III

ALGEBRAIC THEORY VIA SCHEMES

10. The theorem of the Cube (II). In this chapter, we shall always mean by a scheme a scheme of finite type over an algebraically closed field k, and a point will always mean a closed point of the scheme.

We begin with the following seemingly innocuous generalization of Corollary 6 to the semicontinuity theorem.

PROPOSITION. *Let X be a complete variety, Y any scheme and L a line bundle on $X \times Y$. Then there exists a unique closed subscheme $Y_1 \hookrightarrow Y$ having the following properties:*

(a) *if L_1 is the restriction of L to $X \times Y_1$, there is a line bundle M_1 on Y_1 and an isomorphism $p_2^* M_1 \cong L_1$ on $X \times Y_1$;*

(b) *if $f : Z \to Y$ is any morphism such that there exists a line bundle K on Z and an isomorphism $p_2^*(K) \cong (1_X \times f)^*(L)$ on $X \times Z$, f can be factored as $Z \to Y_1 \hookrightarrow Y$.*

PROOF. The uniqueness is immediate, since if $Y_1 \hookrightarrow Y$ and $Y_1' \hookrightarrow Y$ are two closed subschemes of Y satisfying (a) and (b), each of these closed immersions can be factored through the other, and they must coincide.

Note next that if $p_2^* M_1 \cong L_1$, then $\underline{M}_1 \cong p_{2,*}(\underline{L}_1)$ (by the Künneth formula), hence to show that there is a line bundle M_1 such that $p_2^* M_1 \cong L_1$, it is equivalent to showing that $p_{2,*}(\underline{L}_1) = \mathfrak{M}_1$ is an invertible sheaf and the natural homomorphism $p_2^*(\mathfrak{M}_1) \to \underline{L}_1$ is an isomorphism.

In view of this, we are reduced to proving that there is an open covering $\{V_i\}$ of Y such that the proposition holds for $X \times V_i \to V_i$ and the restriction of L to $X \times V_i$. In fact, if we have done this, we obtain a closed subscheme $W_i \hookrightarrow V_i$ such that (a) and (b) are valid with Y replaced by V_i. Then clearly $W_i \cap (V_i \cap V_j)$ and $W_j \cap (V_i \cap V_j)$ are two closed subschemes of $V_i \cap V_j$ such that (a) and (b) hold with Y replaced by $V_i \cap V_j$, hence they are equal. Thus we obtain a closed subscheme Y_1 of Y such that $Y_1 \cap V_i = W_i$,

and (a) (because of our local reformulation) is clearly valid. As for (b), the local version of (b) implies that for each i, $f^{-1}(V_i) \to V_i$ factorizes through W_i hence $f^{-1}(V_i) \to Y$ factorizes through Y_1, and so $Z \xrightarrow{f} Y$ factorizes through Y_1.

Thus we may assume $Y = \operatorname{Spec} A$, and it suffices to find an open neighborhood of each point of Y in which the proposition is valid. By shrinking Y if necessary, we may assume that we have a free complex $0 \to A^{r_0} \xrightarrow{\phi} A^{r_1} \to \dots$ giving the direct images of L universally, as in §5. Let M be the cokernel of the transpose ${}^t\phi$ of $\phi: A^{r_1} \xrightarrow{{}^t\phi} A^{r_0} \to M \to 0$. Then for any A-algebra B, $B^{r_1} \xrightarrow{{}^t\phi_B} B^{r_0} \to M \otimes_A B \to 0$ is exact, and hence so is $0 \to \operatorname{Hom}_B(M \otimes_A B, B) \to B^{r_0} \xrightarrow{\phi_B} B^{r_1}$. This shows that for all $f: \operatorname{Spec} B \to \operatorname{Spec} A = Y$, $p_{2,*}((1_X \times f)^*(\underline{L})) \simeq \operatorname{Hom}_A(M, B)$. Now let F be the set of points $y \in Y$ such that the restriction $L_y = L \mid X \times \{y\}$ is trivial, so that F is a closed subset of Y by our earlier result (applied to Y_{red} and the restriction of L to $X \times Y_{\text{red}}$). If $Y' = Y - F$, the empty subscheme $Y_1 = \emptyset$ of Y' satisfies (a) and (b) with respect to Y'. Hence, it suffices to show that for any $y \in F$, y has an open neighborhood in which the proposition holds. If $y \in F$, $1 = \dim H^0(X \times \{y\}, \underline{L}_y) = \dim \operatorname{Hom}_A(M, A/\mathfrak{M}_y) = \dim_k \frac{M}{\mathfrak{M}_y M}$, so that by Nakayama's lemma, there is an element of M which generates M in an open neighborhood of y. Restricting ourselves to this neighborhood we may assume that $M \simeq A/\mathfrak{A}$, where $\mathfrak{A}$ is an ideal of A. Let Y_1' be the closed subscheme defined by $\mathfrak{A}$, L_1' the restriction of L to $X \times Y_1'$ and $\underline{L}_1'$ the associated sheaf. Then $p_{2,*}(\underline{L}_1')$ is the sheaf associated to $\operatorname{Hom}_A(A/\mathfrak{A}, A/\mathfrak{A}) \simeq A/\mathfrak{A}$ on Y_1', and is hence free of rank one. Consider the natural homomorphism $p_2^*(p_{2,*}(\underline{L}_1')) \xrightarrow{\lambda} L_1'$ on $X \times Y_1'$. Since both sides are locally free of rank one, this is an isomorphism, at a point $z \in X \times Y_1'$ if and only if the induced homomorphism of 'fibers'

$$[p_2^*(p_{2,*}(\underline{L}_1'))_z] \otimes_{\mathcal{O}_z} k \to [\underline{L}_{1z}'] \otimes_{\mathcal{O}_z} k$$

is surjective. Now, since $\operatorname{Hom}_A(A/\mathfrak{A}, A/\mathfrak{A}) \to \operatorname{Hom}_A(A/\mathfrak{A}, A/\mathfrak{M}_y) = H^0(X \times \{y\}, L|X \times \{y\})$ is surjective and $L|X \times \{y\}$ is trivial, λ is an isomorphism at all points of $X \times \{y\}$. On the other hand, the set Z of points on $X \times Y_1'$ where λ is not an isomorphism, being the union of the supports of $\ker \lambda$ and $\operatorname{coker} \lambda$, is closed and does not meet $X \times \{y\}$. Hence its projection into Y is a closed subset not containing y. By restricting ourselves to an affine open neighborhood of y not meeting this projection, we may assume that $M \simeq A/\mathfrak{A}$, and that if Y_1 is the closed subscheme defined by $\mathfrak{A}$, condition (a) is fulfilled on Y_1. We claim that (b) follows. In fact, since the condition that $f: Z \to Y$ factorize through Y_1 is local on Z, we may assume $Z = \operatorname{Spec} B$ affine, and B becomes an A-algebra via f. Further, we may assume K trivial on Z, so that $(1_X \times f)^*(\underline{L}) \simeq \mathcal{O}_{X \times Z}$ and $p_{2,*}(1_X \times f)^*(\underline{L}) \simeq p_{2,*}(\mathcal{O}_{X \times Z}) \simeq \mathcal{O}_Z$ (since X is a complete variety). Hence we have an isomorphism of B-modules $B \simeq \operatorname{Hom}_A(A/\mathfrak{A}, B)$, so that $\mathfrak{A}.B = 0$ and $A \to B$ factors through $A/\mathfrak{A}$. Thus f factors through Y_1, proving the proposition.

Under the assumptions of the proposition, we shall refer to the closed subscheme Y_1 of Y given by the proposition as the maximal closed subscheme of Y over which L is trivial.

We get the following strengthened version and direct proof of the theorem of the cube.

THEOREM. *Let X and Y be complete varieties, Z a connected scheme, and L a line bundle on $X \times Y \times Z$ whose restrictions to $\{x_0\} \times Y \times Z$, $X \times \{y_0\} \times Z$ and $X \times Y \times \{z_0\}$ are trivial for some $x_0 \in X, y_0 \in Y$, and $z_0 \in Z$. Then L is trivial.*

PROOF. Let Z' be the maximal closed subscheme of Z over which L is trivial, so that $Z' \neq \emptyset$ since $z_0 \in Z'$. We have to show that $Z' = Z$, and since Z is connected, it suffices to show that if a point belongs to Z', Z' contains an open neighborhood (considered as an open subscheme of Z) of that point. Let us denote this point again by z_0, by $\mathfrak{M}$ the maximal ideal of $\mathcal{O}_{Z,z_0}$ and by $I = I_{z_0}$ the

ideal defining Z' at z_0, so that $I \subset \mathfrak{M}$. We have to show that $I=(0)$. If not, since $\bigcap_{n>0} \mathfrak{M}^n = (0)$ by Krull's Theorem, we can find an integer $n > 0$ such that $\mathfrak{M}^n \supset I$, $\mathfrak{M}^{n+1} \not\supset I$, so that

$$[\mathfrak{M}^{n+1} + I/\mathfrak{M}^{n+1}] \subset [\mathfrak{M}^n/\mathfrak{M}^{n+1}]$$

is a non-zero k-vector space. Hence, if $\mathfrak{A}_1 = \mathfrak{M}^{n+1} + I$, we can find an ideal $\mathfrak{A}_2$ with $\mathfrak{A}_1 \supset \mathfrak{A}_2 \supset \mathfrak{M}^{n+1}$ and $\dim_k \frac{\mathfrak{A}_1}{\mathfrak{A}_2} = 1$. Hence $\mathfrak{A}_1 = \mathfrak{A}_2 + k.a$ for some $a \in \mathfrak{A}_1$ and $\mathfrak{A}_1 \supset I$ but $\mathfrak{A}_2 \not\supset I$. Let $\mathfrak{A}_0 = \mathfrak{M}$. Let z_i be the closed subschemes of Z consisting of the single point z_0, with structure sheaf $\mathcal{O}_{Z,z_0}/\mathfrak{A}_i$, so that:

$$\begin{array}{ccccc} & & Z' & & \\ & \cup & & \subset & \\ \{z_0\} = Z_0 & \subset & Z_1 & \subset & Z \\ & \cap & & \cup & \\ & & Z_2 & & \end{array}$$

Let $\underline{L}_i$ $(i=0,1,2)$ be the restriction to $X \times Y \times Z_i$ of the sheaf $\underline{L}$ of sections of L. Note that $\underline{L}_0, \underline{L}_1$ are trivial on $X \times Y \times Z_0$, $X \times Y \times Z_1$ respectively, since $Z_0, Z_1 \subset Z'$, so that we have isomorphisms $\underline{L}_i \simeq \mathcal{O}_{X \times Y \times Z_i}$ $(i=0,1)$. Further, since the structure sheaves of Z_0, Z_1 and Z_2 are related by the exact sequence

$$0 \longrightarrow \mathcal{O}_{Z_0} \xrightarrow{\text{mult. by } a} \mathcal{O}_{Z_2} \xrightarrow{\text{restr.}} \mathcal{O}_{Z_1} \longrightarrow 0,$$

we also have an exact sequence of sheaves on the topological space Z_0:

$$0 \longrightarrow \underline{L}_0 \xrightarrow{\text{mult. by } a} \underline{L}_2 \xrightarrow{\text{restr.}} \underline{L}_1 \longrightarrow 0.$$

Consider the section $s \in \Gamma(X \times Y \times Z_1, \underline{L}_1)$ equal to $\lambda(1)$ under the isomorphism λ: $\mathcal{O}_{X \times Y \times Z_1} \xrightarrow{\approx} \underline{L}_1$. The necessary and sufficient

condition that $\underline{L}_2$ be trivial is that s can be lifted to a section s' of $\underline{L}_2$. In fact, if we can do this, multiplication by s' is a homomorphism λ': $\mathcal{O}_{X \times Y \times Z_1} \to \underline{L}_2$ which reduced modulo the maximal ideal of any point ζ of $X \times Y \times \{z_0\}$ is an isomorphism $k \xrightarrow{\sim} \underline{L}_2 \otimes_{\mathcal{O}_\zeta} k$, hence λ' is an isomorphism (the sheaves being locally free). Conversely, if $\underline{L}_2$ is trivial, using the induced trivialization of $\underline{L}_1$, the map $\Gamma(\underline{L}_2) \to \Gamma(\underline{L}_1)$ becomes the map $\Gamma(\mathcal{O}_{Z_2}) \to \Gamma(\mathcal{O}_{Z_1})$, which is surjective. Now, fix an isomorphism $\underline{L}_0 \simeq \mathcal{O}_{X \times Y}$. The obstruction to lifting s to $\Gamma(\underline{L}_2)$ is then an element $\xi \in H^1(X \times Y, \mathcal{O}_{X \times Y})$. Since the restrictions of L to $X \times \{y_0\} \times Z$ and $\{x_0\} \times Y \times Z$, hence also to $X \times \{y_0\} \times Z_2$ and $\{x_0\} \times Y \times Z_2$, are trivial, the restrictions of s to $X \times \{y_0\} \times Z_1$ and $\{x_0\} \times Y \times Z_1$ can be lifted to $L \mid X \times \{y_0\} \times Z_2$ and $L \mid \{x_0\} \times Y \times Z_2$ respectively. This means that the image of ξ by the maps $H^1(X \times Y, \mathcal{O}_{X \times Y}) \to H^1(X, \mathcal{O}_X)$ and $H^1(X \times Y, \mathcal{O}_{X \times Y}) \to H^1(Y, \mathcal{O}_Y)$ induced by $x \longmapsto (x, y_0)$ and $y \longmapsto (x_0, y)$ are zero. But by the Künneth formula, these maps induce an isomorphism $H^1(X \times Y, \mathcal{O}_{X \times Y}) \simeq H^1(X, \mathcal{O}_X) \oplus H^1(Y, \mathcal{O}_Y)$. Therefore $\xi = 0$, and s can be lifted to $X \times Y \times Z_2$, and $\underline{L}_2$ is trivial. This is a contradiction, so Z' contains an open neighborhood of z_0.

11. **Basic Theory of Group Schemes.** We continue to work over a fixed algebraically closed field k, with schemes always of finite type over k, and with closed points only. $\underline{\text{Sch}}$ will denote the category of schemes of finite type over k.

One of the most basic tools in the theory of schemes is the concept of *S-valued points*: if X and S are schemes, an S-valued point of X is a morphism from S to X. The set of all such is denoted

$$\text{Hom}_k(S, X) \text{ or } \underline{X}(S).$$

If X is fixed, the map $S \longmapsto \underline{X}(S)$ is a contravariant functor:

$$\underline{X}\colon \underline{\text{Sch}}^0 \longrightarrow \underline{\text{Sets}}.$$

The importance of this functor is this: if X and Y are two schemes, then (a) a morphism $f\colon X \to Y$ defines a morphism from the functor

$\underline{X}$ to the functor $\underline{Y}$ (i.e. a map $\underline{X}(S) \xrightarrow{f(S)} \underline{Y}(S)$ for every S such that for every $g: S \to T$, the diagram

$$\begin{array}{ccc} \underline{X}(S) & \longleftarrow & \underline{X}(T) \\ {\scriptstyle f(S)}\downarrow & & \downarrow{\scriptstyle f(T)} \\ \underline{Y}(S) & \longleftarrow & \underline{Y}(T) \end{array}$$

commutes), and (b) conversely, a morphism from the functor $\underline{X}$ to the functor $\underline{Y}$ is defined by a unique morphism of schemes $f: X \to Y$. (a) and (b) are really tautologies holding for any category: the reader should prove them for himself if he has not seen them. This remark will turn out to be an excellent tool for constructing morphisms as we will see. Formally, (a) and (b) say that

$$X \longmapsto \underline{X}$$

is itself a fully faithful functor from the category $\underline{\text{Sch}}$ to the category Fun ($\underline{\text{Sch}}^0$, $\underline{\text{Sets}}$) of all contravariant functors from $\underline{\text{Sch}}$ to $\underline{\text{Sets}}$, hence $\underline{\text{Sch}}$ is equivalent to a full subcategory of Fun ($\underline{\text{Sch}}^0$, $\underline{\text{Sets}}$). Cf. Mumford [M 3], Ch. 2.

