COMPOSITIO MATHEMATICA

MADHAV V. NORI

On the representations of the fundamental group

Compositio Mathematica, tome 33, nº 1 (1976), p. 29-41

<http://www.numdam.org/item?id=CM_1976__33_1_29_0>

COMPOSITIO MATHEMATICA, Vol. 33, Fasc. 1, 1976, pag. 29–41
Noordhoff International Publishing
Printed in the Netherlands

ON THE REPRESENTATIONS OF THE FUNDAMENTAL GROUP

Madhav V. Nori

Let $\tilde{X}$ be a finite unramified Galois covering of a compact Riemann surface X with Galois group G, and let V be a finite-dimensional complex vector space on which G acts. The group G then acts on $\tilde{X} \times \tilde{V}$ in a natural way. The quotient of $\tilde{X} \times \tilde{V}$ by the action of G, which we call V, is a holomorphic vector bundle on X.

We call a holomorphic vector bundle W on X a finite vector bundle if there are polynomials f and g whose coefficients are non-negative integers, with $f \neq g$, such that $f(W)$ and $g(W)$ are isomorphic (for the definition of $f(W)$, see §3). It was shown by Weil in [4] that the vector bundle V constructed above is a finite vector bundle.

We shall prove the converse: for any finite vector bundle V on X, there exist $\tilde{X}$, $\tilde{V}$, G as above, such that V is the quotient of $\tilde{X} \times \tilde{V}$ by G.

This theorem holds, in fact, when X is a complete, connected, reduced scheme defined over a field k of characteristic zero, and goes through with only slight modifications in positive characteristic, enabling us to define a "fundamental group scheme" in this case.

Note that a special case of this theorem is classical: if π denotes the algebraic fundamental group of X, then the group of characters (one-dimensional representations) of π is identical to the group of line bundles L on X such that $L^{\otimes m}$ is trivial, for some positive integer m. This is a simple consequence of the standard Kummer theory for abelian extensions.

We explain the formalism of Tannaka Categories in §1, and §2 contains generalities on principal bundles, which we require for the proof of our theorem.

I am grateful to Professor Seshadri for the keen interest he has taken in this paper, and for the many discussions I have had with him.

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

$\mathscr{C}1$: $\mathscr{C}$ is an abelian k-category (existence of direct sums of finitely many objects of $\mathscr{C}$ included)

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

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

$\mathscr{C}4$: $\hat{\otimes}$: $\mathscr{C} \times \mathscr{C} \to \mathscr{C}$ is a functor which is k-linear in each variable, and

$$T \circ \hat{\otimes} = \otimes \circ (T \times T).$$

$\mathscr{C}5$: $\hat{\otimes}$ is associative, preserving T, in the following sense: Let H: $\hat{\otimes} \circ (1_{\mathscr{C}} \times \hat{\otimes}) \to \hat{\otimes} \circ (\hat{\otimes} \times 1_{\mathscr{C}})$ be the equivalence of functors that gives the associativity of $\hat{\otimes}$. For objects V_1, V_2, V_3 of $\mathscr{C}$, $T(H(V_1, V_2, V_3))$ 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.

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

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

$\mathscr{C}8$: For every object L of $\mathscr{C}$ 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 $(\mathscr{C}, \hat{\otimes}, T, L_0)$ shall be called a Tannaka category.

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

$$\bar{S} = \{W \in \operatorname{Obj}\mathscr{C} : \exists P_i \in S, 1 \le i \le t, \text{ and } V_1, V_2 \in \operatorname{Obj}\mathscr{C}$$

$$\text{such that } V_1 \subset V_2 \subset \bigoplus_{i=1}^{t} P_i, \text{ and } W \text{ is isomorphic to } V_2/V_1\}.$$

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

Theorem 1 of [2]):

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. Principal bundles

Let X be a nonempty k-prescheme, $\mathcal{S}(X)$ the category of quasi-coherent sheaves on X, $\otimes : \mathcal{S}(X) \times \mathcal{S}(X) \to \mathcal{S}(X)$ 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) $\Phi : P \times G \to P$ defines an action of G on P such that $j \circ \Phi = j \circ p_1$,

(c) Ψ: $P \times G \to P \times_X P$ by $\Psi = (p_1, \Phi)$ is an isomorphism.

In this case, $\mathfrak{F} \to j^*(\mathfrak{F})$ gives an isomorphism of $\mathcal{S}(X)$ with the category of G-sheaves on P, by the method of flat descent (see [1]). 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 $F(P) : G\text{-mod} \to \mathcal{S}(X)$, and putting $F = F(P)$, we note that the following are true:

$F1$: F is a k-additive exact functor,

$F2$: $F \circ \hat{\otimes} = \otimes \circ (F \times F)$,

$F3$: The obvious statements parallel to $\mathscr{C}5$, $\mathscr{C}6$, $\mathscr{C}7$; in particular, $FL_0 = \theta_X$, where L_0 is the trivial representation, and finally,

$F4$: 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 $F4$ hold.

