VECTOR BUNDLES OVER AN ELLIPTIC CURVE

By M. F. ATIYAH

[Received 30 January 1957.—Read 14 February 1957]

Introduction

THE primary purpose of this paper is the study of algebraic vector bundles over an elliptic curve (defined over an algebraically closed field k). The interest of the elliptic curve lies in the fact that it provides the first non-trivial case, Grothendieck (**6**) having shown that for a rational curve every vector bundle is a direct sum of line-bundles.

In order to provide the necessary background a certain amount of general material, not found in the literature, has been included. This consists of a brief discussion of 'Theorems A and B' and their relation with Universal bundles, a little on projective bundles, and some results on reduction of structure group. The case of vector bundles over an algebraic curve is treated in greater detail, and more precise results are obtained. In particular a refinement of Theorems A and B is given (Theorem 1) which seems to be a necessary preliminary in any attempt at classification of vector bundles. This concludes Part I of the paper.

Part II is devoted to the classification of vector bundles over an elliptic curve. The problem is completely solved and the main result is stated in Theorem 7. The characteristic of the field does not enter into this part of the problem, and the results are valid in both characteristic 0 and p.

In Part III we examine the operation of the tensor product. This is most easily expressed in terms of the ring $\hat{\mathscr{E}}$ generated by the vector bundles (cf. Part I, § 1). We show (Theorem 12) that $\hat{\mathscr{E}}$ is the tensor product of certain sub-rings $\hat{\mathscr{E}}_0$ and $\hat{\mathscr{E}}_p$ (over all primes p), and the ring structure of $\hat{\mathscr{E}}_0$ and $\hat{\mathscr{E}}_p$ is given by Theorems 8, 13, and 14. These results are all for the characteristic zero case, and we make only a few isolated remarks for the case of characteristic p.

We conclude the paper with a few brief applications of the results of Parts II and III.

PART I

1. Generalities

Let X be an algebraic variety defined over an algebraically closed field k. We shall suppose that X is irreducible and projective (i.e. that it can be embedded biregularly in some projective space). We shall be concerned with vector bundles over X, i.e. algebraic fibre bundles over X with a vector space as fibre and the general linear group as structure group. If k is the complex field then it has been shown by Serre (**9**) that the algebraic and analytic vector bundles over X coincide. Thus we prefer to adopt the more general approach rather than limit ourselves to the complex analytic case; the proofs are no more difficult, except that the characteristic of k does enter the picture later on.

If E is any vector bundle over X we shall denote by $\mathbf{E}$ the sheaf of germs of regular sections of E, and by $\Gamma(E)$ the vector space of global regular sections of E; thus $\Gamma(E) = H^0(X, \mathbf{E})$.

We denote by $\mathscr{E}(X)$ the set of equivalence classes of all vector bundles over X. We have two operations in $\mathscr{E}(X)$: the direct sum $\oplus$, and the tensor product $\otimes$. Since the Krull–Schmidt theorem holds in $\mathscr{E}(X)$ (cf. (**3**)) it follows that $\mathscr{E}(X)$ is a free abelian semi-group with respect to $\oplus$. Hence we may embed it in a free abelian group $\hat{\mathscr{E}}(X)$. If we extend the $\otimes$ operation to $\hat{\mathscr{E}}(X)$ we obtain a commutative ring with unit (the trivial line-bundle). If E is a vector bundle we denote by e the corresponding element of $\mathscr{E}(X)$ (or $\hat{\mathscr{E}}(X)$), and we write $e+e'$, ne, ee' instead of $e \oplus e'$, $e \oplus e \oplus \ldots \oplus e$ (n terms), $e \otimes e'$ respectively. For any vector bundle E we have a dual bundle E^*, and so we obtain an automorphism $e \to e^*$ of the ring $\hat{\mathscr{E}}(X)$. We note the canonical isomorphism: $\operatorname{Hom}(E, F) \cong E^* \otimes F$. If $\mathscr{E}' \subset \mathscr{E}(X)$ is any subset we shall write $E \in \mathscr{E}'$ instead of $E \in e$, $e \in \mathscr{E}'$.

If L is a line-bundle over X (i.e. a vector bundle in which the fibre is of dimension one), then $L \otimes L^* \cong 1$, where 1 denotes the trivial line-bundle. Thus the equivalence classes of line-bundles form a group $\Delta(X)$. If X is non-singular then $\Delta(X)$ is canonically isomorphic with the divisor class group of X. We denote by $\Lambda(X)$ the subring of $\hat{\mathscr{E}}(X)$ generated by $\Delta(X)$. In particular we shall regard $\hat{\mathscr{E}}(X)$ as a $\Lambda(X)$-module. In view of the relation between line-bundles and divisor classes we define the relation $L_1 \geqslant L_2$ to mean: there exists a regular homomorphism of L_2 into L_1, not identically zero, i.e. $\Gamma \operatorname{Hom}(L_2, L_1) \neq 0$. Clearly $L_1 \geqslant L_2$ if and only if $L_1 \otimes L_2^* \geqslant 1$. If X is a non-singular curve the line bundle L corresponds to a divisor class D, and we put $\deg(L) = \deg D$. Then $L_1 \geqslant L_2$ implies $\deg L_1 \geqslant \deg L_2$.

If E is an r-dimensional vector bundle over X, and if k is now the complex field, we have *Chern classes* $C_i(E) \in H^{2i}(X, C)$, $i = 0, \ldots, r$. Following Hirzebruch it is convenient to introduce a map t: $\hat{\mathscr{E}}(X) \to H^*(X, C)$ defined by $t(E) = e^{\delta_1}+e^{\delta_2}+\ldots+e^{\delta_r}$, where the δ_i are the formal symbols given by

$$(1+\delta_1 x)(1+\delta_2 x)\ldots(1+\delta_r x) = 1+C_1 x+C_2 x^2+\ldots+C_r x^r.$$

The advantage of t lies in the fact that it is a *ring homomorphism*. If X is a non-singular curve then $H^*(X, C)$ is generated by $1 \in H^0(X, C)$ and an element $\mu \in H^2(X, C)$ (the fundamental class) with $\mu^2 = 0$. Then

$$t(E) = r.1 + d.\mu,$$

where r is the dimension of the fibre and $d.\mu = C_1(E)$. We can also define d as follows: the homomorphism det: $GL_r(C) \to GL_1(C) = C^*$ gives rise to an induced line-bundle $\det(E)$; we put $d = \deg(\det(E))$. Thus d is an integer, and this definition works for any field k; we write $d = \deg(E)$. If we denote by $\mathscr{D}$ the ring of dual numbers (i.e. the ring generated by two elements $1, \mu$ with $\mu^2 = 0$) we see that $t\colon \hat{\mathscr{E}}(X) \to \mathscr{D}$ is a ring homomorphism, valid for any ground field k.

2. Theorems A and B†

We recall here the form of 'Theorems A and B' for vector bundles over a projective algebraic variety (cf. (9)). Let H be the line-bundle corresponding to a hyperplane section, then we put $E(n) = E \otimes H^n$, where H^n denotes the tensor product $H \otimes H \otimes \ldots \otimes H$ (n times). Then we have:

THEOREM A. *For sufficiently large n (depending on E) the canonical homomorphism $\Gamma(E(n)) \to E(n)_x$ is an epimorphism for all $x \in X$.*

THEOREM B. *For sufficiently large n (depending on E)*

$$H^q(X, \mathbf{E}(\mathbf{n})) = 0 \quad (q > 0).$$

If E is such that $\Gamma(E) \to E_x$ is an epimorphism for all x we shall say that *E has sufficient sections*. This condition is obviously equivalent to requiring that E should be *a quotient bundle of a trivial bundle*. Thus Theorem A asserts that, for sufficiently large n, $E(n)$ is a quotient bundle of a trivial bundle. Dually we also have that $E(-n)$ is a *sub-bundle* of a trivial bundle, for sufficiently large n.

Let V be a vector space of dimension $r+r'$, and let $G^r_{r'}(V)$ denote the Grassmannian of subspaces of V of dimension r', or equivalently the Grassmannian of quotient spaces of V of dimension r. If we denote the trivial bundle $V \times G^r_{r'}(V)$ also by V, we get an exact sequence of vector bundles over $G^r_{r'}(V)$:

$$0 \to W' \to V \to W \to 0. \tag{1}$$

W is r-dimensional and W' r'-dimensional. Suppose now that E is an r-dimensional vector bundle over X with sufficient sections. Putting

$$V = \Gamma(E),$$

we obtain an exact sequence of vector bundles over X

$$0 \to E' \to V \to E \to 0. \tag{2}$$

† The ideas of this section are due to J.-P. Serre.

It is almost immediate that the map $f: X \to G^r_{r'}(V)$ defined by assigning to each x the subspace E'_x of V (or equivalently the quotient space E_x of V) is such that $f^{-1}(1) \cong (2)$, where $f^{-1}(1)$ denotes the sequence on X induced from (1) by f. Thus $E \cong f^{-1}(W)$, $E' \cong f^{-1}(W')$.

In the usual terminology W' is the 'universal bundle' over the classifying space $G^r_{r'}(V)$. However, it would seem preferable to distinguish between W and W' by calling W the *universal quotient-bundle* and W' the *universal sub-bundle*. Theorem A, joined with the preceding remarks, then gives the following:

(i) for sufficiently large n, $E(n)$ is induced by a regular map $f: X \to G^r(V)$ from the universal quotient bundle;

(i)* for sufficiently large n, $E(-n)$ is induced by a regular map

$$g: X \to G_r(V)$$

from the universal sub-bundle.

In (i) we take $V = \Gamma(E(n))$ and in (i)* we take $V = [\Gamma(E^*(n))]^*$.

If E has sufficient sections there may be many different maps

$$f: X \to G^r(V)$$

(for different spaces V) such that $E \cong f^{-1}(W)$. However, they can all be obtained from the canonical one defined above (in which $V = \Gamma(E)$). In fact let $g: X \to G^r(U)$ be such a map, then we have an epimorphism $U \to E$. This induces a map $U \cong \Gamma(U) \to \Gamma(E) = V$, and so $U \to E$ may be factored into $U \to V \to E$. The map $g: X \to G^r(U)$ is then clearly describable in terms of $f: X \to G^r(V)$ and the homomorphism $U \to V$.

Whether or not E has sufficient sections we always have a homomorphism $\Gamma(E) \to E$. If $\Gamma(E) \to E_x$ is a *monomorphism* for all $x \in X$ it follows that $\Gamma(E)$ (regarded as a trivial bundle) can be identified with a sub-bundle of E. This remark will come in useful in Parts II and III.

For future reference we shall require an elementary lemma. We define a vector bundle E to be *ample*† if it has sufficient sections and if $H^q(X, \mathbf{E}) = 0$ for $q > 0$. Then we have

LEMMA 1. *Let* $0 \to E' \to E \to E'' \to 0$ *be an exact sequence of vector bundles on* X. *Then*

(i) *if* E' *and* E'' *are ample so is* E,

(ii) *if* E *has sufficient sections so does* E''.

Proof. (i) Since $H^q(X, \mathbf{E}') = H^q(X, \mathbf{E}'') = 0$ for $q > 0$, the exact co-

† One could adopt a stronger definition of this term by insisting that the canonical map of X into the Grassmannian is biregular.

homology sequence gives $H^q(X, \mathbf{E}) = 0$ for $q > 0$ and we have an exact sequence

$$0 \to \Gamma(E') \to \Gamma(E) \to \Gamma(E'') \to 0.$$

We consider the diagram

$$\begin{array}{ccccccccc} 0 \to & \Gamma(E') & \to & \Gamma(E) & \to & \Gamma(E'') & \to 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ 0 \to & E'_x & \to & E_x & \to & E''_x & \to 0. \end{array}$$

Since $\Gamma(E') \to E'_x$, $\Gamma(E'') \to E''_x$ are epimorphisms for all $x \in X$ it follows that $\Gamma(E) \to E_x$ is an epimorphism for all x. Hence E is ample.

(ii) We have a diagram

$$\begin{array}{cccc} \Gamma(E) & \to & \Gamma(E'') & \\ \downarrow & & \downarrow & \\ E_x & \to & E''_x & \to 0. \end{array}$$

By hypothesis $\Gamma(E) \to E_x$ is an epimorphism. It follows at once that $\Gamma(E'') \to E''_x$ is also an epimorphism, i.e. E'' has sufficient sections.

3. The projective group

In this section k will be the field of complex numbers C, and we denote by C^* the multiplicative group of C. Let $P_r = GL_r(C)/C^*$ be the projective group corresponding to $GL_r(C)$. By general results of Serre (**9**) two algebraic bundles with group P_r which are analytically equivalent are also algebraically equivalent. It is not known in general whether every analytic bundle with group P_r is necessarily algebraic.† If X is a curve, however, we shall see that this is in fact the case.

We consider the exact sequence of non-abelian groups:

$$1 \to C^* \to GL_r(C) \to P_r \to 1,$$

and the corresponding exact sequence of germs of analytic maps on X:

$$1 \to \mathbf{C}^* \to \mathbf{GL}_r(\mathbf{C}) \to \mathbf{P}_r \to 1.$$

Since C^* is the centre of $GL_r(C)$, and since X is a Hausdorff space‡ we have an exact sequence of cohomology (cf. (**4**) or (**5**)):

$$H^1(X, \mathbf{GL}_r(\mathbf{C})) \to H^1(X, \mathbf{P}_r) \to H^2(X, \mathbf{C}^*).$$

The exactness is to be understood in the following sense: an element of $H^1(X, \mathbf{P}_r)$ lies in the image of $H^1(X, \mathbf{GL}_r(\mathbf{C}))$ if and only if its image in $H^2(X, \mathbf{C}^*)$ is zero. Thus if $H^2(X, \mathbf{C}^*) = 0$ every P_r-bundle is the image of a $GL_r(C)$-bundle and therefore algebraic. Now we have an exact sequence of sheaves:

$$0 \to Z \to \mathbf{C} \to \mathbf{C}^* \to 0,$$

† [*Added in proof.*] Recent results of Serre and Grothendieck show that there exist analytic P_r-bundles which are not algebraic.

‡ The Zariski topology is non-Hausdorff and so the corresponding algebraic sequence may not (*a priori*) be exact.

where Z is the sheaf of integers and $\mathbf{C} \to \mathbf{C}^*$ is given by $\exp(2\pi i)$. The exact cohomology sequence gives

$$H^2(X, \mathbf{C}) \to H^2(X, \mathbf{C}^*) \to H^3(X, Z).$$

Hence we certainly have $H^2(X, \mathbf{C}^*) = 0$ if $H^2(X, \mathbf{C}) = H^3(X, Z) = 0$. These conditions are satisfied notably in the following two cases:

(i) X is a curve,

(ii) X is a projective space.

Hence in these cases every analytic P_r-bundle is algebraic.