If $\underline{\text{Alg}}$ denotes the category of k-algebras of finite type, and $R \in \text{Obj } \underline{\text{Alg}}$, let us put $\underline{X}(R) = \underline{X}(\text{Spec } R)$. Then $\underline{X}$ defines a covariant functor from $\underline{\text{Alg}}$ to $\underline{\text{Sets}}$, which functor again we denote by the same symbol $\underline{X}$. The elements of $\underline{X}(R)$ are also referred to as R-valued points of X. If $\mathscr{C} = \text{Fun } (\underline{\text{Alg}}, \underline{\text{Sets}})$, it is once again an easy matter to show that $\text{Hom}_{\underline{\text{Sch}}}(X, Y) \xrightarrow{\sim} \text{Hom}_{\mathscr{C}}(\underline{X}, \underline{Y})$ is bijective, so that $\underline{\text{Sch}}$ can be identified with a full subcategory of $\mathscr{C}$.

DEFINITION. *A group scheme is a scheme G together with* (a) *a multiplication morphism $m: G \times G \to G$,* (b) *an identity point, i.e. a morphism e: Spec $k \to G$, and* (c) *an inverse morphism $i: G \to G$, such that the following axioms hold.*

(1) *(Associativity). The diagram*

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{m \times 1_G} & G \times G \\ {\scriptstyle 1_G \times m}\downarrow & & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow{m} & G \end{array}$$

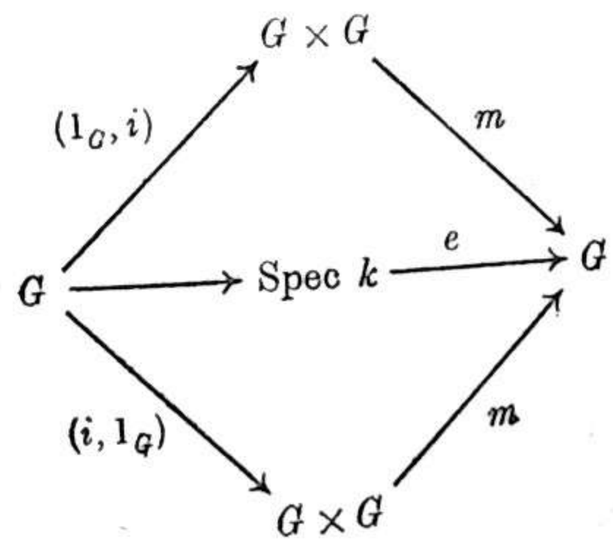
is commutative.

(2) *The diagram*

$$\begin{array}{ccc} G \times \text{Spec } k & \xrightarrow{1_G \times e} & G \times G \\ \wr\downarrow & & \downarrow{\scriptstyle m} \\ G & \xrightarrow{1_G} & G \\ \wr\downarrow & & \uparrow{\scriptstyle m} \\ \text{Spec } k \times G & \xrightarrow{e \times 1_G} & G \times G \end{array}$$

is commutative.

(3) *The diagram*



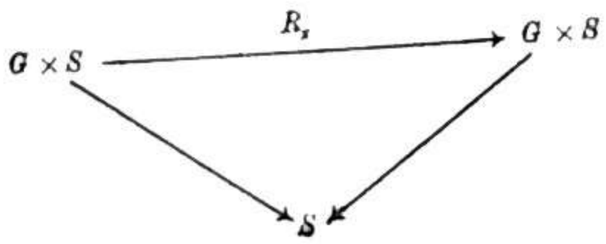
is commutative.

Now let G be a scheme, and let us interpret the conditions for giving a structure of group scheme to G in terms of the functor which it represents (either on $\underline{\mathrm{Sch}}$ or on $\underline{\mathrm{Alg}}$). In view of our earlier remarks and the fact that products in $\underline{\mathrm{Sch}}$ correspond to products of functors, m, i, and e can be interpreted respectively as maps $\underline{G}(S) \times \underline{G}(S) \to \underline{G}(S)$, $\underline{G}(S) \to \underline{G}(S)$, and as giving a distinguished element of $\underline{G}(S)$, functorially in S in the obvious sense. The conditions (1)-(3) then simply say that $\underline{G}(S)$ is a group for each S with m, i, and e defining the group law, inverse and identity element, and that for all morphisms $S' \to S$ of schemes, the induced map $\underline{G}(S) \to \underline{G}(S')$ is a group homomorphism. We thus see that to give a group scheme structure on a scheme G is *equivalent* to making the set of S-valued points of G into a group for every S, functorially in S. It would also be enough to make the set of R-valued points of G into a group, for every k-algebra R, functorially in R.

If x is an ordinary point of G, then the morphism

$$R_x\colon G \xrightarrow{\sim} G \times \{x\} \subset G \times G \xrightarrow{m} G$$

is an automorphism of G, called right-multiplication by x. More generally, if $x\colon S \to G$ is an S-valued point of G, x induces an automorphism R_x of $G \times S$ over S, which we can call right-multiplication by x. We use $m \circ (1_G \times x)\colon G \times S \to G$ and let $R_x = (m \circ (1_G \times x), p_2)$ so as to get a commutative diagram.



It is easy to check that with the group structure on $\underline{G}(S)$, we get $R_{x \cdot y} = R_y \circ R_x$. Interchanging the factors in $G \times G$, we can define left-multiplication L_x similarly.

Lie Algebras. Let X be a scheme, and Ω_X the sheaf of Kähler differentials on X over k. By a *vector field* on X we shall mean

a k-linear map of sheaves $D\colon \mathcal{O}_X \to \mathcal{O}_X$ such that the induced map $D\colon \mathcal{O}_X(U) \to \mathcal{O}_X(U)$ is a derivation over k, for every open set U. This is equivalent to saying that D factors:

$$\mathcal{O}_X \xrightarrow{d} \Omega_X \xrightarrow{f} \mathcal{O}_X\ ,$$

where f is an $\mathcal{O}_X$-linear homomorphism of sheaves.

By a tangent vector at $x \in X$, we mean a derivation $\mathcal{O}_{X,x} \to k$, or equivalently an element of $\mathrm{Hom}_{\mathcal{O}_{X,x}}(\Omega_{X,x}, k)$. Now, it is well known that if $\mathfrak{M}_x$ is the maximal ideal of $\mathcal{O}_{X,x}$ the natural map

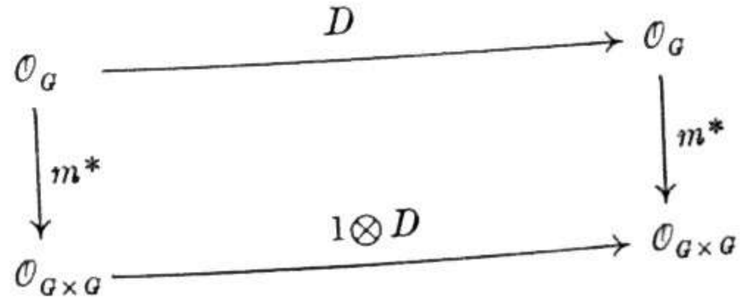
$$\frac{\mathfrak{M}_x}{\mathfrak{M}_x^2} \longrightarrow \Omega_{X,x} \otimes_{\mathcal{O}_{X,x}} k,$$

$$f \longmapsto df \otimes 1$$

is an isomorphism. Thus, a tangent vector is uniquely determined by giving a linear form on $\mathfrak{M}_x/\mathfrak{M}_x^2$. Clearly, a tangent field in a neighborhood of x determines a tangent vector at x (by composition of the derivation $\mathcal{O}_{X,x} \to \mathcal{O}_{X,x}$ and the evaluation map $\mathcal{O}_{X,x} \to k$), which we shall call the value of the vector field at x.

Let X and Y be two schemes, and D a vector field on X. If p_i $(i = 1,2)$ denotes the i^{th} projection of $X \times Y$, we have a canonical isomorphism $p_1^*(\Omega_X) \oplus p_2^*(\Omega_Y) \xrightarrow{\sim} \Omega_{X \times Y}$, so that there is a unique vector field $D \otimes 1$ on $X \times Y$ such that when factored through $\Omega_{X \times Y}$, $D \otimes 1$ agrees on $p_1^*(\Omega_X)$ with D and it is zero on $p_2^*(\Omega_Y)$, i.e., $D \otimes 1(f \otimes g) = Df \otimes g$.

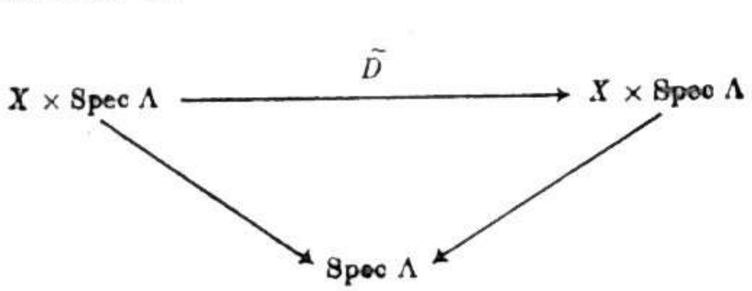
Now let G be a group scheme. A vector field D on G is said to be *left invariant* if the following diagram commutes:



the vertical maps being the natural ones induced by the multiplication morphism $G \times G \xrightarrow{m} G$.

PROPOSITION. *For any tangent vector t at e to G, there is a unique left invariant vector field on G having the value t at e.*

PROOF. First we interpret tangent vectors and vector fields in a slightly different way. Let Λ be the k-algebra $k[\epsilon]/(\epsilon^2)$ and η: $k[\epsilon]/(\epsilon^2) \to k$ the homomorphism with $\eta(\epsilon) = 0$. If A and B are k-algebras and B is an A-algebra, the k-derivations D of A in B are in one-one correspondence with algebra homomorphisms ϕ: $A \to \dfrac{B[\epsilon]}{(\epsilon^2)} \simeq B \otimes_k \Lambda$ such that $\phi(a) = a.1 +$ multiple of ϵ. This correspondence is given by $D \longleftrightarrow \phi$, $\phi(a) = a.1 + (Da).\epsilon$. Thus, we deduce that if X is a scheme and x a point of X, a tangent vector at x is a morphism $\operatorname{Spec} \Lambda \to X$ such that $\operatorname{Spec}(k) \hookrightarrow \operatorname{Spec} \Lambda \to X$ is the point x; and a vector field D on X is an automorphism over Λ:



which restricts to the identity 1_X: $X \to X$ when you look at the fibres over $\operatorname{Spec}(k) \hookrightarrow \operatorname{Spec}(\Lambda)$.

One then sees easily that a vector field D on a group scheme G is left invariant if and only if for the associated automorphism $\tilde{D}$, the diagram

$$\begin{array}{ccc} G \times G \times \operatorname{Spec} \Lambda & \xrightarrow{1_G \times \tilde{D}} & G \times G \times \operatorname{Spec} \Lambda \\ \downarrow{\scriptstyle m \times 1} & & \downarrow{\scriptstyle m \times 1} \\ G \times \operatorname{Spec} \Lambda & \xrightarrow{\tilde{D}} & G \times \operatorname{Spec} \Lambda \end{array} \qquad (*)$$

is commutative. If $D' = p_1 \circ \tilde{D}$: $G \times \operatorname{Spec} \Lambda \to G$, then in terms of S-valued points x, y of G and l of $\operatorname{Spec} \Lambda$, this diagram says:

$$D'(x.y, l) = x.D'(y, l).$$

This clearly holds if and only if $D'(x,l) = x.D'(e,l)$ for all x and l. In other words, if $\tilde{t}$ equals $p_1 \circ \tilde{D} \circ (e,1)$: $\operatorname{Spec} \Lambda \to G$ then we want $\tilde{D}$ to be right-multiplication by the Λ-valued point $\tilde{t}$ of G. Therefore given any Λ-valued point $\tilde{t}$ of G, we get a unique automorphism $\tilde{D}$ of $G \times \operatorname{Spec}(\Lambda)$ such that (*) commutes and $p_1 \circ \tilde{D} \circ (e,1) = \tilde{t}$. But this means exactly that D is left invariant and has value t at e.

Thus we get a canonical isomorphism of the k-vector space of left invariant vector fields on G and the tangent space at e to G. Now, given any two vector fields D_1, D_2 on a scheme X, considering them as endomorphisms of $\mathcal{O}_X$, we see that $D = [D_1, D_2] = D_1 D_2 - D_2 D_1$ is again a vector field on X, called the *Poisson bracket* of D_1 and D_2. Furthermore, if $\operatorname{char} k = p > 0$, D_1^p is again a vector field. If G is a group scheme, one verifies trivially that the Poisson bracket and p^{th} power operation take left invariant vector fields to left invariant vector fields.

DEFINITION. *The Lie algebra of a group scheme is the k-vector space of left invariant vector fields, together with the operation of Poisson bracket defined on it, as well as the p^{th} power operation if* $\operatorname{char} k = p > 0$.

We shall agree to denote the Lie algebra of G, H, G_1, ... etc. by $\mathfrak{g}$, $\mathfrak{h}$, $\mathfrak{g}_1$, ... etc. We have then:

(1) The map $\mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$, $(X, Y) \longmapsto [X, Y]$, is bilinear over k and the map $X \longmapsto X^p$ satisfies $(\lambda X)^p = \lambda^p X^p$.

(2) For $X \in \mathfrak{g}$, $[X, X] = 0$.

(3) For X, Y and $Z \in \mathfrak{g}$, we have
$$[X, [Y, Z]] + [Y, [Z, X]] + [Z, [X, Y]] = 0.$$

(4) If $\operatorname{char} k = p > 0$, there is a certain universal non-commutative polynomial F_p (depending only on p) in two variables such that

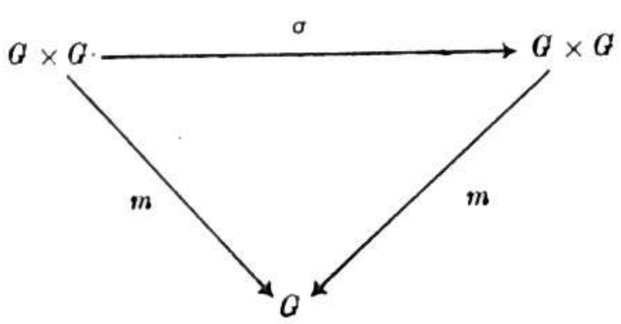
$$\text{ad}\,(X^p) = (\text{ad}\,X)^p,$$

$$(X+Y)^p = X^p + Y^p + F_p(\text{ad}\,X, \text{ad}\,Y)\,Y,$$

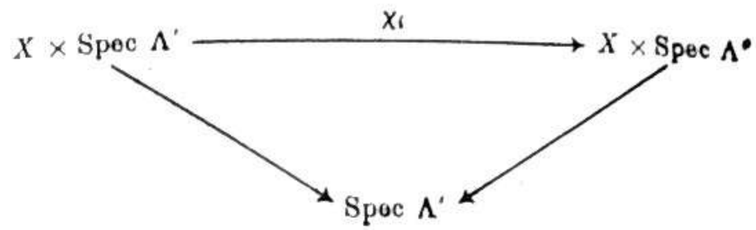
where ad X is the endomorphism of $\mathfrak{g}$ defined by $\text{ad}\,X(Y) = [X, Y]$.

