A \to A$ given by $a \otimes b \mapsto ab$ induces $\mu : R \to R \otimes R$. Because $\triangle : A \to A \hat{\otimes} A$ is an algebra homomorphism and not just a linear map, it follows that μ is a homomorphism of k-algebras. Thus μ induces $m : G \times G \to G$.

The associativity of the algebra structure on A shows that m makes G an affine semi-group-scheme (*i.e.*, the multiplication m is associative) and finally the identity of A gives an identity to G making G an affine monoid-scheme. We have to use $\mathcal{C}$ 8 to show that G is an affine group-scheme.

For a discrete monoid M there is a natural embedding $M \to k[M]$. This generalises in the above situation to a closed immersion $i : G \to \underline{A}$.

Any finite dimensional vector space V gives a scheme $\underline{V}$ by $\underline{V} = \text{Spec}\, S(V^*)$. For any k-scheme X, $\Gamma(X, \mathbf{O}_x) \otimes V = \text{Mor}\,(X, \underline{V})$.

We define $\underline{A} = \text{Spec}\, S(R)$. The reason being: for any k-scheme X, $\varinjlim_{I} \text{Mor}\,(X, (\underline{A/I})) = \text{Mor}\,(X, \underline{A})$ where the I run through open two-sided ideals of A.

The natural homomorphism $j : S(R) \to R$ given by $jx = x$ for all $x \in R$ induces a closed immersion $i : G \to \underline{A}$.

Next note that $\underline{A}$ is a monoid-scheme and in fact an inverse limit of the monoid-schemes $\underline{A/I}$. The operation $\underline{A} \times \underline{A} \to \underline{A}$ is given by $S(R) \to S(R) \otimes S(R)$ so that for $x \in R$ its image is $\mu \times \varepsilon R \otimes R \subseteq S(R) \otimes S(R)$. It is clear that $i : G \to \underline{A}$ is a homomorphism of monoid-scheme.

Similarly we form the schemes $(\underline{A/I})^*$ and $\underline{A}^*$; these are affine group-schemes for $f \in (A/I)$, $Nf =$ determinant of left-multiplication by f is a polynomial function on $(\underline{A/I})$, thus it is an element $d(I) \in S((A/I)^*)$. Put $(\underline{A/I})^* = \text{Spec}\;\; S\,(A/I)^*)_{d(I)}$ and $\underline{A}^*$ is the spectrum of the ring got from inverting all the $d\,(I)$ in $S\,(R)$.

Let us now assume $\mathcal{C}$ 8. Then for an open two-sided ideal I, if $r = rk\,(A/I)$, consider $\Lambda^r(A/I)$. By $\mathcal{C}$ 8 it will follow that the composite $G \xrightarrow{i} \underline{A} \to \underline{A/I}$ has its image in $(\underline{A/I})^*$. This gives a factoring

$$\begin{tikzcd}
G \arrow[rr, "i"] \arrow[dr, "j"'] & & \underline{A} \\
& \underline{A}^* \arrow[ur] &
\end{tikzcd}$$

and clearly j is a closed immersion. That G is an affine group-scheme follows from

Lemma: If $G \to P$ is a closed monoid-schcme of an affine group-scheme, then G is an affine group-scheme.

Proof: Let $P = \text{Spec}\, B$ and let I be the ideal defined by G. The morphism $Z : P \times P \to P \times P$ given by $(p_1, p_2) \mapsto (p_1, p_1 p_2)$ is an isomorphism. It suffices to show that Z induces an isomorphism from $G \times G$ to itself.

Let $Z^* : B \otimes B \to B \otimes B$ be the induced homomorphism on co-ordinate rings. Let $J = I \otimes B + B \otimes I$. Then $Z^*(J) \subseteq J$. We have to show that $Z^*(J) = J$.

It is well-known that B is the union of its finitely generated Hopf sub-algebras $\{C\}$. For any such C, Spec C is a group-scheme and Z^* restricts to an isomorphism of C. Thus if $(Z^*)^{-1}(J \cap (C \otimes C)) \neq J \cap (C \otimes C)$, then $(Z^*)^{-n}(J \cap (C \otimes C)) = J_n$ gives a strictly increasing sequence of ideals, which is not possible because C is Noetherian. Therefore, $Z^*(J \cap (C \otimes C)) = J \cap (C \otimes C)$ for all C implying that $Z^*(J) = J$. This proves the lemma.