In any case the image of $H^1(X, \mathbf{GL}_r(\mathbf{C}))$ in $H^1(X, \mathbf{P}_r)$ is in (1–1) correspondence with the equivalence classes of $H^1(X, \mathbf{GL}_r(\mathbf{C}))$ under the operation of the group $H^1(X, \mathbf{C}^*)$. This is a consequence of the exact sequence [cf. (**5**)]. If we turn from principal bundles with group $GL_r(C)$ to the corresponding vector bundles, the operation mentioned above simply becomes the tensor product $E \otimes L$, where L is a line-bundle (defined by an element of $H^1(X, \mathbf{C}^*)$).

Thus if X is a curve a knowledge of the Λ-module structure of $\hat{\mathscr{E}}(X)$ determines completely the classification of bundles with the projective group as structure group.

We have proved this when k is the complex field (for either analytic or algebraic bundles). In fact it is not difficult to show that it holds for any field k.†

4. Reduction of structure group for curves

In this section we suppose that X is a non-singular curve. We then have the following purely local result: let f: $X \to Y$ be a rational map of X into a *complete* variety Y, then f is regular. Suppose now that E is a vector bundle over X, and let $\phi \in \Gamma(E)$ ($\phi \neq 0$). Then ϕ defines a rational section of the projective bundle associated to E. By the result just mentioned this section is necessarily regular, and so defines a sub-bundle of E of dimension one—its counterimage in E. We denote this sub-bundle by $[\phi]$ and call it the line-bundle generated by ϕ. If $x \in X$ and t is a local parameter at x, we can write $\phi = t^\nu \phi'$ where $\nu \geqslant 0$ and $\phi'(x) \neq 0$. Then $[\phi]_x$ is just the vector space of dimension one generated by $\phi'(x)$; in particular $\phi(X) \subset [\phi]$, and so ϕ is a section of $[\phi]$. We define the divisor of ϕ by

$$\operatorname{div} \phi = \sum_x \nu_x x,$$

and we put $\deg \phi = \deg \operatorname{div} \phi = \sum \nu_x$. Thus $\deg \phi = \deg [\phi]$.

If E has sufficient sections, then $E' = E/[\phi]$ also has sufficient sections

† I am indebted to J.-P. Serre for this remark.

(Lemma 1), and so by repeating this construction we end up with a series of sub-bundles of E:

$$0 = E_0 \subset E_1 \subset E_2 \subset \ldots \subset E_r = E,$$

where $L_i = E_i/E_{i-1}$ is a line-bundle ($E_1 = [\phi]$). Such a series will be called a *splitting* of E, and we write $E = (L_1, L_2, \ldots, L_r)$. By considering $E(n)$ instead of E we can always remove the restriction on E to have sufficient sections. In fact if $E(n) = (L_1, \ldots, L_r)$, then $E = (L_1(-n), \ldots, L_r(-n))$.

One consequence of the existence of splittings is the Riemann–Roch theorem. In fact let

$$\chi(E) = \dim H^0(X, \mathrm{E}) - \dim H^1(X, \mathrm{E}),$$

and let $E = (L_1, \ldots, L_r)$. Then from the exact cohomology sequences of the splitting we find immediately:

$$\chi(E) = \sum_{i=1}^{r} \chi(L_i).$$

On the other hand we have the Riemann–Roch theorem for a line-bundle (or divisor)

$$\chi(L_i) = \deg L_i - g + 1,$$

where g is the genus of X. Hence we obtain

$$\chi(E) = \deg E + r(1-g).$$

A splitting of E may also be viewed as a reduction of the structure group from GL_r to Δ_r (the triangular group with zeros below the diagonal). Such a reduction is always possible. In fact $F_r = GL_r/\Delta_r$ the 'flag manifold' is a projective variety and so complete. Let Y be the bundle associated to E with fibre F_r. This has a rational section (by definition of an algebraic fibre bundle) and so a regular section, but this is precisely equivalent to giving a reduction of the structure group to Δ_r (cf. (9)).

Of course the reduction to Δ_r is possible in many different ways. In fact even the factors L_i of a splitting are not unique. We try, therefore, to pick out certain maximal splittings. This is essentially a classical idea (cf. 'minimal directrix curves' in (**1**)) and has been utilized by Grothendieck (**6**). First we need a lemma:†

LEMMA 2. *The integers* $\deg(\phi)$, *for* $\phi \in \Gamma(E)$ $(\phi \neq 0)$, *are bounded above.*

Proof. Let $0 = E_0 \subset E_1 \subset E_2 \subset \ldots \subset E_r = E$ be a fixed splitting of E, and let $L_i = E_i/E_{i-1}$. Let $\phi \in \Gamma(E)$ $(\phi \neq 0)$, then there exists an integer $i \geqslant 1$ such that $[\phi] \subset E_i$, $[\phi] \not\subset E_{i-1}$. It follows that there is a non-zero homomorphism $[\phi] \to L_i$, and so $[\phi] \leqslant L_i$, $\deg(\phi) \leqslant \deg L_i$. Thus for all $\phi \in \Gamma(E)$, $\deg(\phi) \leqslant \sup(L_i)$.

† This proof is given in Grothendieck (**6**).

If $\phi \in \Gamma(E)$ has the maximum degree (finite by Lemma 2) we say that ϕ is a *maximal section* of E. $[\phi]$ is called a *maximal line-bundle* of E.

DEFINITION. $(L_1, L_2,..., L_r)$ *is a* maximal splitting *of* E *if*

(i) L_1 *is a maximal line-bundle of* E,

(ii) $(L_2,..., L_r)$ *is a maximal splitting of* E/L_1.

If E has sufficient sections then a maximal splitting always exists. We shall now obtain an inequality on the degrees of the factors in a maximal splitting. First we consider a two-dimensional bundle, and we denote the genus of X by g.

LEMMA 3. *Let* (L_1, L_2) *be a maximal splitting of* E, *then*

$$\deg L_2 - \deg L_1 \leqslant 2g.$$

Proof. We have an exact sequence

$$0 \to 1 \to E \otimes L_1^* \to L_2 \otimes L_1^* \to 0.$$

Hence the exact cohomology sequence:†

$$0 \to \Gamma(1) \to \Gamma(E \otimes L_1^*) \to \Gamma(L_2 \otimes L_1^*) \to H^1(X, \mathbf{1}) \to .$$

Suppose that $\deg(L_2 \otimes L_1^*) \geqslant 2g+1$, then by the Riemann–Roch theorem

$$\dim \Gamma(L_2 \otimes L_1^*) \geqslant 2g+1-g+1 = g+2.$$

But $\dim H^1(X, \mathbf{1}) = g$. Hence the exact sequence gives

$$\dim \Gamma(E \otimes L_1^*) \geqslant 1+2 = 3.$$

Let $x \in X$, then the kernel of

$$\Gamma(E \otimes L_1^*) \to (E \otimes L_1^*)_x$$

must have dimension at least one. Thus there exists a section $\phi \in \Gamma(E \otimes L_1^*)$ with $\operatorname{div}\phi \geqslant (x)$ and so $\deg \phi \geqslant 1$. Now $[\phi] \subset E \otimes L_1^*$, and therefore $[\phi] \otimes L_1 \subset E \otimes L_1 \otimes L_1^* \cong E$. But $\deg[\phi] \otimes L_1 \geqslant 1+\deg L_1$ contradicting the maximality of L_1. This proves the lemma.

LEMMA 4. *Let* $(L_1, L_2,..., L_r)$ *be a maximal splitting of* E. *Then*

$$\deg L_i - \deg L_{i-1} \leqslant 2g, \qquad i = 2,..., r.$$

Proof. We proceed by induction on r. For $r = 2$ it has just been proved (Lemma 3). Suppose it is true for all $s < r$, then since $(L_2,..., L_r)$ is a maximal splitting of E/L_1 it follows that $\deg L_i - \deg L_{i-1} \leqslant 2g$ for $i = 3,..., r$. It remains to prove the inequality for $i = 2$. But let E_2 be the sub-bundle of E of dimension two given by the splitting. Then, since L_1 is a maximal line-bundle of E, it is *a fortiori* maximal for E_2. Hence (L_1, L_2) is a maximal splitting, and by Lemma 3, $\deg L_2 - \deg L_1 \leqslant 2g$.

† $\mathbf{1}$ is simply the sheaf of local rings on X (usually denoted by $\mathbf{0}$ or $\mathcal{O}$).

Our next object is to obtain an inequality in the opposite direction, and for this purpose we must suppose that E is indecomposable.

LEMMA 5. *Let E be indecomposable, and let $0 \to E_1 \to E \to E_2 \to 0$ be an exact sequence. Then $\Gamma\,\mathrm{Hom}(E_1, E_2 \otimes K) \neq 0$, where K denotes the canonical line-bundle.*

Proof. The classes of extensions of E_2 by E_1 are described by the elements of $H^1(X, \mathrm{Hom}(\mathrm{E}_2, \mathrm{E}_1))$ (cf. (2)). By Serre duality this is dual to the vector space $\Gamma\,\mathrm{Hom}(E_1, E_2 \otimes K)$. Since E is indecomposable the extension must be non-trivial and so $\Gamma\,\mathrm{Hom}(E_1, E_2 \otimes K) \neq 0$.

LEMMA 6. *Let E be indecomposable and with sufficient sections. Then E has a maximal splitting $(L_1, L_2,..., L_r)$ with $\deg L_i \geqslant \deg L_1-(i-1)(2g-2)$, $i = 1, 2,..., r$.*

LEMMA 6′. *Let X be an elliptic curve, and let E be indecomposable and with $\Gamma(E) \neq 0$. Then E has a maximal splitting $(L_1, L_2,..., L_r)$ with $L_i \geqslant L_1 \geqslant 1$, $i = 1, 2,..., r$.*

Proof. We shall construct a maximal splitting with the required properties and we proceed inductively. Since $\Gamma(E) \neq 0$, E has a maximal line-bundle $E_1 \geqslant 1$. Suppose now that we have constructed a sequence

$$0 = E_0 \subset E_1 \subset E_2 \subset ... \subset E_i,$$

where $L_j = E_j/E_{j-1}$ is a maximal line-bundle of E/E_{j-1} for $j = 1,..., i$, and such that the L_i satisfy the requirements of Lemma 6 (or Lemma 6′ if X is elliptic). We put $E_i' = E/E_i$. Then, by Lemma 5, there exists a non-zero $f \in \Gamma\,\mathrm{Hom}(E_i, E_i' \otimes K)$. Since $f \neq 0$ there exists an integer j, $1 \leqslant j \leqslant i$ such that

$$f(E_k) = 0, \quad k < j,\ f(E_j) \neq 0.$$

Then f induces a non-zero homomorphism $\bar{f}\colon L_j \to E_i' \otimes K$. Let ϕ_j be a non-zero section of L_j (this exists by inductive hypothesis). Then $\bar{f}(\phi_j) \neq 0$, and $\mathrm{div}(\bar{f}\phi_j) \geqslant \mathrm{div}\,\phi_j$, so that $[\bar{f}\phi_j] \geqslant L_j$. Since

$$[\bar{f}\phi_j] \subset E_i' \otimes K, \qquad [\bar{f}\phi_j] \otimes K^* \subset E_i' \otimes K \otimes K^* \cong E_i'.$$

We now distinguish two cases, corresponding to Lemmas 6, 6′ respectively:

(i) X any curve, hypotheses of Lemma 6. Then E_i' has sufficient sections, since E has. Let L_{i+1} be a maximal line-bundle of E_i', then

$$\begin{aligned}\deg(L_{i+1}) &\geqslant \deg[\bar{f}\phi_j] \otimes K^* \geqslant \deg L_j - \deg K \\ &\geqslant \deg L_1-(j-1)(2g-2)-(2g-2), \quad \text{by inductive hypothesis,} \\ &\geqslant \deg L_1-i(2g-2), \quad \text{since } j \leqslant i.\end{aligned}$$

(ii) X elliptic, hypotheses of Lemma 6′. Then $K = 1$, and $\bar{f}\phi_j$ is a non-zero section of E_i'. If $\bar{f}\phi_j$ is a maximal section we take $L_{i+1} = [\bar{f}\phi_j]$. If not let L_{i+1} be a maximal line-bundle, then $\deg L_{i+1} \geqslant \deg[\bar{f}\phi_j]+1$. Since X

is elliptic this implies $L_{i+1} \geqslant [\bar{f}\phi_j]$, and we already have $[\bar{f}\phi_j] \geqslant L_j$. Hence $L_{i+1} \geqslant L_j \geqslant L_1$ by inductive hypothesis.

In both cases therefore we have found a maximal line-bundle L_{i+1} of E'_i satisfying the required conditions. We then take E_{i+1} to be the sub-bundle of E lying over L_{i+1} in the projection $E \to E'_i$. This establishes the induction and Lemmas 6 and 6′ are proved.

Remark. The inequality in Lemma 6 is actually valid for any maximal splitting. However, we wanted to prove the two lemmas together, and so chose this form of the result, which is sufficient for our purposes.

LEMMA 7. *Let E be indecomposable of dimension r and degree d. Then $E = (L_1, L_2,..., L_r)$ where*

$$\deg L_i \geqslant d/r-(r-1)(3g-2).$$

Proof. It is sufficient to prove the lemma for an ample vector bundle E, for if $E(n) = (L'_1, L'_2,..., L'_r)$ with $\deg L'_i \geqslant (d+hnr)/r-3(r-1)(g-1)$ then $E = (L_1, L_2,..., L_r)$ with $\deg L_i = \deg L'_i-hn \geqslant d/r-3(r-1)(g-1)$. Here $h = \deg H$, where H is the line-bundle of a hyperplane section. Suppose, therefore, that E is ample, then by Lemma 6, E has a maximal splitting $(L_1, L_2,..., L_r)$ with

$$\deg L_i \geqslant \deg L_1-(i-1)(2g-2) \quad (\text{for } i \geqslant 1). \tag{α}$$

Also by Lemma 4 we must have

$$\deg L_i - \deg L_{i-1} \leqslant 2g \quad (\text{for } i \geqslant 2). \tag{β}$$

Hence, combining (α) and (β) we obtain, for $i \geqslant 1$,

$$-2g(i-1) \leqslant \deg L_1 - \deg L_i \leqslant (i-1)(2g-2). \tag{γ}$$

Summing for $i = 1,..., r$ we get

$$-gr(r-1) \leqslant r\deg L_1-d \leqslant (g-1)r(r-1)$$

or

$$-g(r-1) \leqslant \deg L_1-d/r \leqslant (g-1)(r-1). \tag{δ}$$

We observe in passing that, if $g = 0$ (i.e. X a rational curve) these inequalities can only be satisfied if $r = 1$. This means that the only indecomposable bundles over a rational curve are line-bundles (Grothendieck (**6**)).