For the actual expression of F_p, which is unimportant for our purposes, we refer to [J]. It is however uniquely determined by the condition that if A is an associative algebra over k and we define $[X, Y] = XY - YX$ and X^p to be the p^{th} power in A, A satisfies (4). Thus, F_p may be calculated by taking A to be a free associative algebra on two generators X and Y over k, and showing that $(X+Y)^p$ can be expanded as in (4) in A. Since we are mainly interested in the case when $\mathfrak{g}$ is "abelian", that is, when $[X, Y] = 0$ for $X, Y \in \mathfrak{g}$, it suffices for us to know that F_p has 'no constant term', that is, $F_p(0, 0) = 0$. Thus, in the abelian case, $X \to X^p$ is just a p-linear map (i.e. an additive homomorphism of $\mathfrak{g}$ into itself with $(\lambda X)^p = \lambda^p X^p$). In the case of the Lie algebra of an abelian variety, the p^{th} power map is called the Hasse-Witt map.

We remark that if G is commutative, that is, if the diagram



is commutative, where σ is the 'switch map' $\sigma = (p_2, p_1)$ then $\mathfrak{g}$ is abelian, that is, $[X, Y] = 0$ for all $X, Y \in \mathfrak{g}$. To prove this, we start with the following observation. Let D_i $(i = 1, 2)$ be vector fields on any scheme X, $D_3 = [D_2, D_1]$ and $\widetilde{D}_i$: $X \times \text{Spec}\,\Lambda \to X \times \text{Spec}\,\Lambda$ be the associated automorphisms, where $\Lambda = k[\epsilon]/(\epsilon^2)$. Put $\Lambda' = k[\epsilon, \epsilon']/(\epsilon^2, \epsilon'^2)$, and let $\sigma_i : \Lambda \to \Lambda'$ be the k-algebra homomorphisms defined by $\sigma_1(\epsilon) = \epsilon, \sigma_2(\epsilon) = \epsilon'$ and $\sigma_3(\epsilon) = \epsilon\epsilon'$. Then σ_i induces a morphism $\phi_i = \text{Spec}\,\sigma_i$: Spec $\Lambda' \to$ Spec Λ $(1 \leqslant i \leqslant 3)$, and we get automorphisms



by taking fibre products with Spec Λ' over Spec Λ via ϕ_i. One then checks easily (by taking X affine) that χ_3 is the commutator $[\chi_1, \chi_2] = \chi_1 \chi_2 \chi_1^{-1} \chi_2^{-1}$. Now suppose G is a group scheme, let t_i: Spec $\Lambda \to G$ $(i = 1, 2)$ tangent vectors at G, and let D_i be corresponding left invariant vector fields. Then $\widetilde{D}_i$ is just right-translation with respect to t_i, and if $t_i \circ \phi_i = T_i$: Spec $\Lambda' \to G$, then χ_i is right translation of $G \times$ Spec Λ' by the point $T_i \in \underline{G}(\Lambda')$. Hence $\chi_1 \chi_2 \chi_1^{-1} \chi_2^{-1}$ is right translation by $[T_1, T_2] \in \underline{G}(\Lambda')$. Since $\underline{G}(\Lambda')$ is a commutative group, it follows that $[T_1, T_2] = 0$, hence $\chi_1 \chi_2 \chi_1^{-1} \chi_2^{-1} = \chi_3 =$ Identity, and $[D_1, D_2] = 0$.

THEOREM. *Any group scheme over a field k of characteristic 0 is smooth (and in particular reduced).*

PROOF. We show in fact that if X is any scheme over k of characteristic zero and x a point of X such that there exist vector fields $D_1, \ldots, D_n$ in a neighborhood of x with $n = \dim_k \dfrac{\mathfrak{M}_x}{\mathfrak{M}_x^2}$ inducing independent tangent vectors at x, then X is smooth at x. We can choose x_i $(1 \leqslant i \leqslant n)$ in $\mathfrak{M}_x$ such that they form a basis modulo $\mathfrak{M}_x^2$ of $\mathfrak{M}_x/\mathfrak{M}_x^2$ and $(D_i\, x_j)(x) = \delta_{ij}$. Since clearly $D_i(\mathfrak{M}_x^p) \subset \mathfrak{M}_x^{p-1}$, D_i extend to derivations of the completion $\hat{\mathcal{O}}_x$ of $\mathcal{O}_x$. Now, we have a unique continuous k-homomorphism α: $k[[t_1, \ldots, t_n]] \to \hat{\mathcal{O}}_x$ with $\alpha(t_i) = x_i$. On the other hand, define β: $\hat{\mathcal{O}}_x \to k[[t_1, \ldots, t_n]]$ by putting

$$\beta(f) = \sum_{\substack{\nu = (\nu_1, \ldots, \nu_n) \\ \nu_i \geqslant 0}} \frac{D^\nu f}{\nu!}(x).t^\nu$$

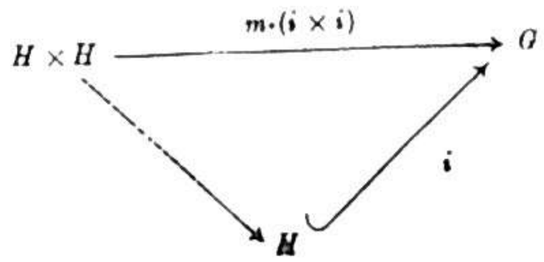
where $D^\nu f = D_1^{\nu_1} \ldots D_n^{\nu_n} f$, $\nu! = \nu_1! \ldots \nu_n!$ and $t^\nu = t_1^{\nu_1} \ldots t_n^{\nu_n}$. By Leibniz's formula and induction on n, one checks trivially that β is again a continuous k-homomorphism of local rings. Now,

α is surjective since its image contains a set of generators of $\mathfrak{M}_x$ and $k[[t_1, \dots, t_n]]$ is complete. On the other hand, $\beta(x_i) \equiv t_i \pmod{(t_1, \dots, t_n)^2}$ so that $\beta(x_i)$ generate the maximal ideal of $k[[t_1, \dots, t_n]]$, and β is also surjective. Hence so is $\beta \circ \alpha$, so that $\beta \circ \alpha$ is an automorphism of $k[[t_1, \dots, t_n]]$. Hence α is also injective, hence an isomorphism. Hence $\hat{\mathcal{O}}_x$ and $\mathcal{O}_x$ are regular, and X is smooth at x.

In positive characteristic, we will soon have plenty of examples of non-reduced group schemes.

SUBGROUP SCHEMES, KERNELS, QUOTIENTS.

Let G be a group scheme, and H a closed subscheme. We say that H is a *subgroup scheme* if, denoting by $i: H \hookrightarrow G$ the closed immersion, $m \circ (i \times i): H \times H \to G$ factors through H:



This is equivalent to saying that for every $S \in \mathrm{Obj}\ \underline{\mathrm{Sch}}$, $\underline{H}(S)$ is a subgroup of $\underline{G}(S)$. Clearly H then becomes a group scheme in its own right, and $i: H \to G$ a homomorphism of group schemes (defined in an obvious way).

To any group scheme G over k of characteristic $p > 0$, one can associate in a natural way an increasing sequence G_n of closed subschemes ($n \geqslant 0$), all having support at the identity element of G, as follows. Let $\mathcal{O} = \mathcal{O}_e$ be the local ring at the identity to G, $\mathfrak{M}$ its maximal ideal, and $\mathfrak{M}^{(p^n)}$ the ideal generated by $\{x^{p^n} | x \in \mathfrak{M}\}$. Put $G_n = \mathrm{Spec}\,[\mathcal{O}/\mathfrak{M}^{(p^n)}]$, so that G_n is a closed subscheme of G with support at e. Let $\mathcal{O}' = \mathcal{O}_{(e,e),G\times G}$ be the local ring of (e,e) on $G \times G$, so that $\mathcal{O}'$ is the localization of $\mathcal{O} \otimes_k \mathcal{O}$ with respect to the maximal ideal $\mathfrak{M} \otimes \mathcal{O} + \mathcal{O} \otimes \mathfrak{M}$. The multiplication map m induces a local homomorphism of rings $m^*: \mathcal{O} \to \mathcal{O}'$, so that for $f \in \mathfrak{M}$, $m^*(f) = g/h$,

$g \in \mathfrak{M} \otimes \mathcal{O} + \mathcal{O} \otimes \mathfrak{M}$, h a unit in $\mathcal{O}'$; hence $m^*(f^{p^n}) \in [\mathfrak{M}^{(p^n)} \otimes \mathcal{O} + \mathcal{O} \otimes \mathfrak{M}^{(p^n)}]\cdot \mathcal{O}'$. This proves that the composite $G_n \times G_n \to G \times G \xrightarrow{m} G$ factorizes through the subscheme G_n, proving that G_n is a subgroup scheme. One has evidently $\mathrm{Lie}\,(G_n) = \mathrm{Lie}\,G$ for $n > 1$.

EXAMPLES. (1) In any characteristic, define $\mathbf{G}_a$, the additive group over k, as $\mathrm{Spec}\,k[T] = \mathbf{A}^1$, the group law $\mathbf{G}_a \times \mathbf{G}_a \to \mathbf{G}_a$ being defined by addition, or equivalently, by the homomorphism $m^*: k[T] \to k[T] \otimes k[T]$, $m^*(T) = T \otimes 1 + 1 \otimes T$. The group of S-valued points $\underline{\mathbf{G}}_a(S)$ is just the group $\Gamma(S, \mathcal{O}_S)$.

If $\mathrm{char}\ k = p > 0$, we also write α_{p^n} for the subgroup scheme $(\mathbf{G}_a)_n$, that is $\alpha_{p^n} = \mathrm{Spec}\left[\frac{k[T]}{(T^{p^n})}\right]$. We have $\mathrm{Lie}\,(\mathbf{G}_a) = \mathrm{Lie}\,(\alpha_{p^n}) = k.\partial/\partial T$, $n \geqslant 1$, and $\underline{\alpha}_{p^n}(S) = \{f \in \Gamma(S, \mathcal{O}_S) \,|\, f^{p^n} = 0\}$.

(2) In any characteristic, define $\mathbf{G}_m$ to be the multiplicative group over k, coinciding as a scheme with $\mathbf{A}^1 - \{0\}$, the group law being multiplication. Writing $\mathbf{G}_m = \mathrm{Spec}\,k[T, 1/T]$, the homomorphism $m^*: k[T, 1/T] \to k[T, 1/T] \otimes_k k[T, 1/T]$ is given by $m^*(T) = T \otimes T$. The group of S-valued points of $\mathbf{G}_m$ is the group of units $\Gamma(S, \mathcal{O}_S^*)$.

If characteristic $k = p > 0$ we shall put $\mu_{p^n} = (\mathbf{G}_m)_n = \mathrm{Spec}\ k[T, T^{-1}]/((T-1)^{p^n}) = \mathrm{Spec}\ k[T]/(T^{p^n} - 1)$. We have $\mathrm{Lie}\,\mathbf{G}_m = \mathrm{Lie}\,\mu_{p^n} = k.T\,\partial/\partial T$ ($n \geqslant 1$), and $\underline{\mu}_{p^n}(S) = \{f \in \Gamma(S, \mathcal{O}_S^*) \,|\, f^{p^n} = 1\}$.

Now, let G and H be group schemes and $f: G \to H$ a homomorphism of group schemes. The fiber $f^{-1}(e_H) = G \times_H \{e_H\}$ over the closed point e_H of H which is the identity element of H is a closed subscheme K of G. By definition, for any S-valued point of G, $\phi: S \to G$, ϕ factorizes through K if and only if $f \circ \phi$ factorizes through $e_H: \mathrm{Spec}\,k \to H$, or in other words, $\underline{K}(S)$ is the kernel of $\underline{G}(S) \to \underline{H}(S)$. Therefore K is a subgroup scheme of G.

As an example, consider the homomorphism $\mathbf{G}_m \to \mathbf{G}_m$ defined by $X \longmapsto X^n$. The kernel is denoted by μ_n. For $(n, p) = 1$, μ_n is just

a discrete group (i.e. reduced and finite group) isomorphic to the n^{th} roots of unity in k^*. On the other hand, it follows from definitions that μ_{p^n} is the same group defined earlier.

Next, suppose G and H are group schemes, and $\phi : H \to G$ a homomorphism. A pair $(G/H, \eta)$, where G/H is a scheme and $\eta : G \to G/H$ is a morphism, is said to be a *quotient* of G by H, if it is universal for all pairs (S,f) where S is a scheme, and $f : G \to S$ a morphism such that the following diagram commutes:

$$\begin{array}{ccc} H \times G & \xrightarrow{m \circ (\phi \times 1)} & G \\ \downarrow{\scriptstyle p_1} & & \downarrow \\ G & \xrightarrow{f} & S\,. \end{array}$$

It can be shown that quotients exist, that f is always flat and surjective, and further that when H is a normal subgroup scheme in G (i.e. $\underline{H}(S)$ is a normal subgroup of $\underline{G}(S)$ for all S), G/H inherits a unique structure of group scheme such that $\eta : G \to G/H$ is a homomorphism and has kernel precisely H. We will not need the result in this generality, but only in the special case when H is a finite group scheme. We will consider this in §12.

LEFT-INVARIANT DIFFERENTIAL OPERATORS.

We want to study the algebra of maps $\mathcal{O}_G \to \mathcal{O}_G$ generated by left-invariant derivations. We first introduce the *hyperalgebra* $\mathbf{H}$ of G :

$$\mathbf{H}_x = \mathrm{Hom}_{\mathrm{cont}}(\mathcal{O}_{x,G}, k)$$

$$\mathbf{H} = \bigoplus_{x \in G} \mathbf{H}_x$$

where $\mathrm{Hom}_{\mathrm{cont}}$ means the maps $L : \mathcal{O}_x \to k$ which are continuous in the sense that $L(\mathfrak{M}_x^{N+1}) = (0)$ for some N. Alternately,

$$\mathbf{H} = \varinjlim_{\substack{\text{0-dim-subschemes} \\ Z \subset G}} \Gamma(\mathcal{O}_Z)^*$$

where W^* means the k-vector space dual to a vector space W. If $L \in \mathbf{H}$ lies in the subspace $\Gamma(\mathcal{O}_Z)^*$, we will say that L is supported by Z. This definition makes it clear that $\mathbf{H}$ is an algebro-geometric analog of the space of distributions on a Lie group supported on a finite set. $\mathbf{H}$ has a lot of structure.

(1) We get an associative and distributive convolution product

$$* : \mathbf{H} \otimes \mathbf{H} \longrightarrow \mathbf{H}$$

by defining

$$(\S) \qquad L_1 * L_2(f) = L_1 \otimes L_2(m^* f).$$

More precisely, if L_i is supported by Z_i, $i = 1, 2$, and if $Z_3 \subset G$ is a finite subscheme such that the group law m factors :

$$\begin{array}{ccc} Z_1 \times Z_2 & \dashrightarrow & Z_3 \\ \cap & & \cap \\ G \times G & \xrightarrow{m} & G \end{array}$$

then $L_1 * L_2$ is to be supported by Z_3 and the equation (§) is to be interpreted with $f \in \Gamma(\mathcal{O}_{Z_3})$ and with m as the restriction of m to $Z_1 \times Z_2$.

(2) Evaluation at any point $x \in G$ is a continuous linear map $\delta_x : \mathcal{O}_x \to k$ hence an element $\delta_x \in \mathbf{H}$ supported by the point x with reduced structure. δ_e is a two-sided identity for convolution:

$$\delta_e * L = L * \delta_e = L.$$

Moreover, evaluation of elements $L \in \mathbf{H}$ at the function $1 \in \Gamma(\mathcal{O}_G)$ induces an augmentation

$$\epsilon : \mathbf{H} \longrightarrow k.$$

Note that if G is finite and reduced, the δ_x's are a basis of $\mathbf{H}$ over k, and since $\delta_x * \delta_y = \delta_{xy}$, $\mathbf{H}$ is nothing but the group algebra $k[G]$ of G.