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

LEMMA (2.1): *There is a unique functor $\bar{F}: G\text{-}mod' \to \mathcal{S}(X)$, such that:*

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

PROOF: Simply define $\bar{F}V$ to be the direct limit of FW, where W runs through the collection of finite-dimensional G-invariant subspaces of V, and the lemma is then easily checked. We will put $\bar{F} = F$ 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 $m: A \otimes_k A \to A$ 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 $\mathcal{O}_X$-algebras with identity. This is enough to conclude that there is an affine morphism $j: Z \to X$ such that $j_*(\mathcal{O}_Z)$ is isomorphic to FA as a sheaf of $\mathcal{O}_X$-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 $j_*(\mathcal{O}_p)$ 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 will 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

$$\Phi = F\varphi : P \times G \to P, \text{ and}$$
$$\Psi = F\psi : P \times G \to P \times_X P.$$

Since φ defines an action of G' on G, Φ defines an action of G on P, and $j \circ p_1 = j \circ \Phi$ 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 to 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 shall denote by V_Z the sheaf $V \otimes_k \mathcal{O}_Z$ 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 $f \in \Gamma(U, \mathcal{O}_Z)$, 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 their 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 shall require the aid of

LEMMA (2.7): *Let Y be an affine scheme on which G operates on the left, and H operates on the right. Assume that 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 $\bar{F}$ 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 and 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 $f \in \Gamma(U, \mathcal{O}_G)$,
(b) $g(v \otimes f) = gv \otimes f \circ L_g^{-1}$, for $v \in V'$, $g \in G$, and $f \in \Gamma(U, \mathcal{O}_G)$.

With $\bar{F}$ as in Lemma 2.7, it is trivial to check that $\bar{F}(V_G) = V_P$ and $\bar{F}(V'_G) = j^*(FV)$. To prove Lemma 2.6, it therefore suffices to prove

LEMMA (2.8): *There is a functorial isomorphism of V_G 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 by the scheme Spec $(S(W^*))$ again by W. Then the sheaf $W \otimes_k \mathcal{O}_G$ 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 λ 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 $F = G\text{-mod} \to \mathcal{S}(X)$ satisfies $F1$ to $F4$. Then $F1$ to $F4$ hold for $f^* \circ F$ also, and $P(f^* \circ F) = f^*(P(F))$.*
(*b*) *Let $X = \mathrm{Spec}\ k$, and $F : G\text{-mod} \to k\text{-mod}$ the forgetful functor. Then $P(F) = G$.*
(*c*) *Let $\varphi : H \to G$ 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 $R_\varphi : G\text{-mod} \to H\text{-mod}$ be the restriction functor. Then $F(P) \circ R_\varphi = F(P')$.*

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.

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) $[V]+[V']=[V\oplus V']$, and

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

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); note that 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 $H^0(X, \text{end } V)$ 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 $\mathbb{Z}$ in $K(X)$.*

(*b*) *$[V]\otimes 1$ is integral over $\mathbb{Q}$ in $K(X)\otimes_{\mathbb{Z}}\mathbb{Q}$.*

(*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 $h\in\mathbb{Z}[t]$ such that $h([V])=0$, and $h\neq 0$. Choose $f,g\in\mathbb{Z}[t]$ 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):

(1) *V_1, V_2 finite $\Rightarrow V_1 \oplus V_2$, $V_1 \otimes V_2$, V_1^* finite.*

(2) *$V_1 \oplus V_2$ finite $\Rightarrow V_1$ finite.*

(3) *A line bundle L is finite $\Leftrightarrow L^{\otimes m}$ is isomorphic to $\mathcal{O}_X$ 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 $S(L) = \{L^{\otimes m} : m \geq 0\}$.

LEMMA (3.3): *Let X be a smooth projective curve. For a vector bundle V, let $C(V) = \sup\{\mu(W) = \deg W/\mathrm{rk}\, W,\ 0 \neq W \subset V\}$.*
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, $C(V) \leq \max(C(V'), C(V''))$.

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

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

such that the horizontal rows are exact, and j', j'' are generic injections. Let U', U'' be the subbundles of V', V'' respectively, such that $j'(W') \subset U'$ and $j''(W'') \subset U''$, and $\mathrm{rk}\, W' = \mathrm{rk}\, U'$ and $\mathrm{rk}\, W'' = \mathrm{rk}\, U''$. Then $\deg W' \leq \deg U'$, and $\deg W'' \leq \deg U''$.