Finally, from (γ) and (δ),

$$\begin{aligned} \deg L_i &\geqslant \deg L_1-(i-1)(2g-2) \\ &\geqslant d/r-g(r-1)-(r-1)(2g-2) \\ &= d/r-(r-1)(3g-2). \end{aligned}$$

We can now prove a stronger form of Theorems A and B. But first we need:

LEMMA 8. *Let E be a line-bundle of degree d, with $d \geqslant 2g$. Then E is ample.*

Proof. First we have $\dim H^1(X, \mathbf{E}) = \dim H^0(X, E^* \otimes K) = 0$ since $\deg(E^* \otimes K) = -d+(2g-2) < 0$. Next let $x \in X$, and let L be the line-bundle corresponding to the divisor $-x$. Then we have an exact sequence of sheaves:

$$0 \to \mathbf{E} \otimes \mathbf{L} \to \mathbf{E} \to E_x \to 0,$$

where E_x is just the constant sheaf C over x. Since

$$\deg(E \otimes L) = d-1 \geqslant 2g-1$$

it follows as above that $H^1(X, \mathbf{E} \otimes \mathbf{L}) = 0$. Hence we get an exact sequence

$$0 \to \Gamma(E \otimes L) \to \Gamma(E) \to E_x \to 0.$$

Thus $\Gamma(E) \to E_x$ is an epimorphism for all x, and so E is ample.

We denote by $\mathscr{E}(r, d)$ the set of indecomposable bundles over X of dimension r and degree d.

THEOREM 1. *There exists an integer $N(g,r,d)$ such that $E(n)$ is ample for all $E \in \mathscr{E}(r,d)$ and all $n \geqslant N(g,r,d)$.*

Proof. We take $N(g,r,d) = -d/r+(r-1)(3g-2)+2g$ (more precisely the first integer greater than or equal to this). Then by Lemma 7

$$E(n) = (L_1(n),..., L_r(n)),$$

where

$$\deg L_i(n) \geqslant d/r+nh-(r-1)(3g-2) \geqslant 2g \quad \text{if } n \geqslant N(g,r,d).$$

Hence, by Lemma 8 each of the line-bundles $L_i(n)$ is ample. Hence by Lemma 1 (i) $E(n)$ is ample.

Suppose now that X is defined over the complex field, and let

$$\rho \colon \pi_1(X) \to GL_r(C)$$

be a representation of the fundamental group of X. This gives rise to a vector bundle over X (cf. (**2**)). We denote by Π the subset of $\mathscr{E}(X)$ arising from such representations, and by $\Pi(r)$ the subset of Π arising from r-dimensional representations. Then it has been shown by Weil (**10**) (cf. also (**2**)) that $E \in \Pi$ if and only if $E \cong E_1 \oplus ... \oplus E_q$ where each E_i is indecomposable and of degree zero. Hence from Theorem 1 we deduce:

COROLLARY. *There exists an integer $N(g,r)$ such that $E(n)$ is ample for all $E \in \Pi(r)$ and all $n \geqslant N(g,r)$.*

This corollary enables us to generate all bundles of $\Pi(r)$ by mapping X into a *fixed* Grassmannian, whereas Theorem A simply asserts the existence of a suitable Grassmannian for each individual bundle.

It is reasonable to ask whether anything analogous to Theorem 1 and its corollary is true when X is no longer a curve. One can show by an example that Theorem 1 does not in fact generalize. More precisely there exists an algebraic surface X and a family of 2-dimensional vector bundles E_k over X such that:

(i) E_k is indecomposable,
(ii) E_k has zero Chern classes (in positive dimensions),
(ii)′ E_k is topologically trivial,
(iii) if n_k is the least integer for which $E_k(n_k)$ is ample, then $n_k \to \infty$ as $k \to \infty$.

Actually, since X is of real dimension 4, (ii) and (ii)′ are equivalent statements. The example is a slight modification of an example given in (**2**). We consider a rational curve Y, an elliptic curve Z, and we put $X = Y \times Z$. Choosing base points in Y and Z we may regard Y and Z as embedded in X. For each integer $k \geqslant 1$ we define an extension:†

$$0 \to [kZ] \to E_k \to [-kZ] \to 0, \tag{A}$$

whose restriction to Z is non-trivial. Such an extension exists, the proof for any $k > 1$ being the same as that for $k = 1$ which is given in (**2**). Moreover E_k is indecomposable (cf. (**2**)) and its Chern classes are clearly zero. The restriction of (A) to Y is a trivial extension (cf. (**2**)), and so

$$E_k|Y \cong [kD] \oplus [-kD]$$

where D is a point divisor on Y. $Z+3Y$ is a hyperplane section of X, and D is a hyperplane section of Y. Suppose now that $E_k(n)$ is ample, then in particular it has sufficient sections and so $E_k(n)|Y$ also has sufficient sections. But $E_k(n)|Y \cong [(n+k)D] \oplus [(n-k)D]$, and this has sufficient sections only if $n \geqslant k$. Hence if n_k is the least integer n for which $E_k(n)$ is ample, then $n_k \geqslant k$ and so $n_k \to \infty$ as $k \to \infty$.

In the preceding example the bundles E_k do not arise from the fundamental group (cf. (**2**)). Hence it is still possible that the corollary of Theorem 1 may generalize. We should perhaps remark that for a *line-bundle* (over a non-singular complex algebraic variety) the answer to this problem is known. First of all a line-bundle L arises from the fundamental group if and only if its Chern class vanishes (rational coefficients). On the other hand, by a well-known theorem of Kodaira (**7**), there exists an integer n depending only on the Chern class of L, such that $L(n)$ is ample.

5. Second reduction method

In the preceding section we showed that any vector bundle over a non-singular curve has a splitting. We shall now give a more general reduction, valid for any base space.‡

† If D is any divisor we denote by $[D]$ the corresponding line-bundle.
‡ This theorem is essentially due to J.-P. Serre.

THEOREM 2. *Let E be a vector bundle over X with sufficient sections. Let $\dim E_x = r$, $\dim X = n$, with $r > n$. Then E has a trivial sub-bundle of dimension $r-n$.*

Proof. Let $V = \Gamma(E)$, and let P be the projective space corresponding to V. Since E has sufficient sections we have for each $x \in X$, an exact sequence (cf. § 2)

$$0 \to E'_x \to V \to E_x \to 0.$$

To prove the theorem it is sufficient to show the existence of a subvector space U of V such that

(i) $\dim U = r-n$,

(ii) $U \cap E'_x = 0$ for all x.

Let P'_x be the projective space in P corresponding to E'_x, and let Y be the subvariety of P generated by the P'_x. Then

$$\dim Y \leqslant \dim X + \dim P'_x = n + \dim P - r.$$

Hence there exists a linear subspace of P of dimension $r-n-1$ not intersecting Y. The corresponding vector subspace U of V has the required properties.

Theorem 2 shows that, over a space of dimension n, the basic vector bundles are those of dimension $\leqslant n$, all others being extensions of these by trivial bundles. For a curve, $n = 1$, and we derive once more the fact that every vector bundle has a splitting. We observe, however, that the present proof is valid even if the curve has singularities. The proof in § 4 was restricted to the non-singular case, but could easily have been modified to allow for singularities.

Let X be a non-singular curve and let the notation be as in § 4. We shall denote by I_s the trivial vector bundle of dimension s. Then combining Theorems 1 and 2 we obtain:

THEOREM 3. *Let n be any fixed integer $\geqslant N(g,r,d)$. Then every $E \in \mathscr{E}(r,d)$ is an extension of a line bundle L by a vector bundle $I_{r-1}(-n)$, where*

$$L = (\det E)((r-1)n).$$

The classes of extensions of L by $I_{r-1}(-n)$ are in (1–1) correspondence with the elements of

$$H^1(X, \mathbf{L}^* \otimes \mathbf{I}_{r-1}(-\mathbf{n})) \cong \Gamma(I_{r-1}) \otimes H^1(X, \mathbf{L}^*(-\mathbf{n})).$$

If we choose n so that $\deg L^*(-n) < 0$, then (by the Riemann–Roch theorem) this vector space will have a dimension independent of the choice of E. The totality of these vector spaces may then be given a vector bundle structure over the Picard variety of X (cf. (8)). Let this vector bundle be denoted by $\mathscr{F}$. Every point of $\mathscr{F}$ corresponds to an extension of L by $I_{r-1}(-n)$, and so to a vector bundle E over X. In this way, by Theorem 3, we obtain all $E \in \mathscr{E}(r,d)$. However, different extensions may give rise to isomorphic vector bundles, and some extensions may correspond to decomposable bundles. Thus the best we can assert is the following:

THEOREM 4. *$\mathscr{E}(r,d)$ is in (1–1) correspondence with a subset of $\mathscr{F}/Q$, where $\mathscr{F}$ is a vector bundle over the Picard variety of X, and Q is a fibre-preserving equivalence relation in $\mathscr{F}$.*

By a more detailed study of the situation one might use Theorem 4 to endow $\mathscr{E}(r,d)$ with the structure of an algebraic variety. For certain special cases ($g = 1, 2$; $r = 2$) this was essentially the method adopted in (**1**).

PART II

ELLIPTIC VECTOR BUNDLES—ADDITIVE STRUCTURE

From now on X will denote a non-singular curve of genus one. We shall denote by A a fixed line-bundle over X of degree one; this corresponds to fixing a base point on X. X may then be identified with its Picard (or Jacobian) variety, the base point being taken as the zero. Also the mapping $E \to E \otimes A^n$ defines a (1–1) correspondence $\mathscr{E}(r,d) \to \mathscr{E}(r,d+nr)$. Hence we may, if convenient, restrict ourselves to the range $0 \leqslant d < r$.

LEMMA 8. *If* $\deg E = d$, *then*

$$\dim \Gamma(E) - \dim H^1(X, E) = d.$$

This is a special case of the Riemann–Roch theorem (cf. Part I, § 4).

LEMMA 9. *Let E be a non-trivial extension of E_2 by E_1*

$$0 \to E_1 \to E \to E_2 \to 0.$$

Then $\Gamma \operatorname{Hom}(E_1, E_2) \neq 0$.

This is a special case of Lemma 5, since $K = 1$ for an elliptic curve.

LEMMA 6′. *Let E be indecomposable and with $\Gamma(E) \neq 0$. Then E has a maximal splitting $(L_1, L_2,..., L_r)$ with $L_i \geqslant L_1 \geqslant 1$.*

This was stated and proved in Part I. We merely reproduce it for convenience.

LEMMA 10. *Let $E \in \mathscr{E}(r,d)$, $0 \leqslant d < r$, and let $s = \dim \Gamma(E) > 0$. Then E has a trivial sub-bundle I_s.*

Proof. By Lemma 6′ E has a maximal splitting $(L_1, L_2,..., L_r)$ where $L_i \geqslant L_1 \geqslant 1$. If $\deg L_1 > 0$, then

$$d = \deg E = \sum_1^r \deg L_i \geqslant r \deg L_1 \geqslant r,$$

a contradiction. Hence $\deg L_1 = 0$, and since $L_1 \geqslant 1$ we must have $L_1 = 1$.

But L_1 is a maximal line-bundle of E. Hence, for all $\phi \in \Gamma(E)$, $\operatorname{div}\phi = 0$; in other words $\Gamma(E) \to E_x$ is a monomorphism for all x. Hence $\Gamma(E)$ generates a trivial sub-bundle I_s of E.

Note. The condition $s > 0$ is always satisfied if $d > 0$, by Lemma 8.

LEMMA 11. *Let $E \in \mathscr{E}(r,r)$. Then E has a maximal splitting $(L, L,\ldots, L)$ where* $\deg L = 1$.

Proof. By Lemma 8 $s = \dim \Gamma(E) \geqslant r$. Then by Lemma 6′ E has a maximal splitting $E = (L_1, L_2,\ldots, L_r)$ where $L_i \geqslant L_1 \geqslant 1$. If $\deg L_1 = 0$, then as in Lemma 10 we find that E has a trivial sub-bundle I_s. But this implies $s = r$ and $E = I_r$, a contradiction since E is indecomposable. Hence $\deg L_1 \geqslant 1$. But

$$r = \deg E = \sum_{1}^{r} \deg L_i \geqslant r \deg L_1,$$

equality holding if and only if $L_i \cong L_1$ for all i. Hence we must have $\deg L_1 = 1$ and $L_i \cong L_1$ for all i.

DEFINITION. *An extension $0 \to E' \xrightarrow{i} E \xrightarrow{p} E'' \to 0$ is said to be E''-partial if there exists a diagram*

$$\begin{array}{ccc} E & \xrightarrow{p} & E'' \\ & {}_{j}\nwarrow & \downarrow q \\ & & E''_1 \\ & & \downarrow \\ & & 0 \end{array}$$

with $E''_1 \neq 0$, the vertical column exact, and $qpj = 1$. An extension which is not E''-partial is said to be E''-complete.

Dually the extension is E'-partial if there exists a diagram

$$\begin{array}{ccc} 0 & & \\ \downarrow & & \\ E'_1 & \nwarrow^{q} & \\ j\downarrow & & \\ E' & \xrightarrow{i} & E \end{array}$$

with $E'_1 \neq 0$, the vertical column exact, and $qij = 1$. Clearly if an extension is E''-partial then the E''_1 given by the diagram is a direct factor of both E and E''. In particular, if E'' is indecomposable, an extension is E''-partial if and only if it is trivial.

LEMMA 12. *An extension $0 \to E' \xrightarrow{i} E \xrightarrow{p} I_s \to 0$ is I_s-complete if and only if $p_*\colon \Gamma(E) \to \Gamma(I_s)$ is zero.*

Proof. A direct factor of I_s is itself a trivial bundle (e.g. by the Krull–

Schmidt theorem (**3**)), and so the extension is I_s-complete if and only if there exists no diagram

$$\begin{array}{ccc} E & \xrightarrow{p} & I_s \\ & \nwarrow & \downarrow q \\ & j & 1 \\ & & \downarrow \\ & & 0 \end{array}$$

(with the vertical column exact and $qpj = 1$). Suppose such a diagram exists, then 1 is a direct factor of I_s and we get a diagram with exact vertical and $q_* p_* j_* = 1_*$

$$\begin{array}{ccc} \Gamma(E) & \xrightarrow{p_*} & \Gamma(I_s) \\ & \nwarrow & \downarrow q_* \\ & j_* & \Gamma(1) \\ & & \downarrow \\ & & 0 \end{array}$$

Hence $p_* \neq 0$. Conversely, suppose $p_* \neq 0$, then for some $\phi \in \Gamma(E)$, $p_*(\phi) = \psi \neq 0$. We have $\operatorname{div} \psi \geqslant \operatorname{div} \phi \geqslant 0$; but $\operatorname{div} \psi = 0$ since $\psi \in \Gamma(I_s)$. Hence $\operatorname{div} \phi = 0$, and so ϕ generates a trivial line-bundle $[\phi]$ of E mapped isomorphically by p onto the trivial line $[\psi]$ of I_s. Thus we get a diagram

$$\begin{array}{ccc} E & \xrightarrow{p} & I_s \\ \uparrow & & \downarrow q \\ [\phi] & \cong & [\psi] \\ & & \downarrow \\ & & 0 \end{array}$$

(in which q is any projection of I_s onto the direct factor $[\psi]$), which shows at once that the extension is I_s-partial. The lemma is therefore proved.