(3) The ordinary product of functions $\mathcal{O}_x \otimes \mathcal{O}_x \to \mathcal{O}_x$ induces a co-product

$$s: \mathbf{H} \longrightarrow \mathbf{H} \otimes_k \mathbf{H}.$$

This satisfies many identities, which we will consider later in §14 for finite commutative group schemes G.

The interesting thing is that the elements $L \in \mathbf{H}$ extend uniquely to left-invariant operators $D_L : \mathcal{O}_G \to \mathcal{O}_G$ such that, roughly, $(D_L f)(e) = L(f)$. These operators D_L are combinations of differential operators (which for every open set $U \subset G$, map $\mathcal{O}_G(U)$ to $\mathcal{O}_G(U)$) and translation operators $f \longmapsto f'$, $f'(x) = f(xa)$, (which map $\mathcal{O}_G(U)$ to $\mathcal{O}_G(U.a^{-1})$). We need some definitions.

DEFINITION. *A differential operator D on a scheme X is a k-linear endomorphism of the structure sheaf $\mathcal{O}_X$ such that there is an integer $N \geq 0$ having the property that if $f \in \mathfrak{M}_x^{N+1}$, some $x \in X$, then $Df(x) = 0$. The least such N is called the order of D.*

For example, the differential operators of order 0 are multiplications by functions, and those of order 1 are the sums of derivations plus multiplications by f's. Now say $L \in \mathbf{H}$ is supported by

$$Z = \bigcup_{i=1}^{n} \operatorname{Spec}(\mathcal{O}_{a_i}/\mathfrak{M}_{a_i}^{d_i}).$$

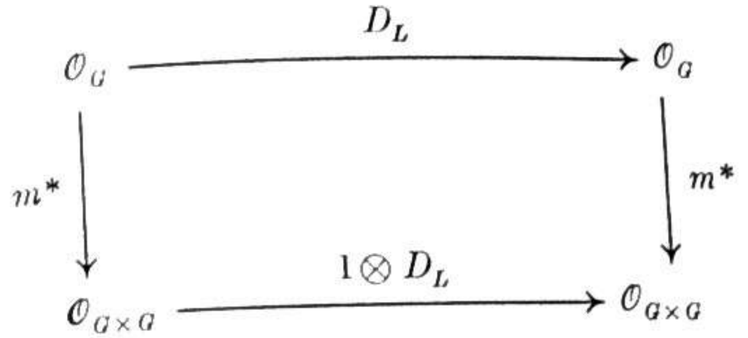
We then define an operator $D_L : \mathcal{O}_G \to \mathcal{O}_G$ which consists of a set of maps

$$D_L : \mathcal{O}_G(U) \longrightarrow \mathcal{O}_G(V)$$

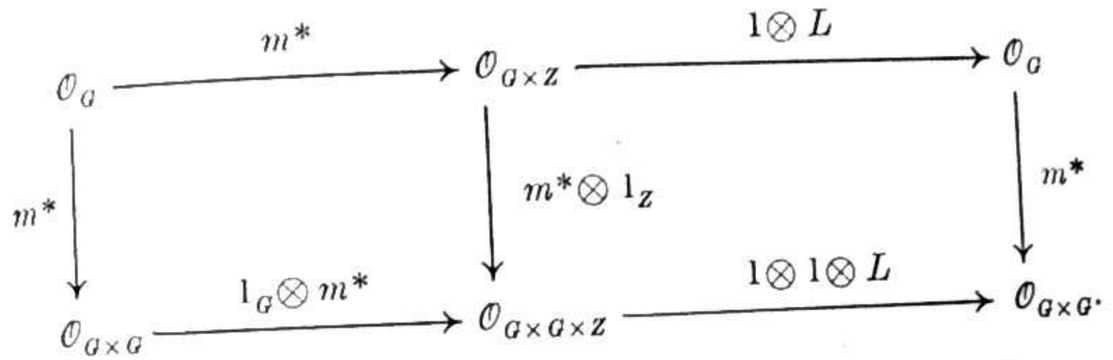
whenever $V.a_i \subset U$, $1 \leq i \leq n$, compatible with restrictions. We define D_L to be the composition:

$$\mathcal{O}_G \xrightarrow{m^*} \mathcal{O}_{G\times G} \xrightarrow{\text{res}} \mathcal{O}_{G\times Z} \xrightarrow{1\otimes L} \mathcal{O}_G.$$

It is easy to see that D_L is a sum of operators $D_{L,i}$ which are given by differential operators of order $< d_i$, followed by right translation by a_i. In particular, if $L \in \mathbf{H}_e$, then D_L is a differential operator. Moreover, D_L is left-invariant, i.e. the diagram



commutes. In fact, substituting the definition of D_L, this diagram becomes the outer rectangle of



The left-square commutes by associativity of the group law m, while the right square obviously commutes.

It follows immediately from the definition that if $f \in \mathcal{O}_G(U)$, and $a_i \in U$, $1 \leq i \leq n$, then $D_L f$ is defined at e and $D_L f(e) = L(f)$. The correspondence $L \longmapsto D_L$ generalizes the isomorphism $T_{e,G} \simeq$ {left-invariant derivations} used in defining the Lie algebra of G. In fact, the tangent space $T_{e,G}$ can be naturally identified with a subspace of $\mathbf{H}$:

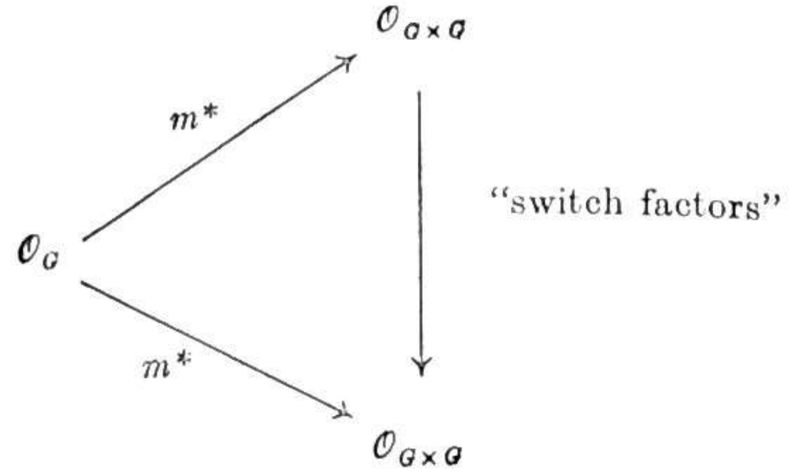
$$T_{e,G} \simeq \{L : \mathcal{O}_{e,G} \to k \mid L(1) = 0,\ L(\mathfrak{M}_e^2) = (0)\} \subset \mathbf{H},$$

and if $L \in T_{e,G}$, then D_L is the unique left-invariant derivation with value L at e. An important fact is that convolution of L's goes over to composition of operators:

$$(*) \qquad D_{L_1 * L_2} = D_{L_1} \circ D_{L_2}.$$

The proof is straightforward and is left to the reader. In particular, (*) shows that the Poisson bracket of left-invariant derivations can be interpreted by a commutator with respect to convolution product in $\mathbf{H}$ and that the p^{th} power on left-invariant

derivations can be interpreted as p^{th} power in $\mathbf{H}$. Note that if G is commutative, then $m^*: \mathcal{O}_G \to \mathcal{O}_{G\times G}$ is co-commutative, i.e.



commutes, and therefore convolution product in $\mathbf{H}$ will be commutative too.

This gives us a second proof that if G is commutative, then the bracket on its Lie algebra is zero.

To illustrate hyperalgebras, look at the simplest cases $G = \mu_p$ and $G = \alpha_p$. Writing

$$\mu_p = \operatorname{Spec} k[X]/(X^p - 1)$$
$$\alpha_p = \operatorname{Spec} k[X]/(X^p),$$

then in the first case all left-invariant differential operators are given by

$$f \longmapsto a_0 f + a_1 X \frac{df}{dX} + \ldots + a_{p-1} \cdot \left(X \frac{d}{dX}\right)^{p-1} f$$

and in the second case by

$$f \longmapsto a_0 f + a_1 \frac{df}{dX} + \ldots + a_{p-1} \frac{d^{p-1} f}{dX^p}.$$

Thus $\mathbf{H} \simeq k[D]/(D^p - D)$ or $\simeq k[D]/(D^p)$, where $D = X \dfrac{d}{dX}$ or $= \dfrac{d}{dX}$.

12. Quotients by Finite Group Schemes. An *action* of a group scheme G on a scheme X is a morphism:

$$\mu: G \times X \to X$$

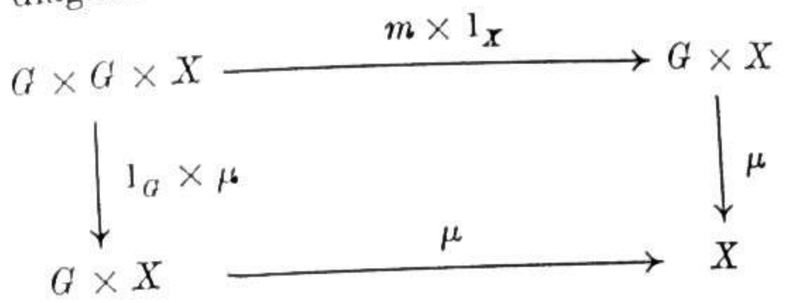
such that

(i) the composite

$$X \simeq \operatorname{Spec}(k) \times X \xrightarrow{e \times 1_X} G \times X \xrightarrow{\mu} X$$

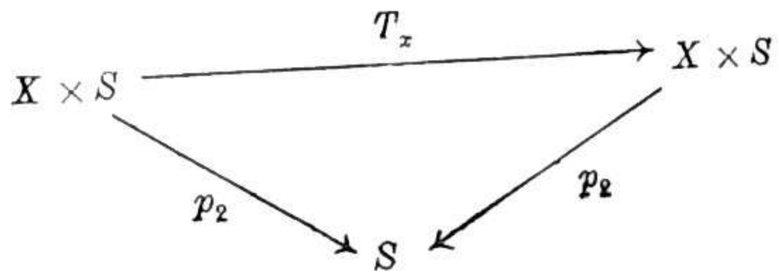
is the identity;

(ii) the diagram



is commutative.

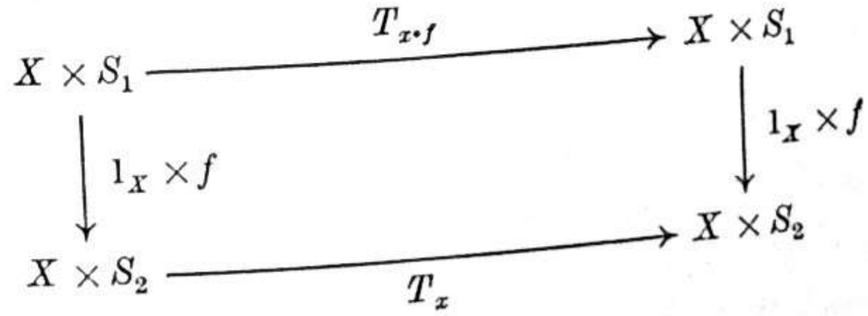
(Here, as usual, e is the identity and m is multiplication.) This is equivalent to saying that $\underline{G}(S)$ acts on $\underline{X}(S)$ for every scheme S (or even every affine S), functorially in S. It is also equivalent to saying that for every S-valued point $x \in \underline{G}(S)$, we are given an automorphism over S:



such that

(i) if $x, y \in \underline{G}(S)$, then $T_x \circ T_y = T_{x \cdot y}$;

(ii) if $f: S_1 \to S_2$ is any morphism, $x: S_2 \to G$ is an S_2-valued point, so $x \circ f: S_1 \to G$ is an S_1-valued point, then



commutes.

Explicitly, the T_x's are induced by μ via the formula $T_x = (\mu \circ \sigma \circ (1_X \times x), p_2)$ where $\sigma: X \times G \to G \times X$ is the switch morphism; and conversely, if we let $S = G$ and take x to be the G-valued point $1_G: G \to G$ of G, then $p_1 \circ T_x: X \times G \to X$ is just μ (except for the factors being reversed).

A morphism $f: X \to Y$ is said to be *G-invariant* if the diagram

$$\begin{array}{ccc} G \times X & \xrightarrow{\mu} & X \\ {\scriptstyle p_2}\downarrow & & \downarrow{\scriptstyle f} \\ X & \xrightarrow{f} & Y \end{array}$$

is commutative, i.e. in terms of S-valued points g and x of G and X, $f(\mu(g, x)) = f(x)$. In particular, taking $Y = \mathbf{A}^1$, we get the notion of a G-invariant function. We say that the action of G on X is *free* if the morphism

$$(\mu, p_2): G \times X \longrightarrow X \times X$$

is a closed immersion.

The action of a group G on a scheme X has a differential-geometric as well as a set-theoretic aspect. Let $\mathbf{H}_e$ be the part of the hyperalgebra of G with supports at e, and let $L \in \mathbf{H}_e$. Then L defines a differential operator D_L on X via

$$\mathcal{O}_X \xrightarrow{\mu^*} \mathcal{O}_{G \times X} \xrightarrow{L \otimes 1} \mathcal{O}_{\{e\} \times X} \approx \mathcal{O}_X.$$

It is easy to check that (a) $D_{L_1 * L_2} = D_{L_2} \circ D_{L_1}$, (b) D_{δ_e} is the identity, and (c) if $L \in T_{e,G} \subset \mathbf{H}_e$, then D_L is a differential operator of order 1, i.e. a derivation from $\mathcal{O}_X$ to $\mathcal{O}_X$. In particular, the Lie algebra of G is represented by derivations of $\mathcal{O}_X$.

Let $\mathcal{F}$ be a coherent sheaf on X. A *lift* of the action μ to $\mathcal{F}$ is by definition an isomorphism $\lambda: p_2^*(\mathcal{F}) \xrightarrow{\sim} \mu^*(\mathcal{F})$ of sheaves on $G \times X$ such that the diagram of sheaves on $G \times G \times X$,

$$\begin{array}{ccc} p_3^*(\mathcal{F}) & \xrightarrow{(p_2, p_3)^*(\lambda)} & \xi^*(\mathcal{F}) \\ & {\scriptstyle (m \times 1_X)^*(\lambda)} \searrow \quad \swarrow {\scriptstyle (1_G \times \mu)^*(\lambda)} & \\ & \eta^*(\mathcal{F}) & \end{array}$$

where $\xi = \mu \circ (p_2, p_3)$, $\eta = \mu \circ (m \times 1_X) = \mu \circ (1_G \times \mu)$, and p_i is the ith projection of $G \times G \times X$, is commutative.

A more manipulable way of defining a lift of an action μ to $\mathcal{F}$ is to require, for every S-valued point f of G, an automorphism λ_f of the sheaf $\mathcal{F} \otimes \mathcal{O}_S$ on $X \times S$ covering the automorphism μ_f of $X \times S$

$$\begin{array}{ccc} \mathcal{F} \otimes \mathcal{O}_S & \xrightarrow{\lambda_f} & \mathcal{F} \otimes \mathcal{O}_S \\ X \times S & \xrightarrow[\mu_f]{} & X \times S \end{array}$$

such that (1) the λ_f's are functorial in f, and (2) $\lambda_{f \cdot g} = \lambda_f \circ \lambda_g$.

Having stated these definitions, let us generalize the principal results of §7 on quotients by finite groups to quotients by finite group schemes. The following theorem is proved analogously to the first proposition of §7, so that we content ourselves with stating the necessary modifications.