Now,

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

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, $C(V^{\otimes^n}) \leq \sup\{C(W): W \in S(V)\} = T(V)$, which is finite, since $S(V)$ is a finite collection. Consequently, for any subbundle W of V, $W \neq 0$, since $W^{\otimes^n}$ is a subbundle of $V^{\otimes^n}$, $\mu(W^{\otimes^n}) \leq T(V)$, for all non-negative integers n. But a simple calculation shows that $\mu(W^{\otimes^n}) = n\mu(W)$, which obviously implies that $\mu(W) \leq 0$.

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

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

(b) for all subbundles W of V, $W \neq 0$, $\mu(W) \leq 0$.

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, connected, 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 bundle 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 subbundle 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 $\mathcal{G}(X)$ with objects as semistable vector bundles on X is an abelian category.

PROOF:

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

(b) Let V and W be semistable vector bundles on X, and let $f: V \to W$ be a morphism. For a geometric point $x: \operatorname{spec} \bar{k} \to X$, let $r(x)$ be the rank of the morphism $x^*(f): x^*(V) \to x^*(W)$. Then, by elementary degree considerations, $r(x)$ is 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 $\operatorname{coker} f$ are locally free, and moreover, $(\ker f)|Y = \ker(f|Y)$ and $(\operatorname{coker} f)|Y = \operatorname{coker}(f|Y)$, 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 $\mathcal{G}(X)$

with objects as semistable vector bundles. 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 called essentially finite vector 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 $W|Y$ 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 subbundle of W_i, and P_i is semistable, and

(iii) V_i is 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 subbundle 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 $j: X' \to X$ a principal G-bundle. Then, for the functor $F(X'): G\text{-mod} \to \mathcal{S}(X)$, $F(X')V$ is always an essentially finite vector bundle.*

PROOF: We shall show that $F(X')V$ is of degree zero restricted to each curve. To do this, we may 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 not reduced, by looking at Hilbert polynomials.

Now, any representation V of G can be embedded (injectively) in $R \oplus R \oplus \cdots \oplus R$, 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 suffice to show that $F(X')R$ is finite, by (a) of Prop. 3.7. But $R \hat{\otimes} R$ is isomorphic to $R \oplus R \oplus \cdots \oplus R$ 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 $x^*: \mathcal{S}(X) \to k\text{-mod}$ 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 $(EF(X), \otimes, x^*, \mathcal{O}_X)$ is a Tannaka category. By Theorem 1.1, this determines an affine group scheme G such that G-mod 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 $\operatorname{Obj} EF(X)$, let $S^* = \{V^* : V \in S\}$. Let $S_1 = S \cup S^*$, and $S_2 = \{V_1 \otimes V_2 \cdots \otimes V_m : V_i \in S_1\}$. Let $EF(X, S) = \bar{S}_2$. Exactly as before, this determines an affine group scheme which we call $\pi(X, S, x)$, such that

$$G_S : EF(X, S) \to \pi(X, S, x)\text{-mod}$$

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

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 $\tilde{X}_S$ is induced from $\tilde{X}_Q$ 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 collection of essentially finite vector bundles. Then, there is a principal G-bundle X' on X, with G a finite group scheme, such that the image of $F(X'): G\text{-mod} \to \mathcal{S}(X)$ contains the given collection S.*

PROOF: For each $W \in S$, choose V such that W is a quotient of a semistable subbundle of V, and V a finite vector bundle. Let Q be the collection of the V as constructed, and note that S is a subset of $\mathrm{Obj}\, EF(X, Q)$.

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 $\pi(X, Q, x)$-mod, and then, we know that $F(X') \cdot G_Q(V) = V$, for all objects V of $EF(X, Q)$, thus proving the Proposition.

For $S = \mathrm{Obj}\, EF(X)$, we shall denote $\tilde{X}_S$, G_S, F_S, $\tilde{x}_S$ by $\tilde{X}$, G, 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 finite 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 $\tilde{x}$ in 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 G-mod to $EF(X)$. Now $EF(X)$ is identified with $\pi(X, x)$-mod in such a way that the forgetful functor T_k on $\pi(X, x)$-mod is equivalent to the functor x^* from $EF(X)$ to k-mod. Thus, the composite $T_k \cdot F(X')$ is simply $x^* \cdot F(X') = F(X'|x)$, by Prop. 2.9(a). Now, the k-rational point u of $X'|x$ gives a unique isomorphism $\varphi : G \to X'|x$ of principal homogeneous spaces such that $\varphi(1) = u$. By Prop. 2.9(b), φ determines a natural equivalence of the functor $F(X'|x)$ with the forgetful functor from G-mod $\to k$-mod. This information yields a morphism (of Tannaka categories) from G-mod to $\pi(X, x)$-mod, which, by Theorem 1.3, is induced by a homomorphism $\rho : \pi(X, x) \to G$. We now appeal to Prop.