LEMMA 13. (i) *The classes of extensions*

$$(E)\colon 0 \to E' \to E \to I_s \to 0$$

are in (1–1) *correspondence with the 'coboundary homomorphisms'*

$$\delta\colon \Gamma(I_s) \to H^1(X, \mathbf{E}').$$

(ii) (E) *is* I_s*-complete if and only if* δ *is a monomorphism.*

(iii) *If* $\dim H^1(X, \mathbf{E}') = s$ *there exists a unique* E (*up to isomorphism*) *such that* (E) *is* I_s*-complete.*

Proof. (i) From the exact sequence $0 \to E' \xrightarrow{i} E \xrightarrow{p} I_s \to 0$ we obtain the exact cohomology sequence:

$$0 \to \Gamma(E') \xrightarrow{i_*} \Gamma(E) \xrightarrow{p_*} \Gamma(I_s) \to H^1(X, \mathbf{E}') \to. \tag{3}$$

Now the classes of extensions of I_s by E' are in (1–1) correspondence with the elements of

$$H^1(X, \mathrm{Hom}(\mathbf{I}_s, \mathbf{E}')) \cong \mathrm{Hom}(\Gamma(I_s), H^1(X, \mathbf{E}'))$$

(cf. (2)). Moreover, it is immediate from the way this correspondence is defined (cf. (2)), that it assigns to each extension (E) the homomorphism δ of the exact sequence (3).

(ii) Using (3) this is simply a restatement of Lemma 12.

(iii) If $\dim H^1(X, \mathbf{E}') = s$, then (E) will be I_s-complete provided δ is an isomorphism. Any two such isomorphisms differ by an automorphism of $\Gamma(I_s)$, and so the vector bundles E of the corresponding extensions are isomorphic.

LEMMA 13*. (i) *The classes of extensions*

$$(E)\colon 0 \to I_s \to E \to E' \to 0$$

are in (1–1) *correspondence with the 'coboundary homomorphisms'*

$$\delta\colon \Gamma(I_s^*) \to H^1(X, \mathbf{E}'^*).$$

(ii) (E) *is* I_s*-complete if and only if* δ *is a monomorphism.*

(iii) *If* $\dim H^1(X, \mathbf{E}'^*) = s$ *there exists a unique* E *(up to isomorphism) such that* (E) *is* I_s*-complete.*

Proof. This follows by duality from Lemma 13.

Remark. Lemmas 12, 13, 13* are valid for any algebraic variety. By contrast Lemma 14 which follows uses properties of the elliptic curve.

LEMMA 14. *Let* $0 \to I_s \to E \to E' \to 0$ *be* I_s*-complete. Then*

$$\dim \Gamma(E) = \dim \Gamma(E').$$

Proof. From the exact cohomology sequence

$$0 \to \Gamma(E'^*) \to \Gamma(E^*) \to \Gamma(I_s^*) \to H^1(X, \mathbf{E}'^*) \to,$$

and using Lemma 13* we see that $\Gamma(E'^*) \cong \Gamma(E^*)$. By duality this gives $\dim H^1(X, \mathbf{E}') = \dim H^1(X, \mathbf{E})$. Also we have $\deg E = \deg E'$, and so by Lemma 8 $\dim \Gamma(E) = \dim \Gamma(E')$.

We now give what is essentially a 'uniqueness theorem' for $\mathscr{E}(r, d)$. The 'existence theorem' will come later.

LEMMA 15. *Let* $E \in \mathscr{E}(r, d)$, $d \geqslant 0$. *Then*

(i) $s = \dim \Gamma(E) = d$ *if* $d > 0$

$= 0$ *or* 1 *if* $d = 0$;

(ii) *if* $d < r$, E *contains a trivial sub-bundle* I_s *and* $E' = E/I_s$ *is indecomposable; moreover* $\dim \Gamma(E') = s$.

Proof. If $d \geqslant r$, then as in the proof of Lemma 11, we find

$$E = (L_1, L_2, \ldots, L_r)$$

where each $L_i > 1$. Thus $H^1(X, \mathbf{L}_i) = 0$ and so $H^1(X, \mathbf{E}) = 0$ (cf. Lemma 1). Hence by Lemma 8 $\dim \Gamma(E) = d$. Suppose now that $d < r$. If $d = 0$ and $\Gamma(E) = 0$ there is nothing to prove; hence we may suppose that $\Gamma(E) \neq 0$ if $d = 0$. If $d > 0$, we always have $\Gamma(E) \neq 0$ by Lemma 8. Then by Lemma 10 we have an exact sequence:

$$(E)\colon 0 \to I_s \to E \to E' \to 0.$$

Since E is indecomposable (E) is certainly I_s-complete. Hence by Lemma 14 $\dim \Gamma(E') = \dim \Gamma(E) = s$, and so by duality $\dim H^1(X, \mathbf{E}'^*) = s$. By Lemma 13* the extension (E) corresponds to a monomorphism

$$\delta\colon \Gamma(I_s^*) \to H^1(X, \mathbf{E}'^*),$$

and since both terms here have dimension s, δ must be an isomorphism Suppose, if possible, that E' is decomposable: $E' = F \oplus G$ with $F \neq 0$, $G \neq 0$. Then we may write $\delta = \delta_1 \oplus \delta_2$ where

$$\delta_1\colon \Gamma(I_f^*) \to H^1(X, \mathbf{F}^*), \qquad \delta_2\colon \Gamma(I_g^*) \to H^1(X, \mathbf{G}^*)$$

are isomorphisms, $f = \dim H^1(X, \mathbf{F}^*)$, $g = \dim H^1(X, \mathbf{G}^*)$. By Lemma 13 δ_1 and δ_2 correspond to extensions

$$(E_1)\colon 0 \to I_f \to E_1 \to F \to 0,$$
$$(E_2)\colon 0 \to I_g \to E_2 \to G \to 0.$$

Thus $\delta_1 \oplus \delta_2$ corresponds to $(E_1) \oplus (E_2)$, and also to (E). Hence, by Lemma 13, $E \simeq E_1 \oplus E_2$, a contradiction. We observe that this proof is valid even if one of f, g is zero.

We have now proved (ii) and (i) for $d \geqslant r$. It remains to prove (i) for $0 \leqslant d < r$. We proceed by induction on r. For $r = 1$ (i) is certainly true; suppose it is true for all $r' < r$, in particular then for $r-s$. Hence, since $E' \in \mathscr{E}(r-s, d)$,

$$\dim \Gamma(E') = d \quad \text{if } d > 0$$
$$= 0 \text{ or } 1 \quad \text{if } d = 0.$$

But we have already shown that $\dim \Gamma(E') = \dim \Gamma(E)$. Hence (i) is established.

We shall now give the 'existence theorem'.

LEMMA 16. *Let $E' \in \mathscr{E}(r', d)$ $d \geqslant 0$, and if $d = 0$ we suppose $\Gamma(E') \neq 0$. Then there exists a vector bundle $E \in \mathscr{E}(r, d)$, unique up to isomorphism, given by an extension*

$$(E)\colon 0 \to I_s \to E \to E' \to 0,$$

where $r = r'+s$, and $s = d$ if $d > 0$

$$= 1 \text{ if } d = 0.$$

Proof. By Lemma 15 (i) we have $\dim \Gamma(E') = s$. Hence by Lemma 13* (iii) there exists a unique E (up to isomorphism) such that (E) is I_s-complete. It remains to show that in this case (E) is I_s-complete if and only if E is indecomposable. One direction is obvious, and we shall now prove the other, viz. if (E) is I_s-complete then E is indecomposable. Suppose if possible that $E = F \oplus G$, $F \neq 0$, $G \neq 0$. By Lemma 14

$$\dim \Gamma(E) = \dim \Gamma(E') = s,$$

so that $\Gamma(I_s) \to \Gamma(E)$ is an isomorphism. Let $\dim \Gamma(F) = f$, $\dim \Gamma(G) = g$, $f+g = s$. Then F must contain a trivial sub-bundle I_f and G must contain a trivial sub-bundle I_g, where $I_f \oplus I_g = I_s$. Hence $E' \cong E/I_s \cong F/I_f \oplus G/I_g$. But E' is indecomposable by hypothesis; hence either $F = I_f$, or $G = I_g$. But this would contradict the fact that (E) is I_s-complete. Thus E is indecomposable.

THEOREM 5. (i) *There exists a vector bundle $F_r \in \mathscr{E}(r, 0)$, unique up to isomorphism, with $\Gamma(F_r) \neq 0$. Moreover we have an exact sequence:*

$$0 \to 1 \to F_r \to F_{r-1} \to 0.$$

(ii) *Let $E \in \mathscr{E}(r, 0)$, then $E \cong L \otimes F_r$ where L is a line-bundle of degree zero, unique up to isomorphism (and such that $L \cong \det E$).*

Proof. (i) Consider all $E \in \mathscr{E}(r, 0)$ with $\Gamma(E) \neq 0$, and let $\bar{\mathscr{E}}(r, 0)$ be the corresponding set of equivalence classes. We prove by induction that $\bar{\mathscr{E}}(r, 0)$ consists of a single element f_r. For $r = 1$, there is only the trivial line-bundle. Suppose now that the result is true for all $r' < r$. If $E \in \bar{\mathscr{E}}(r, 0)$, then by Lemma 15 we have an exact sequence

$$0 \to 1 \to E \to E' \to 0,$$

where $E' \in \bar{\mathscr{E}}(r-1, 0)$. By inductive hypothesis we must have $E' \cong F_{r-1}$. On the other hand, by Lemma 16, there is a unique E (up to isomorphism) in $\bar{\mathscr{E}}(r, 0)$ given by an extension

$$0 \to 1 \to E \to F_{r-1} \to 0.$$

Thus $\bar{\mathscr{E}}(r, 0)$ consists of a single element and the induction is established.

(ii) Let $E \in \mathscr{E}(r, 0)$, then $E \otimes A \in \mathscr{E}(r, r)$ and so by Lemma 11

$$E \otimes A = (L_1, L_1, \ldots, L_1)$$

where $\deg L_1 = 1$. Hence $E \otimes A \otimes L_1^* \in \bar{\mathscr{E}}(r, 0)$, and so by (i)

$$E \otimes A \otimes L_1^* \cong F_r,$$

i.e. $E \cong F_r \otimes L$ where $L = L_1 \otimes A^*$. We must now show that $F_r \cong F_r \otimes L$ implies $L \cong 1$. But $F_r = (1, 1, \ldots, 1)$ and so $F_r \otimes L = (L, L, \ldots, L)$, where $\deg L = 0$. If L is not a trivial line-bundle, then

$$\dim \Gamma(F_r \otimes L) \leqslant r \dim \Gamma(L) = 0.$$

But $\dim \Gamma(F_r) = 1$. This gives the required contradiction. Finally, since $\det F_r \cong 1$ we get $\det E \cong L^r$.

COROLLARY 1. *F_r is self-dual, i.e.* $F_r \cong F_r^*$.

Proof. By construction F_r is a successive extension of trivial line-bundles. In particular F_r has 1 as a quotient bundle. Hence F_r^* has 1 as a sub-bundle and so $\Gamma(F_r^*) \neq 0$. Thus $F_r^* \in \bar{\mathscr{E}}(r, 0)$ and so, from Theorem 5 (i), $F_r^* \cong F_r$.

COROLLARY 2. *For all $s < r$ we have exact sequences*

$$0 \to F_s \to F_r \to F_{r-s} \to 0.$$

Proof. Since F_r has a unique trivial line-bundle 1, and since $F_r/1 \cong F_{r-1}$, it follows that F_r has, for each $s < r$, a *unique* sub-bundle E_s of dimension s which is a successive extension of trivial line-bundles, and we have an exact sequence:

$$0 \to E_s \to F_r \to F_{r-s} \to 0.$$

Interchanging s and $r-s$ and then dualizing we obtain an exact sequence

$$0 \to F_s^* \to F_r^* \to E_{r-s}^* \to 0.$$

By Corollary 1 $F_r^* \cong F_r$, $F_s^* \cong F_s$. But F_s is a successive extension of trivial line-bundles. Hence we must have $F_s \cong E_s$, by the uniqueness of E_s in F_r.

THEOREM 6. *Let A be a fixed line-bundle on X. Then A determines a* (1–1) *correspondence*

$$\alpha_{r,d}\colon \mathscr{E}(h, 0) \to \mathscr{E}(r, d),$$

where $h = (r, d)$ is the highest common factor of r and d. If we choose representative vector bundles E from the classes of $\mathscr{E}(h, 0)$, $\alpha_{r,d}$ is defined uniquely by the following properties:

(i) $\alpha_{r,0} = 1$ (*the identity*),

(ii) $\alpha_{r,d+r}(E) \cong \alpha_{r,d}(E) \otimes A$,

(iii) *if $0 < d < r$, we have an exact sequence*:

$$0 \to I_d \to \alpha_{r,d}(E) \to \alpha_{r-d,d}(E) \to 0.$$

Finally we have $\det \alpha_{r,d}(E) \cong \det E \otimes A^d$.

Proof. First A determines a (1–1) correspondence $\mathscr{E}(r, d) \leftrightarrow \mathscr{E}(r, d+r)$ by the operation $\otimes A$. Hence it is sufficient to consider $0 \leqslant d < r$. If $d = 0$ we have $h = r$ and we take $\alpha_{r,0} = 1$. If $d > 0$, then by Lemma 15 we have, for each $E \in \mathscr{E}(r, d)$, an exact sequence:

$$0 \to I_d \to E \to E' \to 0,$$

in which $E' \in \mathscr{E}(r-d, d)$. Conversely let $E' \in \mathscr{E}(r-d, d)$, then by Lemma 16 there is a unique E (up to isomorphism) in $\mathscr{E}(r, d)$ which is an extension of E' by I_d. This gives a (1–1) correspondence between $\mathscr{E}(r, d)$ and $\mathscr{E}(r-d, d)$. Using this together with (ii) we clearly obtain a (1–1) correspondence $\alpha_{r,d}\colon \mathscr{E}(h, 0) \to \mathscr{E}(r, d)$. The number of times the steps (ii) and (iii) have to be performed, and the order in which they occur are given explicitly by the Euclidean algorithm for determining the highest common factor h of r and d.

The formula for $\det \alpha_{r,d}(E)$ follows at once from (ii) and (iii).

In $\mathscr{E}(h, 0)$ we have the preferred element f_h. We put $e_A(r, d) = \alpha_{r,d}(f_h)$, so in particular

$$e_A(h, 0) = f_h.$$

By Theorem 5 (ii) $\mathscr{E}(h, 0)$ is in (1–1) correspondence with $\mathscr{E}(1, 0)$, i.e. with the Picard variety of X. Since X is of genus one the Picard variety may be identified with X itself, once we have picked a base point A. Thus by Theorem 6 we have a (1–1) correspondence between $\mathscr{E}(r, d)$ and X, and we may use this to define the structure of an algebraic curve on $\mathscr{E}(r, d)$. Using the final statements of Theorems 5 and 6 we can then summarize our results in the following form:

THEOREM 7. *Let X be an elliptic curve, A a fixed base point on X. We may regard X as an abelian variety with A as the zero element. Let $\mathscr{E}(r, d)$ denote the set of equivalence classes of indecomposable vector bundles over X of dimension r and degree d. Then each $\mathscr{E}(r, d)$ may be identified with X in such a way that*

$$\det\colon \mathscr{E}(r, d) \to \mathscr{E}(1, d) \text{ corresponds to } H\colon X \to X,$$

where $H(x) = hx = x+x+\ldots+x$ (h times), and $h = (r, d)$ is the highest common factor of r and d.