THEOREM 1. (A) *Let G be a finite group scheme acting on a scheme X such that the orbit of any point is contained in an affine open subset of X. Then there is a pair (Y, π), where Y is a scheme and $\pi: X \to Y$ a morphism, satisfying the following conditions:*

(i) *as a topological space, (Y, π) is the quotient of X for the action of the underlying finite group;*

(ii) *the morphism $\pi: X \to Y$ is G-invariant, and if $\pi_*(\mathcal{O}_X)^G$ denotes the subsheaf of $\pi_*(\mathcal{O}_X)$ of G-invariant functions, the natural homomorphism $\mathcal{O}_Y \to \pi_*(\mathcal{O}_X)^G$ is an isomorphism.*

The pair (Y, π) is uniquely determined up to isomorphism by these conditions. The morphism π is finite and surjective. Y will be denoted X/G, and it has the functorial property: $\forall$ G-invariant morphisms $f: X \to Z$, $\exists$ a unique morphism $g: Y \to Z$ such that $f = g \circ \pi$.

(B) *Suppose further that the action of G is free and $G = \mathrm{Spec}(R)$, $n = \dim_k R$. Then π is a flat morphism of degree n, i.e. $\pi_*(\mathcal{O}_X)$ is a locally free $\mathcal{O}_Y$-module of rank n, and the subscheme of $X \times X$ defined by the closed immersion*

$$(\mu, p_2) : G \times X \longrightarrow X \times X$$

is equal to the subscheme $X \times_Y X \subset X \times X$. Finally, if $\mathcal{F}$ is a coherent $\mathcal{O}_Y$-module, $\pi^*\mathcal{F}$ has a naturally defined G-action lifting that on X, and

$$\mathcal{F} \longmapsto \pi^*\mathcal{F}$$

is an equivalence of the category of coherent $\mathcal{O}_Y$-modules (resp. locally free $\mathcal{O}_Y$-modules of finite rank) and the category of coherent $\mathcal{O}_X$-modules with G-action (resp. locally free $\mathcal{O}_X$-modules of finite rank with G-action).

Proof of (A). As before we are reduced to the case when $X = \mathrm{Spec}\ A$ is affine. Let R be the ring of G, $\epsilon: R \to k$ the evaluation map at e, $m^*: R \to R \otimes_k R$ and $\mu^* : A \to R \otimes_k A$ the homomorphisms of k-algebras induced by m and μ. Let $B = A^G = \{a \in A \mid \mu^*(a) = 1 \otimes a\}$ be the algebra of G-invariants in A. Let $\mathrm{Nm}_A : R \otimes_k A \to A$ be the norm mapping (defined since $R \otimes_k A$ is free of finite rank over A), so that Nm is a homogeneous polynomial function over A of degree $n = \dim_k(R)$ which is multiplicative. Define $N: A \to A$ by putting $N(\alpha) = \mathrm{Nm}(\mu^*(\alpha))$, so that N is again multiplicative and k-homogeneous of degree n. We assert that $N(A) \subset B$.

To prove this, we have to show that for any $\alpha \in A$, $\mu^*(N(\alpha)) = 1 \otimes N\alpha$. For any k-algebra B, denote by Nm_B the norm mapping $R \otimes_k B \to B$. Define $\phi : A \to R \otimes_k A$ and $\psi : R \otimes_k R \otimes_k A \to R \otimes_k R \otimes_k A$ by setting

$$\phi(a) = 1 \otimes a,$$

$$\psi(\xi \otimes \eta \otimes a) = (m^*(\xi) \otimes 1)(1 \otimes \eta \otimes a).$$

Note that if $f : B \to C$ is a homomorphism of k-algebras, we have $\mathrm{Nm}_C \circ (1_R \otimes f) = f \circ \mathrm{Nm}_B$. We thus have

$$\begin{aligned}
\mu^* \circ N &= \mu^* \circ \mathrm{Nm}_A \circ \mu^* \\
&= \mathrm{Nm}_{R \otimes_k A} \circ (1_R \otimes \mu^*) \circ \mu^* \\
&= \mathrm{Nm}_{R \otimes_k A} \circ (m^* \otimes 1_A) \circ \mu^* \\
&= \mathrm{Nm}_{R \otimes_k A} \circ \psi \circ (1_R \otimes \phi) \circ \mu^*.
\end{aligned}$$

Now, if we consider $R \otimes_k R \otimes_k A$ as an $R \otimes_k A$ algebra via the homomorphism $R \otimes_k A \to R \otimes_k R \otimes_k A$ given by $\eta \otimes a \longmapsto 1 \otimes \eta \otimes a$, ψ is an automorphism of the $R \otimes_k A$ algebra $R \otimes_k R \otimes_k A$, so that $\mathrm{Nm}_{R \otimes_k A} \circ \psi = \mathrm{Nm}_{R \otimes_k A}$. Thus, we obtain

$$\begin{aligned}
\mu^* \circ N &= \mathrm{Nm}_{R \otimes_k A} \circ (1_R \otimes \phi) \circ \mu^* \\
&= \phi \circ \mathrm{Nm}_A \circ \mu^* \\
&= \phi \circ N.
\end{aligned}$$

This proves our assertion.

Now, G also acts on $X \times \mathbf{A}^1$, (by acting trivially on $\mathbf{A}^1$), so that $N: A[T] \to A[T]$ is also defined. For any $a \in A$, put $\chi_a(T) = N(T - a)$. Then $\chi_a(T) = T^n + s_1 T^{n-1} + \cdots + s_n$ is G-invariant, and is the characteristic polynomial of the endomorphism of the free A-module $R \otimes_k A$ defined by the element $\mu^*(a)$. Since $\epsilon \otimes 1: R \otimes_k A \to A$ is surjective and $(\epsilon \otimes 1)(\mu^*(a)) = a$, $\mu^*(a) - a$ defines the zero map on the quotient A of $R \otimes_k A$ (via $\epsilon \otimes 1$), hence $\det(\mu^*(a) - a) = \chi_a(a) = 0$. The equation $\chi_a(a) = 0$ shows that a is integrally dependent on B. Thus A is integral over B. Since A is finitely generated over k, A is also integral over a finitely generated subalgebra of B. Thus A and hence B is a finite module over this subalgebra, and so B is also finitely generated over k. Let $Y = \mathrm{Spec}\ B$ and let $\pi: X \to Y$ be the induced morphism. Then π is finite and surjective. Using the map N, one sees as before that π separates orbits, so that (i) holds. Further π is clearly G-invariant, so that we have an inclusion $\mathcal{O}_Y \subset \pi_*(\mathcal{O}_X)^G$, inducing isomorphism of global sections. On the other hand, $\pi_*(\mathcal{O}_X)^G$ is a coherent $\mathcal{O}_Y$-module, being the kernel

of the $\mathcal{O}_Y$-homomorphism $\lambda : \pi_*(\mathcal{O}_X) \to \pi_*(\mathcal{O}_X) \otimes_k R$, $\lambda(f) = \mu^*(f) - f \otimes 1$, and this shows that $\mathcal{O}_Y = \pi_*(\mathcal{O}_X)^G$. This proves (ii).

PROOF OF (B). For the construction of the G-action on $\pi^*(\mathcal{F})$, the basic fact is the following. If $X \xrightarrow{f} Y \xrightarrow{g} Z$ are morphisms and $\mathcal{F}$ a sheaf of $\mathcal{O}_Z$-modules, there is a natural isomorphism $\lambda_{f,g}(\mathcal{F}) : (g \circ f)^*(\mathcal{F}) \xrightarrow{\sim} f^*(g^*(\mathcal{F}))$, satisfying the following condition: if $X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} T$ are morphisms, the square

$$\begin{array}{ccc} f^*g^*h^*(\mathcal{F}) & \xrightarrow{f^*(\lambda_{g,h})} & f^*(h\circ g)^*(\mathcal{F}) \\ \downarrow{\scriptstyle \lambda_{f,g}(h^*(\mathcal{F}))} & & \downarrow{\scriptstyle \lambda_{f,h\circ g}} \\ (g\circ f)^*h^*(\mathcal{F}) & \xleftarrow{\lambda_{g\circ f,h}} & (h\circ g\circ f)^*(\mathcal{F}) \end{array}$$

is commutative.

Returning to our special case, the equality of the two composites $G \times X \underset{p_2}{\overset{\mu}{\rightrightarrows}} X \xrightarrow{\pi} Y$ enables us (by means of λ) to define an isomorphism λ: $p_2^*(\mathfrak{g}) \to \mu^*(\mathfrak{g})$, $\mathfrak{g} = \pi^*(\mathcal{F})$, and one checks that this is an action, using the above remark.

On the other hand, let $\mathfrak{g}$ be a sheaf on X with a G-action covering the action on X. A section $\sigma \in \mathfrak{g}(X)$ is said to be G-invariant if $\lambda(p_2^*(\sigma)) = \mu^*(\sigma)$. Localizing, we have the notion of the subsheaf $\pi_*(\mathfrak{g})^G$ of G-invariants of $\pi_*(\mathfrak{g})$. This is clearly an $\mathcal{O}_Y$-module which is coherent, being the subsheaf of $\pi_*(\mathfrak{g})$ where two $\mathcal{O}_Y$-homomorphisms $\pi_*(\mathfrak{g}) \rightrightarrows \pi_*(\mathfrak{g} \otimes_k R)$ coincide. As before, we have evident natural transformations $S(\mathcal{F}) : \mathcal{F} \to \pi_*(\pi^*(\mathcal{F}))^G$ and $T(\mathfrak{g}) : \pi^*(\pi_*(\mathfrak{g})^G) \to \mathfrak{g}$, and it is again sufficient to show that (when the action is free) π is flat, $G \times X \xrightarrow{\sim} X \times_Y X$, and $T(\mathfrak{g})$ is an isomorphism for every G-sheaf $\mathfrak{g}$ on X (as in the proof of Proposition 2, §7). In view of these remarks, since all the definitions localize, we may assume $X = \operatorname{Spec} A$ affine. Recall that the freeness of the action means that the morphism

$$(\mu, p_2) : G \times X \longrightarrow X \times X$$

is a closed immersion. Since π is G-invariant, (μ, p_2) factors through a closed immersion of $G \times X$ into $X \times_Y X$. On the ring level, this means that the homomorphism

$$\lambda : A \otimes_B A \longrightarrow R \otimes_k A$$

$$\lambda(a_1 \otimes a_2) = \mu^*(a_1) \cdot (1 \otimes a_2)$$

is surjective. We have to show (a) that A is flat over $B = A^G$ and λ is injective, (b) if $\mathfrak{g}$ is a G-sheaf on X with $\mathfrak{g}(X) = M$, $A \otimes_B M^G \to M$ is an isomorphism, and (c) if M is projective over A, M^G is B-projective. Note however that (c) is an immediate consequence of (a) and (b). In fact, it suffices to show that M^G is B-flat, i.e. the functor $N \longmapsto N \otimes_{A^G} M^G$ is exact on the category of A^G-modules, and since A is faithfully flat over A^G, it suffices to show that $N \longmapsto (N \otimes_{A^G} M^G) \otimes_{A^G} A \simeq (N \otimes_{A^G} A) \otimes_A (A \otimes_{A^G} M^G) \simeq (N \otimes_{A^G} A) \otimes_A M$ is exact, and this holds in view of (a).

To prove (a), we may pass to the ring of quotients of A and B with respect to $S = B - \mathfrak{M}$, where $\mathfrak{M}$ is a maximal ideal of B, so that we may assume B local and A semilocal.

If we consider $A \otimes_B A$ and $R \otimes_k A$ as A-modules through their second factors, λ is a surjective A-homomorphism, so that $R \otimes_k A$ is generated by $\mu^*(A)$. Since A is semilocal and $\mu^*(A)$ generates the free module $R \otimes_k A$, one shows easily that there are $\{a_i\}$ $(1 \leq i \leq n = \dim_k R)$ such that $\mu^*(a_i)$ form a basis of $R \otimes_k A$ over A. Now suppose $a, \lambda_1, \ldots, \lambda_n \in A$. I claim:

$$\left[\mu^*(a) = \sum_{i=1}^{n} (1 \otimes \lambda_i) \cdot \mu^*(a_i) \right] \tag{*}$$

$$\Longleftrightarrow \left[a = \sum \lambda_i a_i \text{ and } \lambda_1, \ldots, \lambda_n \in B \right].$$

The implication $\Leftarrow$ is obvious by applying μ^* and using the fact that $\mu^*(\lambda_i) = (1 \otimes \lambda_i)$ if $\lambda_i \in B$. To prove $\Rightarrow$, use the fact that $(1 \otimes \mu^*)(\mu^* a) = (m^* \otimes 1)(\mu^* a)$ in $R \otimes_k R \otimes_k A$, hence substituting the expansion of $\mu^* a$, we deduce that

$$\sum_1^n (1 \otimes \mu^* \lambda_i) \cdot (1 \otimes \mu^*)(\mu^* a_i) = \sum_1^n (1 \otimes 1 \otimes \lambda_i) \cdot (m^* \otimes 1)(\mu^* a_i)$$

$$= \sum_1^n (1 \otimes 1 \otimes \lambda_i) \cdot (1 \otimes \mu^*)(\mu^* a_i).$$

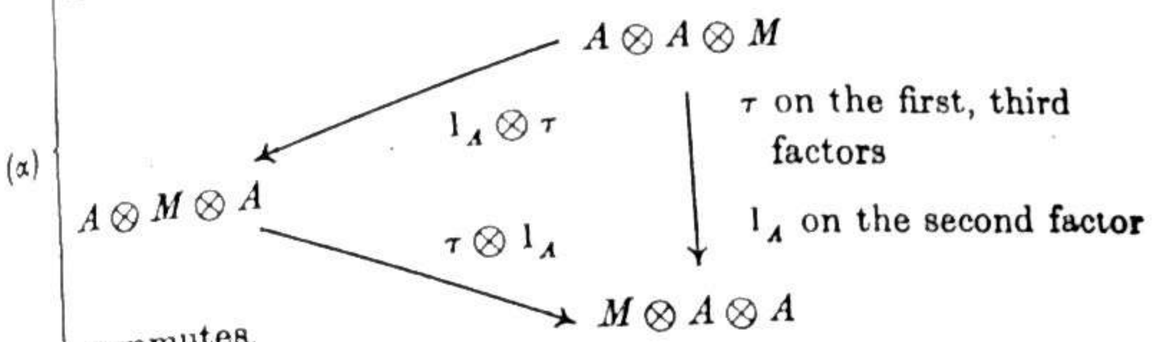
Since the $\mu^*(a_i)$ are linearly independent over A in $R \otimes_k A$, $(1 \otimes \mu^*)(\mu^* a_i)$ are linearly independent over $R \otimes_k A$ in $R \otimes_k R \otimes_k A$, the latter being considered as an algebra over the former via the last two factors. Hence the above equation yields that $1 \otimes \mu^* \lambda_i = 1 \otimes 1 \otimes \lambda_i$ i.e. $\lambda_i \in A^G = B$. Applying the homomorphism $\epsilon \otimes 1$ to the equation $\mu^*(a) = \Sigma(1 \otimes \lambda_i).\mu^*(a_i)$, we get that $a = \Sigma \lambda_i a_i$, as required. This proves (*). But (*) says that A is a free B-module with basis $a_1, \ldots, a_n$ and that the homomorphism $\lambda : A \otimes_B A \to R \otimes_k A$, regarded as a map of free A-modules via the second factor, takes the basis $a_i \otimes 1$ of the module on the left to the basis $\mu^*(a_i)$ of the module on the right. Therefore λ is an isomorphism.