The second assertion about homomorphisms of Tannaka categories follows again from Proposition 2.

From now on $R(G)$ will denote the co-ordinate ring of an affine group-scheme G and $A(G)$ will denote its dual.

A homomorphism $G \to H$ is said to be surjective if $R(H) \to R(G)$ is injective ; equivalently if $A(G) \to A(H)$ is surjective.

Proposition 5 : A homomorphism $G \to H$ is surjective if and only if the corresponding functor $F : |H| \to |G|$ is fully faithful and for any exact sequence $0 \to W' \to FV \to W'' \to 0$ in $|G|$ there is an exact sequence $0 \to V' \to V \to V''$ $\to 0$ in $|H|$ and a commutative diagram :

$$\begin{tikzcd}
0 \arrow[r] & W' \arrow[r] \arrow[d, "="'] & FV \arrow[r] \arrow[d, "1"] & W'' \arrow[r] \arrow[d, "="] & 0 \\
0 \arrow[r] & FV' \arrow[r] & FV \arrow[r] & FW'' \arrow[r] & 0
\end{tikzcd}$$

This is an immediate consequence of Proposition 3.

Proposition 6 : An affine group-scheme is finite if and only if there is a finite set S of G-representations such that any representation of G is a sub-quotient of a finite direct sum of representations from S.

Proof : If G is finite, then any representation is contained in a direct sum of copies of $R(G)$ which is itself a finite-dimensional representation of G.

Conversely, given such a set, put $(\mathcal{C}, T) = (|G|, T_k)$. To prove that $R(G)$ is finite dimensional, it suffices to prove that $A(G) = A(\mathcal{C})$ is finite-dimensional. We shall show in fact that $A(\mathcal{C}) \to A(S)$ is an injection. Let $a \in A(\mathcal{C})$. Suppose that $\pi_V(a) = 0$ for all $V \in S$. If V and W belong to S, and p and q are the projection from $V \oplus W$ to V and W respectively, then $Tp \circ \pi_{V \oplus W}(a) = \pi_V(a) \circ Tp = 0$ and $Tq \circ \pi_{V \oplus W}(a) = \pi_W(a) \circ Tq = 0$. This shows that $\pi_{V \oplus W}(a) = 0$. Similarly $\pi_Q(a) = 0$, for all Q whenever Q is a finite direct sum of objects from S. If $i : P \to Q$ is an injection and $\pi_Q(a) = 0$, then $Ti \circ \pi_p(a) = \pi_Q(a) \circ Ti = 0$ showing that $\pi_p(a) = 0$. Similarly if $j : P \to Q$ is a surjection and $\pi_p(a) = 0$, then $\pi_Q(a) = 0$. Thus we have shown that $\pi_P(a) = 0$ for all sub-quotients of all finite direct sums of members of S, *i.e.*, $\pi_P(a) = 0 \ \forall\ P \in \operatorname{obj} \mathcal{C}$, and therefore $a = 0$. Q.E.D.

The last two propositions are just what are required to show that (see Chapter I, § 3) :

1. $\pi(X, x_0) \to \pi(S, x_0)$ is a surjection, for all finite sets S of essentially finite vector bundles.

2. $\pi(X, x_0) \to \varprojlim\limits_{S} \pi(S, x_0)$ is an isomorphism with the S as above,

3. $\pi(S, x_0)$ is a finite group-scheme with the S as above.

References

Atiyah M F 1957 Vector bundles on an elliptic curve, *Proc. London Math. Soc.*, **Third Series, 7** 412–452

Grothendieck A 1965 *Elements de Geometrie Algebrique.*, I.H.E.S. Publications **24**

Kunze Ernst 1969 Characterizations of Regular local rings of characteristic *p*, *Am. J. Math.* **91** 772–784

Saavedra Rivano 1972 Categories Tannakiennes, Lecture Notes, Springer Verlag **265**

Safarevic I R 1956 On *p*-extensions, *Am. Math. Soc. Translations, Series* **2**, Vol. **4** 59–72

Seshadri C S 1967 Space of unitary vector bundles on a compact Riemann surface; *Ann. Math.* **85** 303–306

Seshadri C S 1977 Moduli of vector bundles on curves with parabolic structures, *Bull. Am. Math. Soc.* Vol. **83**, No. 1

Weil A 1938 Generalisation des fonctions abeliennes; *J. Mathematiques Pures et Appliques* **17** 47–87