COROLLARY. *Let $h = (r, d) = 1$. Then if $E \in \mathscr{E}(r, d)$*

(i) *$E \to \det E$ gives a (1–1) correspondence $\mathscr{E}(r, d) \to \mathscr{E}(1, d)$,*

(ii) *$E \cong E_A(r, d) \otimes L$ for some line-bundle L of degree zero,*

(iii) *$E_A(r, d) \otimes L \cong E_A(r, d)$ if and only if $L^r \cong 1$,*

(iv) *$E_A(r, d)^* \cong E_A(r, -d)$.*

Proof. (i) is an immediate consequence of Theorem 7. (ii), (iii), and (iv) then follow from (i). In fact

$$\det[E_A(r, d) \otimes L] \cong A^d \otimes L^r;$$

but there exists an L such that $A^d \otimes L^r \cong \det E$, and $A^d \otimes L^r \cong A^d$ if and only if $L^r \cong 1$. Also $\det E_A(r, d)^* \cong \det E_A(r, -d) \cong A^{-d}$.

The analogue of this corollary for $h > 1$—which gives the Λ-module structure of $\hat{\mathscr{E}}$—is more involved, and we postpone consideration of it till Part III (cf. Theorem 10).

PART III

ELLIPTIC VECTOR BUNDLES—MULTIPLICATIVE STRUCTURE

1. The ring $\mathscr{F}$

It is well known that the multiplicative structure of the divisor class group depends on the characteristic of the ground field k. Thus, for an elliptic curve, if k is of characteristic zero there are n^2 divisor classes of order dividing n. But if k is of characteristic p there are either p^0 or p^1 divisor classes of order dividing p, according as the Hasse invariant of X is zero or non-zero. Clearly, therefore, the multiplicative structure of the ring $\mathscr{E}(X)$ will depend on the characteristic, and on the Hasse invariant. To avoid complication *we shall suppose k is of characteristic zero*, but we shall indicate whenever possible which results extend (with or without modification) to the case of characteristic p.

We start by examining the products $F_r \otimes F_s$, where F_r is the vector bundle defined in Theorem 5.

LEMMA 17. (i) $\dim \Gamma(F_r \otimes F_s) = \min(r, s)$,

(ii) *Let L be a line-bundle, then* $\dim \Gamma(L \otimes F_r \otimes F_s) = 0$ *unless* $L \geqslant 1$.

Proof. (i) Suppose $r \leqslant s$. If $r = 1$ then $\dim \Gamma(F_s) = 1$ (Lemma 15 (i)). We proceed by induction on $r > 1$. We have an exact sequence

$$0 \to 1 \to F_r \to F_{r-1} \to 0, \tag{4}$$

and hence an exact sequence

$$0 \to \mathrm{Hom}(F_{r-1}, F_s) \to \mathrm{Hom}(F_r, F_s) \xrightarrow{\beta} \mathrm{Hom}(1, F_s) \to 0.$$

Now we have an injection $i\colon F_r \to F_s$ (Corollary 2 of Theorem 5), and $\beta_*(i)$ is a generator of the one-dimensional vector space $\Gamma\,\mathrm{Hom}(1, F_s)$. Hence

$$\dim \Gamma\,\mathrm{Hom}(F_r, F_s) = \dim \Gamma\,\mathrm{Hom}(F_{r-1}, F_s) + 1.$$

But $F_r \cong F_r^*$ (Corollary 1 of Theorem 5), and so $\mathrm{Hom}(F_r, F_s) \cong F_r \otimes F_s$. Hence

$$\begin{aligned} \dim \Gamma(F_r \otimes F_s) &= \dim \Gamma(F_{r-1} \otimes F_s) + 1 \\ &= r - 1 + 1 \quad \text{by inductive hypothesis,} \\ &= r. \end{aligned}$$

(ii) Since $F_r = (1, 1, \ldots, 1)$ and $F_s = (1, 1, \ldots, 1)$, it follows that

$$L \otimes F_r \otimes F_s = (L, L, \ldots, L).$$

Hence $\Gamma(L \otimes F_r \otimes F_s) = 0$ unless $\Gamma(L) \neq 0$, i.e. unless $L \geqslant 1$.

LEMMA 18. $\qquad F_r \otimes F_s \cong \sum_{j=1}^{\min(r,s)} F_{r_j}, \qquad \sum_j r_j = rs.$

Proof. Let $F_r \otimes F_s \cong \sum_{j=1}^{N} E_j$ be the direct decomposition of $F_r \otimes F_s$ into indecomposable factors. We assert first that $\deg E_j = 0$ for all j. If not, since $\sum_j \deg E_j = 0$, $\deg E_j > 0$ for at least one j. Let L be a line-bundle of degree zero, $L \not\cong 1$. Then $\Gamma(L \otimes F_r \otimes F_s) = 0$ by Lemma 17. But $\deg(L \otimes E_j) > 0$ and so $\dim \Gamma(L \otimes E_j) > 0$ (Lemma 8). This gives a contradiction. Thus $E_j \in \mathscr{E}(r_j, 0)$, and so $E_j \cong L_j \otimes F_j$ (Theorem 5 (ii)). We assert that $L_j \cong 1$ for all j. If $L_j \not\cong 1$ then $\Gamma(L_j^* \otimes F_r \otimes F_s) = 0$ (Lemma 17), but $\Gamma(F_j) \neq 0$, a contradiction. Finally, since $\dim \Gamma(F_j) = 1$, we have

$$\begin{aligned} N &= \dim \Gamma(F_r \otimes F_s) \\ &= \min(r, s) \quad \text{by Lemma 17 (i).} \end{aligned}$$

COROLLARY. *Let $\mathscr{F}$ denote the subset of $\mathscr{E}$ generated by the f_r $(r \geqslant 1)$ with respect to $\oplus$, $\hat{\mathscr{F}}$ the corresponding subgroup of $\hat{\mathscr{E}}$. Then $\hat{\mathscr{F}}$ is a sub-ring of $\hat{\mathscr{E}}$.*

Considered abstractly $\hat{\mathscr{F}}$ is a commutative ring with unit satisfying the following conditions:

(*a*) with respect to addition $\hat{\mathscr{F}}$ is a free abelian group with elements f_r $(r = 1, 2, \ldots)$ as generators,†

(*b*) $f_r f_s = \sum_{j=1}^{\min(r,s)} f_{r_j}$, where $\sum_j r_j = rs$.

Condition (*b*) implies that $f_1 = 1$.

Since Lemmas 17 and 18 did not involve the characteristic of k, $\hat{\mathscr{F}}$ has the above properties whatever the characteristic. However, (*a*) and (*b*) do not quite suffice to determine $\hat{\mathscr{F}}$ completely, and we shall see that the structure of $\hat{\mathscr{F}}$ does in fact depend on the characteristic. We consider the following additional hypothesis on $\hat{\mathscr{F}}$,

$$(H_r): f_r^2 = 1 + \sum_{j=2}^{r} f_{r_j}.$$

Conditions under which this is satisfied are contained in the following lemma.

LEMMA 19. *Let p be the characteristic of k, and let r be prime to p. Then if E is a vector bundle of dimension r, we have a canonical decomposition:*

$$\mathrm{End}(E) \cong 1 \oplus E',$$

where E'_x is the subspace of $\mathrm{End}(E_x)$ *consisting of endomorphisms of trace zero.*‡

Proof. Let $\phi_x \in \mathrm{End}\, E_x$, and let trace $(\phi_x) = \lambda_x$. Then

$$\phi_x = \frac{\lambda_x}{r} 1_x + \left(\phi_x - \frac{\lambda_x}{r} 1_x\right)$$

† In the sense of *finite* linear combinations.

‡ $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ is the bundle of endomorphisms of E.

gives the canonical isomorphism, where 1_x denotes the identity endomorphism of E_x.

COROLLARY. *If r is prime to p, then $F_r \otimes F_r \cong 1 \oplus F'$.*

Proof. $F_r \cong F_r^*$ and so $\operatorname{End} F_r \cong F_r \otimes F_r$.

Thus $\mathscr{F}$ satisfies hypothesis (H_r) whenever r is prime to p. In particular if $p = 0$, $\mathscr{F}$ satisfies (H_r) for all r. We shall prove shortly that (a), (b), and (H_r) (for all r) characterize the ring $\mathscr{F}$. First we give a preliminary result:

LEMMA 20. *Let $\mathscr{F}$ be a ring satisfying (a) and (b). Then*

$$f_2 f_r = f_{r-1} + f_{r+1} \quad \textit{if } (H_r) \textit{ holds } (r \geqslant 2),$$
$$= 2f_r \quad \textit{otherwise.}$$

Proof. Consider first the case $r = 2$. By (b) we must have $f_2^2 = 1 + f_3$ or $f_2^2 = 2f_2$. Thus the lemma is true for $r = 2$. Assume now that it is true for $r-1$ $(r \geqslant 3)$, and let $f_2 f_r = f_s + f_{2r-s}$. Consider the equation

$$(f_2 f_{r-1}) f_r = f_{r-1}(f_2 f_r) = f_{r-1}(f_s + f_{2r-s}).$$

By inductive hypothesis $f_2 f_{r-1} = f_{r-2} + f_r$ or $2f_{r-1}$; in either case it follows from (b) that $(f_2 f_{r-1}) f_r$ contains $2r-2$ terms in its expansion. Hence, using (b) again, we see that we must have $s \geqslant r-1$, $2r-s \geqslant r-1$. Hence the only possibilities are:

(i) $f_2 f_r = f_{r-1} + f_{r+1}$,

(ii) $f_2 f_r = 2f_r$.

Suppose first that (H_r) holds, then if (ii) held we would get

$$f_2 f_r^2 = 2f_r^2.$$

The number of terms in $2f_r^2$ is $2r$, while in $f_2 f_r^2$ it is at most $2r-1$ (by (H_r) and (b)). This is a contradiction, and so we must have (i) if (H_r) holds.

Suppose now that (H_r) does not hold, and examine (i). This would give $f_2 f_r^2 = (f_{r-1} + f_{r+1}) f_r$. Since (H_r) is false $f_2 f_r^2$ contains $2r$ terms, while the right-hand side of this equation contains only $2r-1$ terms. This is a contradiction and so we must have (ii) if (H_r) does not hold. This completes the proof of the lemma.

LEMMA 21. *Let $\mathscr{F}$ be a ring satisfying (a), (b), and (H_r) for all $r \geqslant 1$. Then $\mathscr{F}$ is unique to within isomorphism, and the multiplicative structure is given by the formula:*

$$f_r f_s = f_{r-s+1} + f_{r-s+3} + \dots + f_{r+s-1} \quad (r \geqslant s).$$

Proof. If $s = 1$, $f_s = 1$ and the formula is trivial.

For $s = 2$ we have Lemma 20. Hence we may suppose $s \geqslant 3$ and we proceed by induction on s. We assume, therefore, that the formula is true for $s-2$ and $s-1$. Consider the associativity equation

$$f_2(f_{s-1}f_r) = (f_2 f_{s-1})f_r.$$

Applying the inductive hypothesis on the left and Lemma 20 on the right we get

$$f_2(f_{r-s+2}+f_{r-s+4}+\dots+f_{r+s-2}) = (f_{s-2}+f_s)f_r.$$

Now apply the inductive hypothesis on the right and Lemma 20 on the left and we get

$$f_{r-s+1}+2f_{r-s+3}+\dots+2f_{r+s-3}+f_{r+s-1} = f_{r-s+3}+\dots+f_{r+s-3}+f_r f_s.$$

Hence $f_r f_s = f_{r-s+1}+f_{r-s+3}+\dots+f_{r+s-1}$.

Combining our results together we get the following:

THEOREM 8. *Let X be an elliptic curve over a field of characteristic zero. Let $\mathscr{F}$ be the subring of $\hat{\mathscr{E}}(X)$ generated by those indecomposable bundles of degree zero which have a non-zero section. Then $\mathscr{F}$ is a free abelian group with f_r, $r \geqslant 1$, as generators and*

$$f_r f_s = f_{r-s+1}+f_{r-s+3}+\dots+f_{r+s-1} \quad (r \geqslant s).$$

The formula of Theorem 8 suggests a relationship with a similar formula in representation theory which we proceed to explain. Let E be a 2-dimensional vector bundle over any algebraic variety X. Then the Clebsch–Gordan formula for the tensor product of two polynomials gives rise to an isomorphism

$$S^p(E)\otimes S^q(E) \cong S^{p+q}(E)\oplus(\det E)\otimes S^{p-1}(E)\otimes S^{q-1}(E),$$

where S^p denotes the pth symmetric product. If we agree that $S^0(E)$ is to be the trivial line-bundle, then this formula is valid for $p, q \geqslant 1$. If in particular $\det E \cong 1$, then by iterating this formula we find

$$S^p(E)\otimes S^q(E) \cong S^{p+q}(E)\oplus S^{p+q-2}(E)\oplus \dots S^{p-q}(E) \quad (p \geqslant q).$$

We return now to the case of an elliptic curve X over a field of characteristic zero, and we prove:

THEOREM 9. *$F_r \cong S^{r-1}(F_2)$ for $r \geqslant 1$.*

Proof. For $r = 1, 2$ this is immediate. Suppose it is true for all $s < r$, $r \geqslant 3$. Then we have

$$S^1(F_2)\otimes S^{r-2}(F_2) \cong F_2 \otimes F_{r-1}.$$

Expanding the left-hand side by the formula given above and the right-hand side by Theorem 8, we get (since $\det F_2 \cong 1$)

$$S^{r-1}(F_2)\oplus S^{r-3}(F_2) \cong F_{r-2}\oplus F_r.$$

But, by inductive hypothesis, $S^{r-3}(F_2) \cong F_{r-2}$. Hence $S^{r-1}(F_2) \cong F_r$.

Remarks

(1) We have deduced Theorem 9 from Theorem 8. However, we could have proved Theorem 9 directly and Theorem 8 would then have followed from the Clebsch–Gordan formula.

(2) In characteristic p the ring $\mathscr{F}$ is more complicated, and we shall not examine it in full. However, one can show the following: $F_2 \otimes F_r \cong F_r \oplus F_r$ if $r \equiv 0 \bmod p$. This shows that (H_r) is false if and only if $r \equiv 0 \bmod p$ (cf. Lemma 20).

2. Λ-module structure of $\hat{\mathscr{E}}$

LEMMA 22. *Let $E \in \mathscr{E}(r,d)$ where $(r,d) = 1$. Then* $\operatorname{End} E \cong \sum_{i=1}^{r^2} L_i$, *where the L_i are the*† *line-bundles of order dividing r.*

Proof. For each line-bundle L_i of order dividing r we have

$$E \otimes L_i \cong E$$

(Corollary to Theorem 7). Hence

$$E^* \otimes E \otimes L_i \cong E^* \otimes E, \quad \text{i.e. } \operatorname{End} E \otimes L_i \cong \operatorname{End} E.$$

But $\operatorname{End} E$ contains 1 as a direct summand (Lemma 19). Hence $\operatorname{End} E$ contains each L_i as direct summand. But there are exactly r^2 such L_i, and $\operatorname{End} E$ is an r^2-dimensional bundle. Hence $\operatorname{End} E \cong \sum_{i=1}^{r^2} L_i$.