We now prove (b). If $M = \mathfrak{g}(X)$ is the A-module corresponding to $\mathfrak{g}$, we first interpret the action of G on $\mathfrak{g}$ in terms of M. Firstly, $M \otimes_B A$ and $A \otimes_B M$ will be considered as $A \otimes_B A$-modules, where the first and second factors in $A \otimes_B A$ act on the first and second factors of the modules. It is easy to see that these are the two $A \otimes_B A$-modules obtained from the A-module M by tensor product with respect to the two homomorphisms $A \rightrightarrows A \otimes_B A$, $a \longmapsto a \otimes 1$ and $a \longmapsto 1 \otimes a$. In view of this, and the fact that $R \otimes_k A$ is naturally isomorphic to $A \otimes_B A$, it is easily checked that an action of G on $\mathfrak{g}$ amounts to an isomorphism of $A \otimes_B A$-modules :

$$\tau : A \otimes_B M \longrightarrow M \otimes_B A$$

such that

(α) if $M \otimes_B A \otimes_B A$, $A \otimes_B M \otimes_B A$, $A \otimes_B A \otimes_B M$ denote the usual $A \otimes_B A \otimes_B A$-modules, then the diagram:



commutes.

What is to be proven is that if N is the sub-B-module of M:

$$N = \{m \in M \mid \tau(1 \otimes m) = m \otimes 1\},$$

then the natural map $N \otimes_B A \to M$ is an isomorphism. We may rephrase the definition of N, and say that N is the kernel of the homomorphism of B-modules :

$$\phi : M \longrightarrow M \otimes_B A$$

$$\phi(m) = m \otimes 1 - \tau(1 \otimes m).$$

Since A is flat over B, it follows that $N \otimes_B A$ is the kernel of the homomorphism

$$\psi : M \otimes_B A \longrightarrow M \otimes_B A \otimes_B A$$

$$\psi(m \otimes a) = m \otimes 1 \otimes a - \tau(1 \otimes m) \otimes a.$$

In other words,

$$N \otimes_B A = \left\{ \sum m_i \otimes a_i \in M \otimes_B A \,\middle|\, \sum m_i \otimes 1 \otimes a_i = \sum \tau(1 \otimes m_i) \otimes a_i \right\}.$$

But the associative law (α), applied to the element $1 \otimes 1 \otimes m \in A \otimes A \otimes M$, says exactly that $\tau(1 \otimes m) \in M \otimes_B A$ has the property described in this equation. Therefore regarding $N \otimes_B A$ and $\tau(1 \otimes M)$ as two subsets of $M \otimes_B A$, we find $N \otimes_B A \supset \tau(1 \otimes M)$. Now both of them are modules over the subring $1 \otimes A \subset A \otimes_B A$. Moreover, $N \otimes_B A$ is generated over this ring by the elements $n \otimes 1$, $n \in N$, and since $\tau(1 \otimes n) = n \otimes 1$, these elements are in $\tau(1 \otimes M)$. Therefore $N \otimes_B A = \tau(1 \otimes M)$. But finally the maps

$$M \longrightarrow 1\otimes M \xrightarrow{\tau} \tau(1\otimes M)$$
$$m \longmapsto 1\otimes m$$

are isomorphisms, since A is faithfully flat over B, hence we obtain an isomorphism $N\otimes_B A \simeq M$. This is clearly the canonical map too, so (b) is proven.

DEFINITION. *A homomorphism $f: X \to Y$ of group schemes is an epimorphism if f is surjective and $f^*: \mathcal{O}_Y \to f_*\mathcal{O}_X$ is injective.*

COROLLARY 1. *Suppose X itself is a group scheme and G is a finite normal† subgroup scheme, acting on X by right-translation. Then X/G is again a group scheme, $\pi: X \to X/G$ is an epimorphism, and $G = \ker(\pi)$. Conversely, if $f: X \to Y$ is an epimorphism of group schemes, and if $G = \ker(f)$ is finite, then $Y \simeq X/G$.*

In other words, for every group scheme X we get a Galois-type correspondence between (a) normal finite subgroup schemes G, and (b) finite epimorphisms $\pi: X \to Y$. In fact, if the word "finite" is dropped from (a) and (b), the correspondence is still correct, but we will not prove this.

PROOF. First, say X is a group scheme and $G \subset X$ a finite normal subgroup. Let $m: X \times X \to X$ be the group law and consider the solid arrows in the diagram:

$$\begin{array}{ccc} X\times X & \xrightarrow{\ m\ } & X \\ \downarrow{\scriptstyle \pi\times\pi} & & \downarrow{\scriptstyle \pi} \\ X/G\times X/G & \dashrightarrow & X/G. \end{array}$$

Then $X/G \times X/G$ is the quotient of $X \times X$ by $G \times G$, and I claim that $\pi \circ m$ is a $G \times G$-invariant morphism. In fact, if x_1, x_2, g_1, g_2 are S-valued points of X and G respectively, then $\pi(m(x_1g_1 \times x_2g_2)) = \pi(x_1g_1 \cdot x_2g_2) = \pi(x_1x_2g_3) = \pi(x_1x_2) = \pi(m(x_1 \times x_2))$ where $g_3 = (x_2^{-1}g_1x_2)\cdot g_2 \in \underline{G}(S)$. It is easy to check that the dotted

† *Normal* means $\underline{G}(S)$ is a normal subgroup of $\underline{X}(S)$ for every S.

arrow defines a group law m' on X/G in terms of which π is a homomorphism. Now since $G \times X \simeq X \times_Y X$, it follows that if $x_1, x_2 \in \underline{X}(S)$, then $\pi(x_1) = \pi(x_2)$ if and only if $x_1 = x_2 \cdot g$, some $g \in G(S)$. In particular, if $K = \text{kernel}(\pi)$,

$$x_1 \in \underline{K}(S) \iff \pi(x_1) = \pi(e) \iff x_1 = g, \text{ some } g \in \underline{G}(S).$$

Thus $G = \text{kernel}(\pi)$.

The second half of the corollary is harder. Let $\pi: X \to X/G$ be the canonical map. In view of the G-invariance of f, there is a unique $g: X/G \to Y$ such that

$$\begin{array}{ccc} & X & \\ {\scriptstyle\pi}\swarrow & & \searrow{\scriptstyle f} \\ X/G & \xrightarrow[g]{} & Y \end{array}$$

commutes. By the first half of the corollary, X/G is a group scheme, and one checks easily that g is a homomorphism. In fact, g is also an epimorphism with trivial kernel and we are reduced to proving the special case that an epimorphism $f: X \to Y$ with trivial kernel is an isomorphism. We recall that if $g: S \to T$ is any morphism such that $g^{-1}(t)$ is a finite set for every $t \in T$, then there is an open dense set $T_0 \subset T$ such that if $S_0 = g^{-1}(T_0)$ $g|_{S_0}: S_0 \to T_0$ is a finite morphism. In our case, say $f|_{X_0}: X_0 \to Y_0$ is finite. Then for every $x \in X$, if R_x is right translation by X, we get a diagram:

$$\begin{array}{ccc} X_0 & \xrightarrow{R_x} & X_0\cdot x \\ \approx & & \\ {\scriptstyle \text{res } f}\downarrow & & \downarrow{\scriptstyle \text{res } f} \\ Y_0 & \xrightarrow{R_{f(x)}} & Y_0\cdot f(x) \\ \approx & & \end{array}$$

so f is a finite morphism from $X_0 \cdot x$ to $Y_0 \cdot f(x)$ too. Since the open sets $Y_0 \cdot f(x)$ cover Y, f itself is a finite morphism. Therefore, to show that f is an isomorphism, it suffices to prove that the homo-

morphism $f^*: \mathcal{O}_Y \to f_*\mathcal{O}_X$ is an isomorphism. But we know f^* is injective, and by Nakayama's lemma, f^* is surjective if for all $y \in Y$, the map

$$f_y^*: k \approx \mathcal{O}_y/\mathfrak{M}_y \longrightarrow f_*\mathcal{O}_X \otimes_{\mathcal{O}_y} (\mathcal{O}_y/\mathfrak{M}_y)$$

is surjective. But $\mathrm{Spec}(f_*\mathcal{O}_X \otimes \mathcal{O}_y/\mathfrak{M}_y)$ is the fibre $f^{-1}(y)$, and all the fibres of f are isomorphic by translation to the kernel of f. This kernel is trivial, so we deduce that for all $y \in Y$, $f^{-1}(y)$ is one point with reduced structure. Therefore f_y^* is surjective, and f is an isomorphism.

COROLLARY 2. *Let $Y = X/G$ as in the theorem. Let $\mathfrak{g}$ be any coherent sheaf on X acted on by G. Then there is a natural isomorphism*

$$\pi^*(\pi_*\mathfrak{g}) \simeq \mathfrak{g} \otimes_k R.$$

PROOF. Given the situation:

$$\begin{array}{ccc} X' & \xrightarrow{g'} & X \\ {\scriptstyle f'}\downarrow & & \downarrow{\scriptstyle f} \\ Y' & \xrightarrow[g]{} & Y \end{array}$$

and a sheaf $\mathfrak{g}$ on X, the natural homomorphism $f^*(f_*(\mathfrak{g})) \to \mathfrak{g}$ induces $g'^*f^*(f_*(\mathfrak{g})) \to g'^*(\mathfrak{g})$, that is, $f'^*g^*(f_*(\mathfrak{g})) \to g'^*(\mathfrak{g})$, or what is the same, $g^*(f_*(\mathfrak{g})) \to f'_*(g'^*(\mathfrak{g}))$. If f is an affine morphism and $X' = Y' \times_Y X$, this is an isomorphism. In fact, the problem being local on Y and Y', we may assume both (and hence all four of X, Y, X', Y') affine, and the assertion is then obvious. Apply this remark with $X = Y'$, $f = g = \pi$, to deduce that $\pi^*(\pi_*(\mathfrak{g})) = p_{2*}p_1^*(\mathfrak{g})$ where $p_i: X \times_Y X \to X$ are the projections. Denoting the i^{th} projection of $G \times X$ by q_i, and using the isomorphism (μ, q_2): $G \times X \to X \times_Y X$ and the G-action on $\mathfrak{g}$, we get that $\pi^*(\pi_*(\mathfrak{g})) \simeq q_{2*}\mu^*(\mathfrak{g}) \simeq q_{2*}q_2^*(\mathfrak{g}) = \mathfrak{g} \otimes_k R$, which proves the corollary.

We now want to prove a theorem on the Euler characteristic of inverse images of coherent sheaves for a class of morphisms. For this, we introduce some definitions.

Let G be a finite group scheme acting freely on a scheme X such that the quotient X/G exists. Let F be a finite scheme on which G acts. Then G acts on $X \times F$ in an obvious way. It is easy to check that this action is again free, that the quotient $U = (X \times F)/G$ exists, and that we have a natural morphism $U \xrightarrow{\pi} V = X/G$. The morphism π obtained in this way will be called the *fibration with fiber F associated to the principal G-bundle $X \to X/G$*. π is finite and flat, so that $\pi_*(\mathcal{O}_U)$ is locally free over $\mathcal{O}_V$ of constant rank. We shall call this rank the *degree* of π.

THEOREM 2. *Let $\pi: U \to V$ be a fibration with finite fibers associated to a principal G-bundle over V, where G is a finite group scheme. For any coherent sheaf $\mathcal{F}$ on V, we have*

$$\chi(\pi^*(\mathcal{F})) = (\deg \pi) \cdot \chi(\mathcal{F}).$$

PROOF. It suffices to prove the theorem when G acts freely on U and $V = U/G$ since in the general case, we have $X \times F \to X \times F/G \to X/G$ and the theorem would be true for the composite and for the first morphism, so that it is also true for the second.

Thus we assume $V = U/G$ for a free action of G on U. For a coherent sheaf $\mathcal{F}$ on V, let $\mathcal{I}$ be the sheaf of ideals annihilating $\mathcal{F}$, and call the closed subschemes of V defined by $\mathcal{I}$ the support of $\mathcal{F}$. Then $\mathcal{F}$ is a coherent sheaf on this subscheme. If the theorem is not true, since V is a noetherian space, we can find an $\mathcal{F}$ with support $V' \subset V$ for which the theorem is not valid, whereas for any coherent $\mathfrak{g}$ with $\mathrm{Supp}\ \mathfrak{g} \subsetneq \mathrm{Supp}\ \mathcal{F}$, the theorem is valid. Set $U' = \pi^{-1}(V')$. Then, using (B) of the proposition, one sees that U' is a principal G-space over V'. Replacing U and V by U' and V' respectively, we see that we may assume the theorem to be valid whenever $\mathrm{Supp}\ \mathcal{F} \subsetneq V$, that is, whenever $\mathrm{Ann}\ \mathcal{F} \neq (0)$. It is further clear that if in a short exact sequence of coherent sheaves on V, the theorem holds for two of the sheaves, it holds for the third (remember π is flat).

Now, if V were reducible, we can find a short exact sequence $0 \to \mathcal{G}_1 \to \mathcal{F} \to \mathcal{G}_2 \to 0$ with $\mathcal{G}_i$ having proper support $\subsetneq V$, and the theorem would hold for $\mathcal{F}$. Hence we may suppose V irreducible. If $\mathcal{I}$ is the subsheaf of nilpotent elements of V and $\mathcal{I} \neq 0$ we have the exact sequence $0 \to \mathcal{I}.\mathcal{F} \to \mathcal{F} \to \mathcal{F}/\mathcal{I}.\mathcal{F} \to 0$ and both $\mathcal{I}.\mathcal{F}$ and $\mathcal{F}/\mathcal{I}.\mathcal{F}$ have supports proper closed subschemes of V. Thus we may assume V reduced and irreducible. Let r be the rank of the generic fiber of $\mathcal{F}$. Then there is a sheaf of ideals $\mathcal{I}$ on V and an injective homomorphism $\mathcal{I}^r \to \mathcal{F}$ with cokernel having proper support. Thus, the theorem holds for $\mathcal{F}$ if and only if it holds for $\mathcal{I}^r$, and again by the exact sequence $0 \to \mathcal{I} \to \mathcal{O}_V \to \mathcal{O}_V/\mathcal{I} \to 0$, we see that the theorem holds for $\mathcal{I}$ if and only if it holds for $\mathcal{O}_V$. We see therefore that it suffices to prove the theorem for *one* coherent sheaf on V of non-zero rank. But then, $\pi_*(\mathcal{O}_U)$ is such a sheaf, since by Corollary 2 to the proposition,

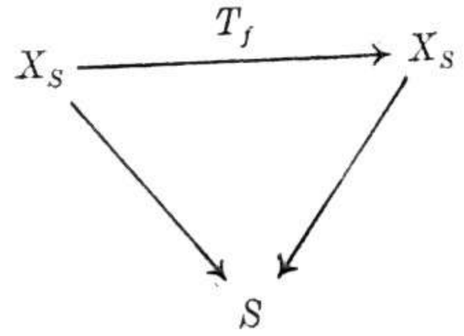
$$\chi(\pi^*(\pi_*(\mathcal{O}_U))) = \chi(\mathcal{O}_U \otimes_k R) = (\deg \pi)\, \chi(\mathcal{O}_U)$$
$$= (\deg \pi)\, \chi(\pi_*(\mathcal{O}_U)).$$

REMARK. The reason we have insisted on an associated fiber space, rather than confine ourselves to a space on which G acts freely is the following. Let $f\colon U \to V$ be a finite étale morphism everywhere of degree n. Then f can always be realized as the associated fiber space with finite fibers of a principal $\Sigma(n)$-space, where $\Sigma(n)$ is the symmetric group of order n. In fact, in the n-fold fiber product $U \times_V U \times_V \cdots \times_V U$, consider the set P of points $(x_1, \ldots, x_n)$ such that $x_i \neq x_j$ for $i \neq j$. Then P is both open and closed in $U \times_V U \times_V \cdots \times_V U$ and is stable for the natural action of $\Sigma(n)$. Further, P is étale over V, and V is the set-theoretic quotient of P by $\Sigma(n)$. It clearly follows that V is the scheme-theoretic quotient of P by $\Sigma(n)$ and P is a principal fiber space with structure group $\Sigma(n)$ over V. Let F be the reduced scheme with n points $[1, 2, \ldots, n]$ on which $\Sigma(n)$ acts naturally. Define a map $P \times F \to V$ by $((x_1, \ldots, x_n), i) \longmapsto x_i$. This map is invariant for the action of $\Sigma(n)$ on $P \times F$ and V is the set-theoretic quotient. Since $P \times F \to V$ is again étale, V is the scheme quotient of $P \times F$ by $\Sigma(n)$.

Thus, the theorem is applicable to any finite étale morphism of constant degree n.

13. **The Dual Abelian Variety in any characteristic.** For a line bundle L on an abelian variety X, we had earlier defined a closed subset $K(L)$ of X as consisting of the points $x \in X$ for which $T_x^*(L) \simeq L$, and we had shown that it is a subgroup. We shall now define a structure of subscheme on $K(L)$. Namely, consider the standard line bundle $M = m^*(L) \otimes p_1^*(L)^{-1} \otimes p_2^*(L)^{-1}$ on $X \times X$, and define $K(L)$ to be the maximal subscheme of X such that $M|K(L) \times X$ is trivial. (See § 10).

We can interpret the S-valued points of $K(L)$ roughly as the set of S-valued points $f\colon S \to X$ such that L is invariant under translation by f. Namely, $X_S = X \times S$, and let T_f:



be the automorphism of X_S induced by f (i.e. $T_f(x, s) = (x + f(s), s)$ in terms of T-valued points x, s of X, S). Let L_S be the induced line bundle $p_1^* L$ on X_S. Now when S is a big space, the condition $T_f^*(L_S) \simeq L_S$ is too strong; for example, L_S and $T_f^*(L_S)$ can be isomorphic on the sets $X \times U_i$ for $\{U_i\}$ an open cover of S, without being isomorphic. The correct condition to look at is:

$$T_f^*(L_S) \simeq L_S \otimes p_2^* N, \qquad N \text{ a line bundle on } S. \qquad (*)$$

Then I claim that (*) holds if and only if f is an S-valued point of $K(L)$.

PROOF. Note that the composite $X \times S \xrightarrow{T_f} X \times S \xrightarrow{p_1} X$ is just the composite $X \times S \xrightarrow{1_X \times f} X \times X \xrightarrow{m} X$, so $T_f^*(L_S) \simeq (1_X \times f)^* m^* L$. Thus $L_S|_{(0) \times S}$ is trivial, while $T_f^*(L_S)|_{(0) \times S} \simeq f^* L$.

Now whenever (*) holds, the N which occurs can be identified by restricting both sides to $(0) \times S$:

$$f^*(L) \simeq T_f^*(L_S)\,|_{(0)\times S} \simeq L_S \otimes p_2^* N\,|_{(0)\times S} \simeq N.$$

Thus (*) holds if and only if

$$(1_X \times f)^* m^* L \simeq p_1^* L \otimes p_2^*(f^* L).$$

But $(1_X \times f)^* m^* L \otimes p_1^* L^{-1} \otimes p_2^*(f^*L)^{-1} \simeq (1_X \times f)^* M$, so (*) holds if and only if $(1_X \times f)^* M$ is trivial, which means, by definition that f factors through $K(L)$.

An immediate consequence is that $\underline{K(L)}\,(S)$ is a *subgroup* of $\underline{X}(S)$, hence $K(L)$ is a subgroup scheme of X.

Our next aim is to construct the dual abelian variety of X, imitating the procedure in characteristic 0. Choose an L which is ample. Then $K(L)$ is a finite group scheme. We define $\hat{X}$ to be the quotient abelian variety $X/K(L)$. Let $\pi: X \to \hat{X}$ be the natural homomorphism. As before, we wish to define the Poincaré line bundle P on $\hat{X} \times X$ by defining it as the quotient of the line bundle M on $X \times X$ by a suitable action of $K(L) \times \{0\}$ lifting the translation action on $X \times X$ (it is easily checked that the natural homomorphism $X \times X/K(L) \times \{0\} \xrightarrow{\sim} X/K(L) \times X$ is an isomorphism).

Recall that an action of a subgroup $H \subset X$ on any coherent sheaf $\mathscr{F}$ on X can be described as the giving, for each $S \in \mathrm{Obj}\ \underline{\mathrm{Sch}}$, an action of the (abstract) group $\underline{H}(S)$ on $\mathscr{F}_S = \mathscr{F} \otimes_k \mathcal{O}_S$ lifting the action on X_S, this action varying functorially in S in an obvious sense.

Let us agree to denote all objects obtained by base extension to S by a subscript S. Now, $\underline{K(L)}(S)$ consists of the subgroup of $x \in \underline{X}(S)$ such that if T_x: $X_S \to X_S$ denotes translation by x, $T_x^*(L_S) \simeq L_S \otimes L_0$, where L_0 is the lift to X_S of a line bundle on S. On $X_S \times_S X_S = (X \times X)_S$, $M_S \simeq m_S^*(L_S) \otimes p_1^*(L_S)^{-1} \otimes p_2^*(L_S)^{-1}$, so that $T_{(x,0)}^*(M_S) \simeq m_S^* T_x^*(L_S) \otimes p_1^* T_x^*(L_S)^{-1} \otimes p_2^*(L_S)^{-1} \simeq M_S \otimes m_S^*(L_0) \otimes p_1^*(L_0^{-1}) \simeq M_S$. Thus, $T_{(x,0)}^*(M_S) \simeq M_S$, and to define a lift of $T_{(x,0)}$ to M_S, or equivalently an isomorphism of $T_{(x,0)}^*(M_S)$ with M_S,

it suffices to give an isomorphism of these line bundles on the subscheme $X_S \times_S 0_S$. This is because any two isomorphisms, either on $X_S \times_S X_S$ or on $X_S \times_S 0_S$, differ by multiplication by a unit, and the groups of global units on these schemes, $H^0((X \times X)_S, \mathcal{O}^*_{(X\times X)_S})$ and $H^0(X_S \times_S 0_S,\ \mathcal{O}^*_{X_S \times_S 0_S})$, are both isomorphic to $H^0(S, \mathcal{O}_S^*)$, hence the restriction map $H^0((X \times X)_S, \mathcal{O}^*_{(X\times X)_S}) \xrightarrow{\sim} H^0(X_S \times_S 0_S, \mathcal{O}^*_{X_S \times_S 0_S})$ is an isomorphism. Next, let V be the 1-dimensional vector space dual to the fiber $L/\mathfrak{M}_0 L$ of L at 0 on X, and let $V \times X_S$ be the trivial line bundle over X_S with fibre V. Then, if i: $X_S = X_S \times_S 0_S \to X_S \times_S X_S$ is the closed immersion,

$$i^*(M_S) \simeq i^* m^*(L_S) \otimes i^* p_1^*(L_S)^{-1} \otimes i^* p_2^*(L_S)^{-1} \simeq L_S \otimes L_S^{-1} \otimes_k V \simeq V \times X_S,$$

where all the isomorphisms are *canonical*. Therefore, we can choose a unique lifting of the translation $T_{(X,0)}$ to M_S by requiring that this lifting when restricted to $X_S \times_S 0_S$, becomes the map $1_V \times T_x$ on $V \times X_S$. It is then easy to check that the action of $\underline{K(L)}(S)$ on M_S defined like this is a group action, as required.

We conclude that there is a unique line bundle P on $\hat{X} \times X = X/K(L) \times X$ such that its pull back is isomorphic, as a line bundle acted on by $K(L)$, to M on $X \times X$. The restrictions of P to $\{0\} \times X$ and $\hat{X} \times \{0\}$ are trivial. Further, since ϕ_L: $X \to \mathrm{Pic}^0 X$ is surjective with kernel $K(L)$ we see that there is an induced isomorphism of abstract groups $\hat{X} \xrightarrow{\sim} \mathrm{Pic}^0 X$, and if $\alpha \in \hat{X}$, the restriction of P to $\{\alpha\} \times X$, considered as a line bundle on X, is nothing but the element of $\mathrm{Pic}^0 X$ corresponding to α. Thus, to check that $\hat{X}$ is a dual variety and P a Poincaré bundle on $\hat{X} \times X$, we have to prove the following

THEOREM. *Let S be any scheme, and L a line bundle on $S \times X$ such that $L\,|\,S \times \{0\}$ is trivial and $L\,|\,\{s\} \times X \in \mathrm{Pic}^0 X$ for every $s \in S$. Then there is a unique morphism ϕ: $S \to \hat{X}$ such that $L \simeq (\phi \times 1_X)^*(P)$.*

PROOF. Consider the line bundle $M = p_{23}^*(P) \otimes p_{13}^*(L)^{-1}$ on $S \times \hat{X} \times X$, and let Γ_S be the maximal subscheme of $S \times \hat{X}$

over which this line bundle is trivial. The main point is to show that if $\pi\colon \Gamma_S \to S$ is the restriction to Γ_S of the projection $S \times X \to S$, π is an isomorphism. For this, it is clearly sufficient to show that for any closed subscheme S_0 of S having support at one point of S, $(S_0 \times_S \Gamma_S) \to S_0$ is an isomorphism. On the other hand, by definition of Γ_S, if Γ_{S_0} denotes the corresponding closed subscheme of $S_0 \times X$ formed with respect to the line bundle $L \mid S_0 \times X$ on $S_0 \times X$, we have $S_0 \times_S \Gamma_S = \Gamma_{S_0}$. Thus for the proof of the main point, we may assume $S = \operatorname{Spec} B$, where B is a finite-dimensional local k-algebra. Further, if s is the unique point of S, one sees easily that the statement to be proved remains unaltered if we replace L by $L \otimes p_2^*(L \mid \{s\} \times X)^{-1}$, (since $\exists\ \hat{x} \in \hat{X}$ such that $L \mid \{s\} \times X \simeq P \mid \{\hat{x}\} \times X$) so that we may further assume that $L \mid \{s\} \times X$ is trivial.

Now, for all points $(s, x) \in S \times X$, the restriction of M to $\{s\} \times \hat{X} \times \{x\}$ belongs to $\operatorname{Pic}^0 \hat{X}$ (since this is so for $(s, 0)$); and there are at most finitely many points (s, x) such that M restricted to $\{s\} \times \hat{X} \times \{x\}$ is trivial, since there are at most finitely many $x \in X$ such that $m^*(L) \otimes p_1^*(L)^{-1} \otimes p_2^*(L)^{-1} \mid X \times \{x\} = T_x^*(L) \otimes L^{-1}$ is trivial. Hence, all the direct images $R^p p_{13,*}(M)$ on $S \times X$ have discrete support, so that by the Leray spectral sequence, $H^p(S \times \hat{X} \times X,\ M) \simeq H^0(S \times X, R^p p_{13,*}(M))$. On the other hand, $R^p p_{13,*}(M) \simeq R^p p_{13,*}(p_{23}^*(P)) \otimes L^{-1}$, so that we have isomorphisms of B-modules $H^p(S \times \hat{X} \times X, M) \simeq H^p(S \times \hat{X} \times X,\ p_{23}^*(P)) \simeq B \otimes_k H^p(\hat{X} \times X,\ P), p \geqslant 0$.

Therefore these cohomology groups are free B-modules. On the other hand, consider the direct images $R^p p_{12,*}(M)$. Since $M \mid \{s\} \times \{\hat{x}\} \times X \in \operatorname{Pic}^0 X$ for all $\hat{x}$ and is trivial only for $\hat{x} = 0$, all these sheaves $R^p p_{12,*}(M)$ are concentrated at the point $(s, 0) \in S \times \hat{X}$. Let $0 \to K_0 \to K_1 \to \dots \to K_g \to 0$ be a complex of free modules of finite type over the local ring $A = B \otimes_k \mathcal{O}_{0,\hat{X}}$ of $(s,0) \in S \times \hat{X}$ given by the base change theorem for direct images. Then $H^i(K.) \simeq [R^i p_{12,*}(M)]_{(s,0)}$ are modules of finite length over A and hence also over $\mathcal{O}_{0,\hat{X}}$. Now we have the

LEMMA. *Let $\mathcal{O}$ be a regular local ring of dimension g, and $0 \to K_0 \to K_1 \to \dots \to K_g \to 0$ be a complex of finitely generated free modules over $\mathcal{O}$. If the $H^i(K.)$ are artinian modules, we have $H^i(K.) = 0$ for $0 \leqslant i < g$.*

PROOF. Since there is nothing to prove for $g = 0$, we may assume $g > 0$ and that the result holds in smaller dimensions. Choose an x in the maximal ideal $\mathfrak{M}$ of $\mathcal{O}$ but not in $\mathfrak{M}^2$, so that $\overline{\mathcal{O}} = \mathcal{O}/\mathcal{O}x$ is regular of dimension $g - 1$. Putting $\overline{K}. = \overline{\mathcal{O}} \otimes_{\mathcal{O}} K.$, we have the exact sequence of complexes $0 \longrightarrow K. \xrightarrow{x} K. \longrightarrow \overline{K}. \longrightarrow 0$, from which we get the exact sequence

$$H^p(K.) \xrightarrow{x} H^p(K.) \longrightarrow H^p(\overline{K}.) \longrightarrow H^{p+1}(K.) \xrightarrow{x} H^{p+1}(K.).$$

This shows that the $H^p(\overline{K}.)$ are artinian. By induction hypothesis, $H^p(\overline{K}.) = 0$ for $p < g - 1$, so $H^{p+1}(K.) \xrightarrow{x} H^{p+1}(K.)$ is injective for $p < g - 1$. But since $H^{p+1}(K.)$ is artinian, x^n kills $H^{p+1}(K.)$ for some n, and hence $H^{p+1}(K.) = 0$, $p < g - 1$. The lemma is proved.