This lemma is the key to the determination of the ring structure of $\hat{\mathscr{E}}$. It will be used constantly. We note in passing that it fails to hold in characteristic p for two reasons: (i) Lemma 19 does not hold, (ii) the number of L_i of order dividing r is not always r^2.

LEMMA 23. *Let $(r,d) = 1$, then $E_A(r,d) \otimes F_h$ is indecomposable.*

Proof. Put $E = E_A(r,d) \otimes F_h$. Then

$$\operatorname{End} E \cong \operatorname{End} E_A(r,d) \otimes \operatorname{End} F_h,$$

and applying Lemma 22 and Theorem 8 we get:

$$\operatorname{End} E \cong \Big(\sum_{i=1}^{r^2} L_i\Big) \otimes \Big(\sum_{k=1}^{h} F_{2k-1}\Big).$$

Now $\Gamma(L_i \otimes F_k) = 0$ unless $L_i \cong 1$ (Lemma 17 (ii)), and this holds for just one value of i. Hence $\Gamma \operatorname{End} E \cong \Gamma \operatorname{End} F_h$, the isomorphism being given by $I \otimes \phi \longleftrightarrow \phi$, where I is the identity endomorphism of $E_A(r,d)$. Hence this isomorphism is an isomorphism of algebras. But the structure

† More precisely $L_i^r \cong 1$ and L_i and L_j are not isomorphic if $i \neq j$. The L_i are unique to within isomorphism.

of the algebra $\Gamma\,\mathrm{End}\,E$ determines whether or not E decomposes. Hence, since F_h is indecomposable, it follows that E is indecomposable.

We shall next find the precise element in $\mathscr{E}(rh, dh)$ defined by $E_A(r,d) \otimes F_h$.

LEMMA 24. *Let* $(r,d) = 1$, *then*

$$E_A(r,d) \otimes F_h \cong E_A(rh, dh).$$

Proof. We prove the lemma by double induction on r and h. More precisely we assume the lemma true (for $h, r \geqslant 2$)

(i) for $h-1$ and all r,

(ii) for h and all $s \leqslant r-1$.

First we observe that if $h = 1$, then $F_h = 1$, and so the lemma is true for all r. Also if $r = 1$, $E_A(r,d) = A^d$, $E_A(rh, dh) = A^d \otimes F_h$ by definition. This starts the induction.

Now we have the exact sequence:

$$0 \to 1 \to F_h \to F_{h-1} \to 0. \tag{5}$$

(5) $\otimes\, E_A(r,d)$ gives the exact sequence:

$$0 \to E_A(r,d) \to E_A(r,d) \otimes F_h \to E_A(r,d) \otimes F_{h-1} \to 0. \tag{6}$$

Since $E_A(r,d) \otimes A \cong E_A(r, d+r)$ it suffices to consider the range $0 < d < r$. Then also $0 < dh < rh$, $0 < d(h-1) < r(h-1)$. For brevity we write (6) as $0 \to E_1 \to E_2 \to E_3 \to 0$, and we put $d_i = \deg E_i$, $r_i = \dim E_i$. Then $E_i \in \mathscr{E}(r_i, d_i)$ (Lemma 23), $0 < d_i < r_i$. Hence, by the results of Part II, $\dim \Gamma(E_i) = d_i$ and $\Gamma(E_i)$ generates a trivial sub-bundle I_{d_i} of E_i; moreover, if $E_i' = E_i/I_{d_i}$ then $E_i' \in \mathscr{E}(r_i - d_i, d_i)$, and $E_i \cong E_A(r_i, d_i)$ if and only if $E_i' \cong E_A'(r_i - d_i, d_i)$. Thus we have an exact sequence diagram:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & I_{d_1} & \to & I_{d_2} & \to & I_{d_3} & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & E_1 & \to & E_2 & \to & E_3 & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & E_1' & \to & E_2' & \to & E_3' & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Applying inductive hypothesis (i) in the last column of the diagram, we find $E_3 \cong E_A(r_3, d_3)$, hence $E_3' \cong E_A(r_3 - d_3, d_3)$ and so again by (i)

$$E_3' \cong E_A(r-d, d) \otimes F_{h-1}.$$

Also $E_1' = E_A(r-d, d)$, hence

$$\begin{aligned}
\dim \Gamma\,\mathrm{Hom}(E_1', E_3') &= \dim \Gamma(\mathrm{End}\,E_A(r-d,d) \otimes F_{h-1}) \\
&= 1 \quad \text{by Lemma 22 and Theorem 5.}
\end{aligned}$$

Now the extension classes of E'_3 by E'_1 correspond to the elements of $H^1(X, \mathrm{Hom}(E'_3, E'_1))$, and the extensions corresponding to a, λa, where $a \in H^1(X, \mathrm{Hom}(E'_3, E_1))$ and λ is a non-zero constant, define isomorphic vector bundles. In the present case this vector space is of dimension one (by duality) and so any two non-trivial extensions define isomorphic vector bundles. Now the bottom row of the diagram is one extension, and (5) $\otimes E_A(r-d, d)$ is another. Moreover, both are non-trivial extensions since E'_2 and $E_A(r-d, d) \otimes F_h$ are indecomposable (the latter by Lemma 23 or by (ii)). Hence

$$E'_2 \cong E_A(r-d, d) \otimes F_h \cong E_A(h(r-d), hd) \quad \text{by inductive hypothesis (ii).}$$

Thus $E_2 \cong E_A(rh, dh)$, and the induction is established.

COROLLARY 1. *For any r, d, $E_A(r,d) \otimes L \cong E_A(r,d)$ if and only if $L^{r/h} \cong 1$, where $h = (r,d)$.*

Proof. Put $r' = r/h$, $d' = d/h$, then by Lemma 24

$$E_A(r,d) \cong E_A(r',d') \otimes F_h.$$

Suppose L is of order dividing r', then by the Corollary to Theorem 7 $E_A(r',d') \otimes L \cong E_A(r',d')$. Hence, $E_A(r,d) \otimes L \cong E_A(r,d)$.

Conversely, suppose that L is such that this holds. Then

$$\mathrm{End}\, E_A(r,d) \otimes L \cong \mathrm{End}\, E_A(r,d).$$

But, by Lemma 22 and Theorem 8, we have

$$\mathrm{End}\, E_A(r,d) \cong \mathrm{End}\, E_A(r',d') \otimes \mathrm{End}\, F_h$$
$$\cong \Big(\sum_{i=1}^{r'^2} L_i\Big) \otimes \Big(\sum_{k=1}^{h} F_{2k-1}\Big).$$

Hence, equating the line-bundle summands of

$$\mathrm{End}\, E_A(r,d) \quad \text{and} \quad \mathrm{End}\, E_A(r,d) \otimes L,$$

we see that $L \cong L_i$ for some i, i.e. $L^{r'} \cong 1$.

COROLLARY 2. $E_A(r,d)^* \cong E_A(r,-d)$.

Proof. By Lemma 24 $E_A(r,d)^* \cong E_A(r',d')^* \otimes F_h^*$, where $h = (r,d)$, $r' = r/h$, $d' = d/h$. But $F_h^* \cong F_h$ (Corollary 1 to Theorem 5) and

$$E_A(r',d')^* \cong E_A(r',-d') \quad \text{(Corollary to Theorem 7).}$$

Hence

$$E_A(r,d)^* \cong E_A(r',-d') \otimes F_h$$
$$\cong E_A(r,-d) \quad \text{by Lemma 24.}$$

LEMMA 25. *Let $(r,d) = 1$, $0 < d < r$ and let L be a line-bundle of degree zero. Then we have an exact sequence:*

$$0 \to I_{dh} \to E_A(rh, dh) \otimes L \to E_A(rh-dh, dh) \otimes L' \to 0,$$

where L' is any line-bundle such that $L'^{(r-d)} \cong L^r$.

Proof. For $h = 1$ this follows from the Corollary to Theorem 7. We proceed by induction on h and we use the diagram in the proof of Lemma 24. We operate on the middle row by $\otimes L$, and we then get a new diagram of the same form in which E'_1, E'_3 are replaced respectively by $E'_1 \otimes L'$, $E'_3 \otimes L'$ with $L'^{(r-d)} \cong L^r$ (the induction hypothesis for the third column and $h = 1$ for the first). But, as before, the middle term in the bottom row is then uniquely determined (up to isomorphism) and so must be $E'_2 \otimes L'$. This completes the proof.

LEMMA 26. *Let $E \in \mathscr{E}(r,d)$. Then there exists a line-bundle L such that $E \cong E_A(r,d) \otimes L$.*

Proof. We proceed by induction on r. Also we may assume $0 < d < r$, since for $d = 0$ we have Theorem 5. Then we have an exact sequence:

$$0 \to I_d \to E \to E' \to 0.$$

By inductive hypothesis $E' \cong E_A(r-d, d) \otimes L'$ for some L'. Let L be any line-bundle such that $L^{r/h} \cong L'^{(r-d)/h}$, where $h = (r,d)$. Then by Lemma 25 we have the exact sequence:

$$0 \to I_d \to E_A(r,d) \otimes L \to E' \to 0.$$

Hence $E \cong E_A(r,d) \otimes L$.

Combining Corollary 1 to Lemma 24 with Lemmas 25 and 26 we obtain:

THEOREM 10. *Every vector bundle $E \in \mathscr{E}(r,d)$ is of the form $L \otimes E_A(r,d)$, and $L \otimes E_A(r,d) \cong E_A(r,d)$ if and only if $L^{r/h} \cong 1$, $h = (r,d)$. Moreover, if $\alpha_{r,d}\colon \mathscr{E}(h,0) \to \mathscr{E}(r,d)$ is the* (1–1) *correspondence given by Theorem* 6, *we have*

$$\alpha_{r,d}(L^{r/h} \otimes F_h) \cong L \otimes \alpha_{r,d}(F_h) \cong L \otimes E_A(r,d).$$

Theorem 10 identifies $\mathscr{E}(r,d)$ more precisely than Theorem 7 and gives the complete Λ-module structure of $\hat{\mathscr{E}}$. As we remarked in Part I § 3 this enables us to determine all projective bundles. Since E and $E \otimes L$ decompose together it follows that we may speak of a projective bundle as being indecomposable. Hence if $P_r = GL_r(k)/k^*$ we obtain:

THEOREM 11. *There are just r equivalence classes of indecomposable P_r-bundles over X.*

Remark. We have determined the Λ-module structure of $\hat{\mathscr{E}}$ via the ring structure. Actually it is possible, though considerably more complicated, to avoid using the ring structure. In particular Theorems 10 and 11 still hold in characteristic p.

3. Ring structure of $\hat{\mathscr{E}}$

LEMMA 27. *Let $(r,d) = (r',d') = 1$, $(r,r') = k$, and let*

$$E_A(r,d) \otimes E_A(r',d') \cong \sum_i E_i,$$

where $E_i \in \mathscr{E}(r_i, d_i)$. Then r_i divides rr'/k and $(r_i, d_i) = 1$.

Proof. Let $E = E_A(r,d) \otimes E_A(r',d')$. Then, by Lemma 22,

$$\operatorname{End} E \cong (\sum L_j) \otimes (\sum L'_m),$$

where the L_j (L'_m) are the line-bundles of order dividing r (r'). Let $h_i = (r_i, d_i)$, then $E_i \cong \bar{E}_i \otimes F_{h_i}$, $\bar{E}_i \in \mathscr{E}(r_i/h_i, d_i/h_i)$ (by Lemmas 26 and 24). Hence

$$\operatorname{End} E_i \cong (\sum \bar{L}_n) \otimes \Big(\sum_{l=1}^{h_i} F_{2l-1}\Big),$$

where the $\bar{L}_n$ are the line-bundles of order dividing r_i/h_i. But $\operatorname{End} E_i$ is a direct summand of $\operatorname{End} E$, and so must decompose completely into line-bundles. This is only possible if $h_i = 1$, i.e. $(r_i, d_i) = 1$. Also the $\bar{L}_n$ must then be of the form $L_j \otimes L'_m$, and so of order dividing rr'/k. Hence r_i divides rr'/k.

If $k = 1$ the situation is very simple and we have:

LEMMA 28. *Let $(r,d) = (r',d') = (r,r') = 1$. Then*

$$E_A(r,d) \otimes E_A(r',d') \cong E_A(rr', rd'+r'd).$$

Proof. Put $E = E_A(r,d) \otimes E_A(r',d')$. Then, by Lemma 22,

$$\operatorname{End} E \cong \sum_{i,m} L_i \otimes L'_m,$$

where the L_i are of order dividing r, the L'_m of order dividing r'. But $L_i \otimes L'_m \cong 1$ implies $L_i \cong L'_m \cong 1$ (since $(r,r') = 1$), and this occurs for just one pair (i,m). Hence $\dim \Gamma \operatorname{End} E = 1$, and so every endomorphism of E is a multiple of the identity. Hence E is indecomposable, and so $E \in \mathscr{E}(rr', rd'+r'd)$. But $\det E \cong \det E_A(r,d) \otimes \det E_A(r',d') \cong A^{rd'+r'd}$. Hence, since $(rr', rd'+r'd) = 1$, $E \cong E_A(rr', rd'+r'd)$ (Corollary to Theorem 7).

LEMMA 29. *Let $(r,d) = 1$, and let $r = r_1 r_2 \dots r_n$ be the factorization of r into prime powers, i.e. $r_i = p_i^{k_i}$ where the p_i are distinct primes. Then $E_A(r,d) \cong E_A(r_1,d_1) \otimes \dots \otimes E_A(r_n,d_n)$ if and only if $\sum_i (d_i/r_i) = d/r$. In particular such decompositions of $E_A(r,d)$ always exist, and they may all be obtained from any given one by replacing $E_A(r_i,d_i)$ by $E_A(r_i,d_i) \otimes A^{m_i}$, where $\sum m_i = 0$.*

Proof. If $E_A(r,d) \cong E_A(r_1,d_1) \otimes \dots \otimes E_A(r_n,d_n)$, then equating degrees we find $d = \sum_i r_1 r_2 \dots r_{i-1} d_i r_{i+1} \dots r_n = r \sum_i d_i/r_i$. Conversely let $(d_1,\dots,d_n)$ be any sequence of integers such that $\sum_i (d_i/r_i) = d/r$. Since $(r,d) = 1$ it follows that $(r_i,d_i) = 1$. Hence, since the r_i are mutually prime, we may apply Lemma 28 $(n-1)$ times and we get

$$E_A(r_1,d_1) \otimes \dots \otimes E_A(r_n,d_n) \cong E_A(r,d).$$

The equation $\sum(d_i/r_i) = d/r$ always has solutions (d_i), this being the decomposition of d/r into 'partial fractions'. Also if (d_i) is one solution, any other is of the form $(d_i+m_i r_i)$ where $\sum m_i = 0$. Since

$$E_A(r_i, d_i+m_i r_i) \cong E_A(r_i, d_i) \otimes A^{m_i},$$

this establishes the last part of the lemma.

We proceed now to state our results in terms of the ring structure of $\hat{\mathscr{E}}$. We consider the following sets:

$\mathscr{A}$: the set of all $\{r, d\}$ with $r \geqslant 1$, $0 \leqslant d < r$,

$\mathscr{A}_0$: the subset of $\mathscr{A}$ with $d = 0$,

$\mathscr{A}_p$: the subset of $\mathscr{A}$ with $r = p^k$, p a prime, $k \geqslant 0$, and $(p, d) = 1$.

We note that $\mathscr{A}_0 \cap \mathscr{A}_p = \mathscr{A}_p \cap \mathscr{A}_q$ is the set consisting of the single element $\{1, 0\}$ (p, q distinct primes).

If $\alpha = \{r, d\} \in \mathscr{A}$ we write $e_\alpha = e_A(r, d)$, and we denote by $\hat{\mathscr{E}}_\alpha$ the Λ-module generated by e_α. In particular if $\alpha = \{1, 0\}$, $e_\alpha = 1$ (the unit of the ring $\hat{\mathscr{E}}$) and $\hat{\mathscr{E}}_\alpha = \Lambda$. We first reinterpret Theorem 10 to give the following:

LEMMA 30. *Let $\alpha = \{r, d\} \in \mathscr{A}$, $h = (r, d)$, $r' = r/h$. Then we have an exact sequence of Λ-modules*

$$0 \to \Lambda(r') \to \Lambda \xrightarrow{\epsilon_\alpha} \hat{\mathscr{E}}_\alpha \to 0,$$

where $\epsilon_\alpha(\lambda) = \lambda e_\alpha$, and $\Lambda(r')$ is the ideal of Λ generated by the elements $(1-l)$ with l an r'-th root of unity.

Proof. We have just to show that $\Lambda(r')$ is the ideal which annihilates e_α. Let $\lambda e_\alpha = 0$. Then we can write λ uniquely in the form $\sum \lambda_i - \sum \mu_j$, where λ_i and μ_j correspond to line-bundles. Then $\sum \lambda_i e_\alpha = \sum \mu_j e_\alpha$, and so after re-ordering the suffixes we must have $\lambda_i e_\alpha = \mu_i e_\alpha$. Then, by Theorem 10, $\mu_i \lambda_i^{-1} = l_i$ is an r'th root of unity. But $\lambda = \sum \lambda_i(1-l_i)$, and so $\lambda \in \Lambda(r')$. Conversely every element of $\Lambda(r')$ is of this form and so, by Theorem 10, it annihilates e_α.

Theorem 10 asserts that, as a Λ-module, $\hat{\mathscr{E}} \cong \sum_{\alpha \in \mathscr{A}} \hat{\mathscr{E}}_\alpha$. We consider now the following sub-modules of $\hat{\mathscr{E}}$:

$$\hat{\mathscr{E}}_0 = \sum_{\alpha \in \mathscr{A}_0} \hat{\mathscr{E}}_\alpha,$$

$$\hat{\mathscr{E}}_p = \sum_{\alpha \in \mathscr{A}_p} \hat{\mathscr{E}}_\alpha.$$

Now if $\alpha \in \mathscr{A}_0$, $\alpha = \{r, 0\}$, $e_\alpha = f_r$ and $r' = 1$. Hence $\hat{\mathscr{E}}_0 \cong \Lambda \otimes \mathscr{F}$ (tensor product of abelian groups), and so $\hat{\mathscr{E}}_0$ is a *sub-ring* of $\hat{\mathscr{E}}$ (since $\mathscr{F}$ is a sub-ring of $\hat{\mathscr{E}}$: Corollary to Lemma 17). Also Lemma 27 shows immediately that $\hat{\mathscr{E}}_p$ is a *sub-ring* of $\hat{\mathscr{E}}$.

Let π be any infinite sequence; if $i \in \pi$ we write $i+1$ for the successor of i in π. Let $\{A_i;\, i \in \pi\}$ be a sequence of rings such that A_i contains a fixed ring Λ for all i. Then we may form the *restricted* infinite tensor product over Λ of the A_i, and we denote it by $\otimes_i A_i$ or A_π. It may be defined as the direct limit (or union) of the finite tensor products

$$B_i = A_1 \otimes_\Lambda A_2 \otimes_\Lambda \dots \otimes_\Lambda A_i$$

under the inclusions $B_i \to B_i \otimes_\Lambda \Lambda \subset B_{i+1}$. A_π is not only a Λ-module but also a ring. If $A_i = \Lambda$ for all but a finite number of indices ($i_1,\dots, i_r$, say), then $A_\pi \cong A_{i_1} \otimes_\Lambda \dots \otimes_\Lambda A_{i_r}$. Similarly if $\{A_i\}$ is any infinite sequence of sets, and if A_i contains a fixed element 1 for all i, we may define A_π as the direct limit (or union) of the finite products $B_i = A_1 \times A_2 \times \dots \times A_i$ under the injections $B_i \to B_i \times 1 \subset B_{i+1}$. Again if $A_i = 1$ for all but a finite number of indices ($i_1,\dots, i_r$, say), then $A_\pi \cong A_{i_1} \times \dots \times A_{i_r}$.

In the present case we take π to be the sequence consisting of 0 and all primes p. Since $\hat{\mathscr{E}}_0$, $\hat{\mathscr{E}}_p$ contain Λ we obtain the ring $\hat{\mathscr{E}}_\pi$. Since the sets $\mathscr{A}_0$, $\mathscr{A}_p$ contain the fixed element $\{1, 0\}$, we obtain the set $\mathscr{A}_\pi$. If $\sigma \in \mathscr{A}_\pi$, then $\sigma = (\alpha_0,\dots, \alpha_p,\dots)$ where all but a finite number of the α's $= \{1, 0\}$. Since σ is itself an infinite sequence we may form $\hat{\mathscr{E}}_\sigma$, and as we remarked above $\hat{\mathscr{E}}_\sigma$ can be identified with the corresponding finite tensor product. Thus $\hat{\mathscr{E}}_\sigma = \Lambda e_\sigma$, where $e_\sigma = \otimes_i e_{\alpha_i}$. By definition $\hat{\mathscr{E}}_0 = \sum_{\alpha \in \mathscr{A}_0} \hat{\mathscr{E}}_\alpha$, $\hat{\mathscr{E}}_p = \sum_{\alpha \in \mathscr{A}_p} \hat{\mathscr{E}}_\alpha$. Hence $\hat{\mathscr{E}}_\pi = \sum_{\sigma \in \mathscr{A}_\pi} \hat{\mathscr{E}}_\sigma$. On the other hand, $\hat{\mathscr{E}} = \sum_{\alpha \in \mathscr{A}} \hat{\mathscr{E}}_\alpha$. Our object is to set up an isomorphism between $\hat{\mathscr{E}}_\pi$ and $\hat{\mathscr{E}}$. First we shall define a commutative diagram of maps (where Z denotes the integers)

$$\begin{array}{ccc} \mathscr{A}_\pi & \xrightarrow{\phi} & \mathscr{A} \times Z \\ & \searrow^{\theta} & \downarrow \psi \\ & & \mathscr{A} \end{array}$$

Let $\sigma \in \mathscr{A}_\pi$, then $\sigma = \{\alpha_i;\, i \in \pi\}$ where $\alpha_i = \{1, 0\}$ for all but a finite number of indices i. Let $\alpha_i = \{r_i, d_i\}$ and define integers r, d, m by

$$r = \prod_{i \in \pi} r_i, \qquad \sum_{i \in \pi} (d_i/r_i) = d/r + m, \quad 0 \leqslant d < r.$$

Conversely, given integers r, d, with $0 \leqslant d < r$ these equations define the $\{r_i, d_i\}$ and m uniquely (cf. Lemma 29). We define $\phi(\sigma) = (\{r, d\}, m)$, and we let $\psi\colon \mathscr{A} \times Z \to \mathscr{A}$ be the natural projection. Then $\theta = \psi\phi$ defines a (1–1) correspondence between $\mathscr{A}_\pi$ and $\mathscr{A}$.

LEMMA 31. *Let $\sigma \in \mathscr{A}_\pi$, $\phi(\sigma) = (\alpha, m) \in \mathscr{A} \times Z$. Then there is a Λ-module isomorphism*

$$\Phi_\sigma\colon \hat{\mathscr{E}}_\sigma \to \hat{\mathscr{E}}_\alpha$$

defined by $\Phi_\sigma(e_\sigma) = a^m e_\alpha$, where $a \in \Lambda$ corresponds to the basic line-bundle A.

Proof. It is sufficient to show that the ideals of Λ which annihilate e_σ and e_α are the same. Let $\sigma = \{\alpha_i\}$, $\alpha_i = \{r_i, d_i\}$, $\alpha = \{r, d\}$, $h_i = (r_i, d_i)$,

$h = (r, d)$, $r' = r/h$, $r'_i = r_i/h_i$. Then by Lemma 30 the annihilator of e_α is $\Lambda(r')$ and the annihilator of e_{α_i} is $\Lambda(r'_i)$. But $r'_0 = 1$, $r'_p = r_p$, and from the definition of ϕ it follows that $h = r_0$, $r' = \prod_p r_p$. Hence the annihilator of $e_\sigma = \otimes_i e_{\alpha_i}$ is $\otimes_p \Lambda(r_p)$, and since the r_p are mutually prime this is precisely $\Lambda(r')$.

Let $\sigma \in \mathscr{A}_\pi$, $\sigma = \{\alpha_i\}$ and let $\phi(\sigma) = (\alpha, m)$. Then Lemmas 24 and 29 give the formula

$$a^m e_\alpha = \prod_i e_{\alpha_i}. \tag{7}$$

On the other hand, we have

$$e_\sigma = \otimes_i e_{\alpha_i}. \tag{8}$$

Hence, if we define a Λ-module isomorphism $\Phi: \hat{\mathscr{E}}_\pi \to \hat{\mathscr{E}}$ by $\Phi = \sum_{\sigma \in \mathscr{A}_\pi} \Phi_\sigma$, (7) and (8) show that Φ preserves the ring structure and so is a ring isomorphism. We summarize our results in a theorem.

THEOREM 12. *Let $\hat{\mathscr{E}}_\pi$ denote the restricted infinite tensor product of the rings $\hat{\mathscr{E}}_0$, $\hat{\mathscr{E}}_p$ (over all primes p), and let $\mathscr{A}_\pi$ denote the restricted product of the sets $\mathscr{A}_0$, $\mathscr{A}_p$. Then as Λ-modules we have: $\hat{\mathscr{E}}_\pi = \sum_{\sigma \in \mathscr{A}_\pi} \hat{\mathscr{E}}_\sigma$, $\hat{\mathscr{E}} = \sum_{\alpha \in \mathscr{A}} \hat{\mathscr{E}}_\alpha$. Let $\theta: \mathscr{A}_\pi \to \mathscr{A}$ be the (1–1) correspondence defined above. Then there are Λ-module isomorphisms*

$$\Phi_\sigma: \hat{\mathscr{E}}_\sigma \to \hat{\mathscr{E}}_{\theta(\sigma)}$$

and $\Phi = \sum_{\sigma \in \mathscr{A}_\pi} \Phi_\sigma$ gives a ring isomorphism $\hat{\mathscr{E}}_\pi \to \hat{\mathscr{E}}$.

In view of Theorem 12 the ring structure of $\hat{\mathscr{E}}$ is completely determined by the ring structure of the sub-rings $\hat{\mathscr{E}}_0$, $\hat{\mathscr{E}}_p$. Since we have already determined the ring structure of $\mathscr{F}$ (Theorem 8) and so of $\hat{\mathscr{E}}_0 \cong \Lambda \otimes \mathscr{F}$, we need only consider the ring $\hat{\mathscr{E}}_p$. This problem is considered in the next section.

4. Ring structure of $\hat{\mathscr{E}}_p$

LEMMA 32. *Let $(r, d) = (r', d') = 1$. Then $E_A(r, d) \otimes E_A(r', d')$ contains a line-bundle as a direct summand if and only if $r' = r$, $d' \equiv -d \bmod r$.*

Proof. Suppose $E_A(r, d) \otimes E_A(r', d') \cong L \oplus \ldots$ where L is a line-bundle. Operate by $E_A(r, d)^* \otimes$ on both sides. The left-hand side becomes

$$\sum L_i \otimes E_A(r', d'),$$

where the L_i are the line-bundles of order dividing r (Lemma 22). The right-hand side contains $L \otimes E_A(r, d)^*$ as a direct summand. Hence, for some L_i,

$$L_i \otimes E_A(r', d') \cong L \otimes E_A(r, d)^*.$$

But $E_A(r, d)^* \cong E_A(r, -d)$ (Corollary 2 to Lemma 24). Hence $r' = r$, $d' \equiv -d \bmod r$. The converse is immediate by Lemma 22.

LEMMA 33. *Let* $(r,d) = (r',d') = 1$. *Then*

$$E_A(r,d) \otimes E_A(r',d') \cong F \otimes E_A(r'',d''),$$

where F *is a direct sum of line-bundles.*

Proof. By Lemma 27 $E = E_A(r,d) \otimes E_A(r',d') \cong \sum_i E_i$, where

$$E_i \in \mathscr{E}(r_i,d_i) \quad \text{and} \quad (r_i,d_i) = 1.$$

Now $\operatorname{End} E \cong \operatorname{End} E_A(r,d) \otimes \operatorname{End} E_A(r',d')$ decomposes completely into a direct sum of line-bundles (Lemma 22). Hence each pair $E_i \otimes E_j^*$ must decompose completely, and so by Lemma 32 $r_i = r_j = r''$, say, and $d_i \equiv d_j \bmod r''$. Put $d'' = d_1$, and let $d_i = d_1+n_i r''$. Then

$$E_i \cong L_i \otimes E_A(r'',d'')$$

for some line bundle L_i and

$$\sum_i E_i \cong \Big(\sum_i L_i\Big) \otimes E_A(r'',d'').$$

Remark. In terms of the ring $\hat{\mathscr{E}}_p$ Lemma 33 asserts the following: if $\alpha, \beta \in \mathscr{A}_p$ then $e_\alpha e_\beta = \lambda_{\alpha\beta\gamma} e_\gamma$, where $\gamma \in \mathscr{A}_p$ and $\lambda_{\alpha\beta\gamma} \in \Lambda$. We observe also that the same proof shows the following: let $e \in \mathscr{E}$ be such that $ee^* \in \Lambda$, then $e = \lambda e'$ where $e' \in \mathscr{E}(r',d')$ with $(r',d') = 1$, and $\lambda \in \Lambda$.

THEOREM 13. *Let* $l > k$, $(p,d) = (p,d') = 1$. *Then*

$$E_A(p^l,d) \otimes E_A(p^k,d') \cong I_{p^k} \otimes E(p^l,d''),$$

where $d'' = p^{l-k}d'+d$, *and* $E(p^l,d'') \in \mathscr{E}(p^l,d'')$.

Proof. By Lemmas 27 and 33 we know that

$$E = E_A(p^l,d) \otimes E_A(p^k,d') \cong F \otimes E_A(p^n,d_0),$$

where $n \leqslant l$, and F is a direct sum of line-bundles. We first show that $n = l$. Suppose $n \leqslant l-1$, then operate by $E_A(p^k,-d') \otimes$, and we get

$$\Big(\sum L_i\Big) \otimes E_A(p^l,d) \cong F \otimes E_A(p^k,-d') \otimes E_A(p^n,d_0),$$

where the L_i are the line-bundles of order dividing p^k (Lemma 22). Now by Lemma 27 the direct summands in the expansion of the right-hand side all have dimension $\leqslant p^{l-1}$. This gives a contradiction, and so $n = l$ as asserted. Then comparing degrees we get $d'' = p^{l-k}d'+d$. It remains to show that we can choose $F = I_{p^k}$. But

$$\operatorname{End} E \cong \Big(\sum L_i\Big) \otimes \Big(\sum L_j'\Big) \cong \Big(\sum L_i\Big) \otimes \operatorname{End} F,$$

where the L_i, L_j' are the line-bundles of orders dividing p^l, p^k respectively. If $F = \sum_{t=1}^{p^k} \bar{L}_t$, then $\bar{L}_1 \otimes \bar{L}_t^*$ are direct summands of End F and so of End E (since one of the $L_i \cong 1$). Thus

$$\bar{L}_1 \otimes \bar{L}_t^* \cong L_i \otimes L_j' \quad \text{for some } i, j.$$

Hence $\bar{L}_1 \otimes \bar{L}_t^*$ is of order dividing p^l. But (Corollary to Theorem 7) this implies that
$$\bar{L}_1 \otimes E_A(p^l, d'') \cong \bar{L}_t \otimes E_A(p^l, d'').$$
Hence
$$F \otimes E_A(p^l, d'') \cong I_{p^k} \otimes \bar{L}_1 \otimes E_A(p^l, d'').$$
Since $\bar{L}_1 \otimes E_A(p^l, d'') \in \mathscr{E}(p^l, d'')$ this completes the proof.

The case $l = k$ is covered by the next result.

Let $\Delta(r)$ denote the subgroup of $\Delta(X)$ (equivalence classes of line-bundles over X) consisting of elements of order dividing r. Then we have

THEOREM 14. *Let $p^{l-k} = (p^l, d_1+d_2)$, $(d_1, p) = (d_2, p) = 1$. Then*
$$E_A(p^l, d_1) \otimes E_A(p^l, d_2) \cong I_{p^k} \otimes (\textstyle\sum L_i) \otimes E(p^k, d_3),$$
where the L_i are representatives for the cosets $\Delta(p^l)/\Delta(p^k)$, $d_3 = (d_1+d_2)/p^{l-k}$, and $E(p^k, d_3) \in \mathscr{E}(p^k, d_3)$.

Proof. Put $d' = d_3$, $d = -d_2$ in Theorem 13. Then $d'' = p^{l-k}d_3 - d_2 = d_1$ and $(p, d) = (p, d') = 1$. Now operate on the equation in Theorem 13 by $E_A(p^l, -d) \otimes$, and we get
$$\left(\sum_{s=1}^{p^{2l}} L_s'\right) \otimes E_A(p^k, d_3) \cong I_{p^k} \otimes E_A(p^l, d_2) \otimes E(p^l, d_1), \tag{9}$$
where the L_s' are the line-bundles of order dividing p^l. Now if $L_s' \otimes L_t'^*$ is of order dividing p^k, we get (Corollary to Theorem 7)
$$L_s' \otimes E_A(p^k, d_3) \cong L_t' \otimes E_A(p^k, d_3).$$
Hence the left-hand side of (9) can be written in the form
$$I_{p^{2k}} \otimes \sum_{i=1}^{p^{2(l-k)}} L_i \otimes E_A(p^k, d_3),$$
where the L_i are representatives of $\Delta(p^l)/\Delta(p^k)$. Hence, equating direct summands in (10), we get
$$E_A(p^l, d_2) \otimes E(p^l, d_1) \cong I_{p^k} \otimes (\textstyle\sum L_i) \otimes E_A(p^k, d_3). \tag{10}$$
Since $E(p^l, d_1) \cong L \otimes E_A(p^l, d_1)$ for some line-bundle L of degree zero (Lemma 26), (10) can be rewritten as
$$E_A(p^l, d_1) \otimes E_A(p^l, d_1) \cong I_{p^k} \otimes (\textstyle\sum L_i) \otimes L^* \otimes E_A(p^k, d_3);$$
since $L^* \otimes E_A(p^k, d_3) \in \mathscr{E}(p^k, d_3)$ the lemma is proved.

Theorems 13 and 14 give almost the complete structure of the ring $\hat{\mathscr{E}}_p$. The only point left is to identify the particular element of $\mathscr{E}(p^l, d'')$ occurring in Theorem 13. Since we deduced Theorem 14 from Theorem 13 the corresponding ambiguity in Theorem 14 would then disappear also. The obvious conjecture is that this particular element is in fact the basic element $E_A(p^l, d'')$. If $p \neq 2$ this can be proved as follows. We regard X as an abelian variety with A as zero. Let $\rho: X \to X$ be the automorphism of period two given by $\rho(x) = -x$. ρ induces an automorphism of the ring $\hat{\mathscr{E}}$, which we denote by $\rho^\#$. Since A is a fixed point of ρ, we have

$$\rho^\#[e_A(r,d)] = e_A(r,d).$$

Now, in the situation of Theorem 13, suppose $E(p^l, d'') \cong L \otimes E_A(p^l, d'')$. Then applying $\rho^\#$ to the equation of Theorem 13 we see that

$$\rho^\#(L) \otimes E_A(p^l, d'') \cong L \otimes E_A(p^l, d'').$$

Hence $\rho^\#(L) \otimes L^*$ is of order dividing p^l (Corollary 1 to Lemma 24). Hence $\rho^\#(L^{p^l}) \cong L^{p^l}$. But the only line-bundles of degree zero invariant under $\rho^\#$ are those of order dividing 2. Hence L is of order dividing $2p^l$. On the other hand, taking determinants in the equation of Theorem 13 we see at once that L is of order dividing p^{l+k}. If $p \neq 2$ these two conditions together imply that L is of order dividing p^l, and so $L \otimes E_A(p^l, d'') \cong E_A(p^l, d'')$. We may therefore improve Theorems 13 and 14 as follows:

THEOREM 13′. *If $p \neq 2$ the bundle $E(p^l, d'')$ occurring in Theorem* 13 *may be replaced by $E_A(p^l, d'')$.*

THEOREM 14′. *If $p \neq 2$ the bundle $E(p^k, d_3)$ occurring in Theorem* 14 *may be replaced by $E_A(p^k, d_3)$.*

The same results presumably hold for $p = 2$, but a different proof would be needed.

SOME APPLICATIONS

1. Effect of homomorphisms on $\hat{\mathscr{E}}$

Let $N\colon X \to X$ be the homomorphism of X onto itself (regarded as an abelian variety with A as zero) defined by $N(x) = nx$, n a positive integer. Then N induces a ring homomorphism $N^\#\colon \hat{\mathscr{E}}(X) \leftarrow \hat{\mathscr{E}}(X)$. The main properties of $N^\#$ are given by the following theorem.

THEOREM 15. (i) $N^\# f_r = f_r$;

(ii) *if $(r,d) = 1$, then there exists an integer n such that $N^\# e_A(r,d)$ decomposes completely, i.e. $N^\# e_A(r,d) \in \Lambda$.*

Proof. (i) Clearly $N^\# 1 = 1$. Also the homomorphism

$$H^1(X, \mathbf{1}) \leftarrow H^1(X, \mathbf{1})$$

induced by N is an isomorphism. In fact it is easy to show in general that this homomorphism is simply multiplication by $\deg(N)$; if the characteristic is zero (or more generally prime to N) it follows at once that

$$H^1(X, \mathbf{1}) \leftarrow H^1(X, \mathbf{1})$$

is an isomorphism. But F_2 is defined by a non-trivial extension:

$$0 \to 1 \to F_2 \to 1 \to 0.$$

Hence by the remark we have just made the extension induced by N from this one will also be non-trivial. Hence $N^\sharp(f_2) = f_2$. If S^r denotes, as in Part III, § 1, the rth symmetric product, we have $N^\sharp S^r = S^r N^\sharp$. But, by Theorem 9, $f_r = S^{r-1}(f_2)$. Hence $N^\sharp f_r = f_r$.

(ii) Let $e \in \mathscr{E}(r,d)$, $(r,d) = 1$, $r > 1$. Then $ee^* \in \Lambda$, and so

$$(N^\sharp e)(N^\sharp e)^* = N^\sharp(ee^*) \in \Lambda.$$

Hence, applying the remark following Lemma 33, we find $N^\sharp e = \lambda e'$, where $e' \in \mathscr{E}(r',d')$, $(r',d') = 1$. We take $n = r$, $N = R$, and suppose if possible that $R^\sharp e$ is indecomposable, i.e. $r' = r$. Then, equating degrees we find

$$r^2 d = r \deg \lambda + d',$$

which contradicts $(r',d') = 1$. Hence $r' < r$. If $r' > 1$ we repeat the process, replacing e by e', and so on. After a finite number of steps the process must terminate. Putting $n = ...r'r$, $N = ...R'R$ we get $N^\sharp e \in \Lambda$.

Theorem 15 (ii) is interesting because of the following fact. Let $f\colon Y \to X$ be a regular map of a complex manifold Y onto a complex manifold X such that

(i) X is an analytic quotient space of Y, i.e. if U is open in X, a function g in U is regular if and only if $g \circ f$ is regular in $f^{-1}(U)$,

(ii) for each $x \in X$, $f^{-1}(x)$ is compact and connected.

Then it is easily shown (cf. (6)) that a vector bundle E over X is indecomposable if and only if $f^{-1}(E)$ is indecomposable. Theorem 15 (ii) shows that the condition that $f^{-1}(x)$ be connected is essential.

2. Coverings

By the results of Weil (10) we know (in the classical case) that a vector bundle over a curve X arises from a representation of the fundamental group if and only if all its indecomposable summands are of degree zero. Moreover the corresponding covering is finite (i.e. algebraic) if and only if the vector bundle corresponds to an algebraic element of the ring $\hat{\mathscr{E}}(X)$, i.e. an element satisfying a polynomial equation with integer coefficients. When X is elliptic we see at once from our explicit determination of the ring structure that the only algebraic elements of $\hat{\mathscr{E}}_0$ are of dimension one, i.e. correspond to line-bundles. This is as it should be, since every covering of X is known to be a homomorphism (X being regarded as an abelian variety) and so corresponds to a divisor class (or line-bundle).

In the case of characteristic p the situation is different. In fact, let X be an elliptic curve and let $p = 2$. Then $f_2^2 = 2f_2$, so that f_2 is an algebraic element of $\hat{\mathscr{E}}$. It is easy to show that F_2 corresponds to a covering of order 2 if and only if the Hasse invariant of X is non-zero. This suggests that the ring structure of $\hat{\mathscr{E}}(X)$ is not in itself sufficient to determine the algebraic coverings of X. Presumably the Frobenius homomorphism $x \to x^p$ must also be taken into consideration.

3. The symmetric product

Let X be an algebraic curve of genus g (any characteristic). Then if $n > 2g-2$ the symmetric product $S^n(X)$ is well known to be a projective bundle over the Picard variety of X, with fibre a projective space of dimension $n-g$. If X is elliptic then it may be identified with its own Picard variety. Hence, for $n \geqslant 1$, $S^n(X)$ is a projective bundle over X with fibre a projective space of dimension $n-1$. Since we have explicitly determined all such projective bundles (Theorem 11), it is natural to try to identify $S^n(X)$. It turns out (we omit the details) that $S^n(X)$ *is the indecomposable projective bundle corresponding to the integer* $(n-1)$, i.e. it arises from a vector bundle in $\mathscr{E}(n, n-1)$. Slightly more can be proved. Let B be a fixed divisor of degree $(n-1)$, $P \in X$, and consider the vector space $\mathscr{L}(B+P)$ of all rational functions ϕ on X with $\operatorname{div} \phi \geqslant -(B+P)$. Then we can, in a canonical manner, construct a vector bundle E over X whose fibre at P is $\mathscr{L}(B+P)$. $S^n(X)$ is then the projective bundle associated to E. The fixed vector space $\mathscr{L}(B)$ defines a trivial sub-bundle I_{n-1} of E, and we have an exact sequence:

$$0 \to I_{n-1} \to E \to [B] \to 0.$$

It can be shown that this extension is I_{n-1}-complete, and this therefore exhibits E as the indecomposable bundle with $\det E = [B]$ (unique up to isomorphism).

This result raises the question of whether $S^n(X)$ is indecomposable for every curve X (and more generally whether the corresponding construct for any algebraic variety X is indecomposable).

4. The sheaf $\mathbf{O}^{1/p}$

In the case of characteristic p we may consider the sheaf $\mathbf{O}^{1/p}$ where $\mathbf{O}$ is the sheaf of local rings. As a sheaf of $\mathbf{O}$-modules this is locally free, and of rank p (if X is a curve). Thus $\mathbf{O}^{1/p}$ defines a vector bundle E over X. In the case of an elliptic curve one can show the following:

(i) if the Hasse invariant of X is non-zero, then there exist just p line-bundles L_i of order dividing p, and $E \cong \sum_{i=1}^{p} L_i$;

(ii) if the Hasse invariant of X is zero, then

$$E \cong F_p.$$

Thus in case (i) E decomposes completely, while in (ii) E is indecomposable.

REFERENCES

1. M. F. Atiyah, 'Complex fibre bundles and ruled surfaces', *Proc. London Math. Soc.* (3) 5 (1955) 407–34.
2. —— 'Complex analytic connections in fibre bundles', *Trans. Amer. Math. Soc.* 84 (1957), 181–207.
3. —— 'On the Krull–Schmidt theorem with application to sheaves', *Bull. Soc. Math. France*, 84 (1956) 307–17.
4. J. Frenkel, 'Cohomologie à valeurs dans un faisceau non abelien', *C.R. Acad. Sci.* (Paris) 240 (1955) 2368–70.
5. A. Grothendieck, *A general theory of fibre spaces with structure sheaf* (Lawrence, Kansas, 1955).
6. —— 'Sur la classification des fibres holomorphes sur la sphère de Riemann', *Amer. J. Math.* 79 (1957) 121–38.
7. K. Kodaira, 'On a differential-geometric method in the theory of analytic stacks', *Proc. Nat. Acad. Sci.* (U.S.A.) 39 (1953) 1268–78.
8. —— 'Characteristic linear systems of complete continuous systems', *Amer. J. Math.* 78 (1956) 716–44.
9. J.-P. Serre, 'Géométrie algébrique et géométrie analytique', *Ann. Inst. Fourier* (1956) 1–42.
10. A. Weil, 'Generalisation des fonctions abeliennes', *J. Math. pur. appl.* 17 (1938) 47–87.

The Institute for Advanced Study,
Princeton, N.J.