Applying the lemma to our complex of A free (and hence $\mathcal{O}_{0,\hat{X}}$-free) modules above, we deduce that $R^i p_{12,*}(M) = 0$ for $0 \leqslant i < g$, and that $0 \to K_0 \to K_1 \to \dots \to K_g \to N \to 0$ is an exact sequence of A-modules, where $N = R^g p_{12,*}(M)_{(s,0)} \simeq H^g(S \times \hat{X} \times X,\ M)$, which we saw above is B-free. Now, the derived modules of the complex $0 \to \hat{K}_g \to \hat{K}_{g-1} \to \dots \to \hat{K}_0 \to 0$, where $\hat{K}_i = \operatorname{Hom}_A(K_i, A)$, are again artinian, so that by another application of the above lemma, we get an exact sequence $0 \to \hat{K}_g \to \dots \to \hat{K}_0 \to K \to 0$, where K is an artinian A-module. Since we have the exact sequence

$$\begin{array}{ccccccc} & & & & k & & \\ & & & & \wr\| & & \\ 0 & \longrightarrow & H^0(\{s\} \times \{0\} \times X,\ P\,|_{\{s\} \times \{0\} \times X}) & \longrightarrow & K_0 \otimes_A k & \longrightarrow & K_1 \otimes_A k \end{array}$$

we get that the cokernel of $\hat{K}_1 \otimes k \to \hat{K}_0 \otimes k$ is of dimension one over k, that is, $K \otimes_A k = K/\mathfrak{M}_A K$ is one-dimensional. Therefore,

$K \simeq A/\mathfrak{A}$ as an A-module, for an ideal $\mathfrak{A}$ of A, and the free complex $(\hat{K}_i)$ resolves $A/\mathfrak{A}$. This implies that the homologies of its dual complex (K_i) are also annihilated by $\mathfrak{A}$, that is, $\mathfrak{A}.N = 0$†. Since N is B-free, $\mathfrak{A} \cap B \otimes 1 = (0)$, that is, $B \to A/\mathfrak{A}$ is injective. For any $\mathfrak{M}$-primary ideal $\mathfrak{b}$ in A, if $V(\mathfrak{b})$ is the closed subscheme defined by $\mathfrak{b}$ in $S \times \hat{X}$, we have

$H^0(V(\mathfrak{b}) \times X, M|_{V(\mathfrak{b})\times X}) \simeq \mathrm{Ker}[K_0/\mathfrak{b}K_0 \to K_1/\mathfrak{b}K_1] \simeq \mathrm{Hom}_A(A/\mathfrak{A}, A/\mathfrak{b})$,

from which it follows that $V(\mathfrak{A})$ contains the maximal subscheme Γ_S of $S \times \hat{X}$ over which M is trivial. On the other hand, $H^0(V(\mathfrak{A}) \times X$, $M|_{V(\mathfrak{A})\times X} \simeq \mathrm{Hom}_A(A/\mathfrak{A}, A/\mathfrak{A}) \simeq A/\mathfrak{A}$, and the natural map of line bundles

$$\mathcal{O}_{V(\mathfrak{A})\times X} \otimes_{A/\mathfrak{A}} H^0(V(\mathfrak{A}) \times X, M|_{V(\mathfrak{A})\times X}) \to M|_{V(\mathfrak{A})\times X}$$

is surjective, since reduced modulo the maximal ideal, the induced map on sections

$$\begin{array}{ccc} \mathrm{Hom}_A(A/\mathfrak{A}, A/\mathfrak{A}) & & \mathrm{Hom}_A(A/\mathfrak{A}, A/\mathfrak{M}_A) \\ \wr\| & & \wr\| \\ H^0(V(\mathfrak{A}) \times X, M|_{V(\mathfrak{A})\times X}) & \longrightarrow & H^0(\{s\} \times \{0\} \times X, M|_{\{s\}\times\{0\}\times X}) \end{array}$$

is surjective, and the line bundle $M|_{\{s\}\times\{0\}\times X}$ is trivial. Hence, $M|_{V(\mathfrak{A})\times X}$ is trivial, which shows that $\Gamma_S = V(\mathfrak{A})$. In particular, $B \to H^0(\Gamma_S, \mathcal{O}_{\Gamma_S}) = A/\mathfrak{A}$ is injective. On the other hand, $\pi^{-1}(s)$ is a closed subscheme of $\Gamma_S \cap \{s\} \times X$ such that the restriction of $\{s\} \times P$ to $\pi^{-1}(s) \times X$ is trivial. Since $\{0\}$ is the maximal subscheme of $\hat{X}$ over which P is trivial (practically by construction of $\hat{X}$), $\pi^{-1}(s)$ becomes the reduced point $(s, 0)$. This means that $A/\mathfrak{A} + \mathfrak{M}_B A = k$, so that $B \to A/\mathfrak{A}$ is also surjective, hence an isomorphism. Thus, π: $\Gamma_S \to S$ is an isomorphism.

Now, for any scheme S and line bundle L on $S \times X$ satisfying the hypothesis of the theorem, and any morphism ϕ: $S \to \hat{X}$, denoting by Γ_ϕ:$S \to S \times \hat{X}$ the graph morphism, we have the

† In fact, for every $a \in \mathfrak{A}$, show that the endomorphism of $(\hat{K}_i)$ given by multiplication by a is null-homotopic; hence so is the same endomorphism of (K_i).

equivalence $(\phi \times 1_X)^*(P) \simeq L \iff \Gamma_\phi$ factors through Γ_S. So the theorem clearly follows from the fact that Γ_S is already the graph of a unique morphism from S to $\hat{X}$.

COROLLARY 1. *We have*

$$H^i(\hat{X} \times X, P) = \begin{cases} (0) & \text{if } i \neq g \\ k & \text{if } i = g. \end{cases}$$

PROOF. Using the notations of the proof of the theorem, with $B = k$, L trivial, we have established that $K \simeq k$, i.e.

$$0 \longrightarrow \hat{K}_g \longrightarrow \hat{K}_{g-1} \longrightarrow \cdots \longrightarrow \hat{K}_0 \longrightarrow k \longrightarrow 0$$

is a free resolution of k. On the other hand, any two free resolutions of one module are homotopically equivalent, and the residue field k of any regular local ring such as $\mathcal{O}_{0,\hat{X}}$ has a well-known standard resolution, the Koszul complex. Namely, let $x_1, \ldots, x_g \in \mathfrak{M}_0$ lift a basis $\{\overline{x}_i\}$ of $\mathfrak{M}_0/\mathfrak{M}_0^2$. Let L_k be the free $\mathcal{O}_{0,\hat{X}}$-module with the formal symbols $e_{i_1} \wedge \cdots \wedge e_{i_k}$ $(1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant g)$ as a basis. Then

$$0 \longrightarrow L_g \xrightarrow{d_g} L_{g-1} \xrightarrow{d_{g-1}} \cdots\cdots \xrightarrow{d_1} L_0 \xrightarrow{d_0} k \longrightarrow 0$$

$$d_k(e_{i_1} \wedge \cdots \wedge e_{i_k}) = \sum_{l=1}^{k} (-1)^l x_{i_l} e_{i_1} \wedge \cdots \wedge \hat{e}_{i_l} \wedge \cdots \wedge e_{i_k}$$

is the Koszul complex. Then the dual complex

$$0 \longrightarrow K_0 \longrightarrow K_1 \longrightarrow \cdots\cdots \longrightarrow K_g \longrightarrow 0$$

is homotopic to the dual of the Koszul complex, which it is easy to see is still isomorphic to the original Koszul complex. This gives Corollary 1 by calculating cohomologies.

COROLLARY 2. *For an abelian variety X of dimension g,*

$$\dim_k H^p(X, \mathcal{O}) = \binom{g}{p}.$$

PROOF. In fact, $H^p(X, \mathcal{O})$ is isomorphic to the p^{th} cohomology of the complex

$$\mathcal{O} \longrightarrow K_0 \otimes k \longrightarrow K_1 \otimes k \longrightarrow \cdots \longrightarrow K_g \otimes k \longrightarrow 0,$$

which is homotopic to the Koszul complex tensored with k. Now, the differential operators of the Koszul complex tensored with k are trivial, so that we have $\dim_k H^p(X, \mathcal{O}) =$ rank of module of p-cochains of Koszul complex $= \binom{g}{p}$.

COROLLARY 3. *There is a canonical isomorphism of the tangent space to* (0) *on* $\hat{X}$ *and* $H^1(X, \mathcal{O}_X)$.

PROOF. Let $S = \operatorname{Spec} \frac{k[\epsilon]}{(\epsilon^2)}$, so that the tangent space to $\hat{X}$ at 0 is canonically isomorphic to $\operatorname{Hom}_0(S, \hat{X})$, where Hom_0 denotes the set of morphisms of S into $\hat{X}$ mapping the unique point s_0 of S onto 0. On the other hand, we have by the theorem,

$$\begin{aligned}\operatorname{Hom}_0(S, \hat{X}) &= \{\text{Line bundles on } S \times X \text{ trivial on } \{s_0\} \times X\} \\ &= \ker\{H^1(S \times X, \mathcal{O}^*_{S\times X}) \longrightarrow H^1(\{s_0\} \times X, \mathcal{O}^*_X)\}.\end{aligned}$$

But now, we have an exact sequence of multiplicative sheaves

$$1 \longrightarrow 1 + \epsilon\, \mathcal{O}_X \longrightarrow \mathcal{O}^*_{S\times X} \longrightarrow \mathcal{O}^*_X \longrightarrow 1,$$

and as sheaves of abelian groups, $1 + \epsilon\, \mathcal{O}_X \simeq \mathcal{O}_X$. Therefore the cohomology sequence gives

$$0 \longrightarrow H^1(\mathcal{O}_X) \longrightarrow H^1(S \times X, \mathcal{O}^*_{S\times X}) \longrightarrow H^1(X, \mathcal{O}^*_X)$$

and this gives a natural isomorphism of the tangent space to 0 at $\hat{X}$ with $H^1(X, \mathcal{O}_X)$, at least as abelian groups. It can be checked that this is actually an isomorphism of k-vector spaces.

Now, let $f: X \to Y$ be an isogeny of abelian varieties. By the theorem, we get a unique homomorphism $\hat{f}: \hat{Y} \to \hat{X}$ of abelian varieties such that if P_X, P_Y are the Poincaré bundles on $X \times \hat{X}$ and $Y \times \hat{Y}$ respectively, we have

$$(1 \times \hat{f})^*(P_X) \simeq (f \times 1)^*(P_Y).$$

Hence, if we denote this line bundle by Q, on applying the proposition of §12, we get that

$$\chi(Q) = \deg \hat{f} \cdot \chi(P_X) = \deg f \cdot \chi(P_Y),$$

and since $\chi(P_X) = \chi(P_Y) = (-1)^g$ by Corollary 1, we get

COROLLARY 4. *For an isogeny* $f: X \to Y$ *of abelian varieties,*

$$\deg f = \deg \hat{f}.$$

COROLLARY 5. *For every line bundle* L *on* X, *the set-theoretic homomorphism* $\phi_L : X \to \operatorname{Pic}^0 X \approx \hat{X}$ *is a morphism, and* $K(L)$, *with its scheme structure as above, is its kernel.*

PROOF. In fact, ϕ_L is the unique morphism from X to $\hat{X}$ such that

$$(\phi_L \times 1_X)^* P \simeq m^* L \otimes p_1^* L^{-1} \otimes p_2^* L^{-1}.$$

Now by definition $K(L)$ is the largest subscheme S of X such that the bundle on the right is trivial on $S \times X$; and in view of the Universal Mapping Property of X, $\ker(\phi_L)$ is the largest subscheme S of X such that the bundle on the left is trivial on $S \times X$.

SYMMETRIC DEFINITION OF $\hat{X}$.

We wish to set up the relations between X and $\hat{X}$ in an obviously symmetric way. Define a *divisorial correspondence* between two abelian varieties X, Y of the same dimension to be a line bundle on $X \times Y$ whose restrictions to $\{0\} \times Y$ and $X \times \{0\}$ are trivial.

PROPOSITION. *For a divisorial correspondence* Q *between* X *and* Y, *the following are equivalent.*

(a) *There is no subscheme* Z *of* X *different from* (0) *such that the restriction of* Q *to* $Z \times Y$ *is trivial.*

(b) *There is no subscheme* Z' *of* Y *different from* (0) *such that* Q *restricted to* $X \times Z'$ *is trivial.*

(c) *The absolute value of* $\chi(Q)$ *is* 1.

When these conditions hold, Y *is canonically isomorphic to the dual of* X, *and* X *is canonically isomorphic to the dual of* Y.

PROOF. By symmetry, it suffices to show that (b) $\Longleftrightarrow$ (c). Now, we get a morphism $f: Y \longrightarrow \hat{X}$ such that $(1_X \times f)^*(P) = Q$. Now, f

has to be a homomorphism since $f(0) = 0$. Clearly, (b) is equivalent to saying that f has trivial kernel. If this holds, then since dim $Y =$ dim $X =$ dim $\hat{X}$, f is an isogeny, hence by Corollary 1, §12, f is an isomorphism. Thus we have to show that f is an isomorphism if and only if $|\chi(Q)| = 1$. By Theorem 2 of §12, if f is an isogeny,

$$|\chi(Q)| = (\deg f).|\chi(P)| = \deg f$$

and the result follows. On the other hand, if f has positive dimensional kernel we can choose a finite subgroup $F \subset \ker(f)$ of arbitrarily large order d. The map $1_X \times f: X \times Y \longrightarrow X \times \hat{X}$ factors as

$$X \times Y \longrightarrow X \times Y/F \longrightarrow X \times \hat{X},$$

so that Q is the pull-back of a line bundle on $X \times Y/F$. Therefore $d \mid |\chi(Q)|$ by Theorem 2, §12, and since this holds for arbitrarily large d, $\chi(Q) = 0$.

COROLLARY. (The duality hypothesis.) *For any abelian variety X, the canonical morphism $i: X \to \hat{\hat{X}}$ defined by the Poincaré bundle P on $X \times \hat{X}$ (regarded as a family of line bundles on $\hat{X}$ parametrized by X) is an isomorphism.*

PROOF. In fact, the divisorial correspondence P on $X \times \hat{X}$ fulfils (b) (or (c)), hence also (a).

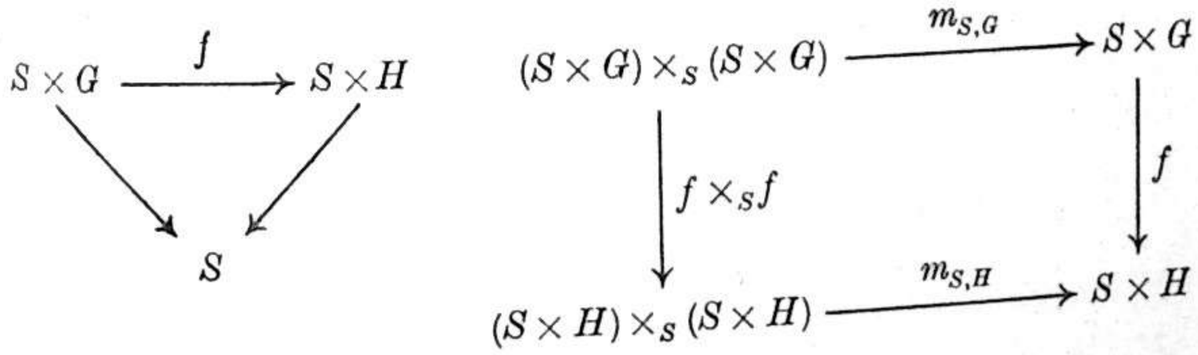
14. Duality Theory of Finite Commutative Group Schemes. Throughout this section, the ground field k is assumed algebraically closed, of positive characteristic $p > 0$.

Let G be a finite commutative group scheme, so that G is affine, hence $G = \text{Spec}\,(R)$, where R is a finite-dimensional k-algebra. The group law gives us a map $\mu: R \to R \otimes_k R$, the inverse gives us a map $i: R \to R$, and evaluation at the identity e gives us an augmentation $\delta: R \to k$. In the present case, the hyperalgebra $\mathbf{H}$ of G is simply the dual vector space R^* of R, and we will use the notation R^* instead of $\mathbf{H}$. As in §11, the group law μ dualizes to an associative multiplication

$$\mu^*: R^* \otimes_k R^* \longrightarrow R^*.$$

Since G is commutative, μ is co-commutative and so μ^* is commutative i.e. R^* is also a finite-dimensional commutative k-algebra. As in §11, the linear functional δ is the identity element of R^*. On the other hand, if $m: R \otimes_k R \to R$ is the multiplication of R, then $m^*: R^* \to R^* \otimes_k R^*$ will be a co-associative, co-commutative map. Together with the dual $i^*: R^* \to R^*$ of i, we get a group law and an inverse making the scheme $\hat{G} = \text{Spec}\ R^*$ into a second finite commutative group scheme. The identity *point* of $\hat{G}$ corresponds to the homomorphism $R^* \to k$ gotten by evaluating linear functionals at $1 \in R$. Thus, to every finite commutative group scheme G we have associated in a canonical fashion another finite commutative group scheme $\hat{G}$, which we shall call the dual of G. This construction is due to Cartier. We shall now give a more 'geometric' definition (cf. Oort [O]).

For group schemes G and H and any scheme S, let $\text{Hom}_S(G, H)$ denote the set of morphisms $f: S \times G \to S \times H$ such that the diagrams



are commutative, where $m_{S,G}$ and $m_{S,H}$ are the multiplications of G and H lifted to $S \times G$ and $S \times H$ respectively. Such morphisms f will be called S-homomorphisms from G to H. One checks easily that if H is commutative, $\text{Hom}_S(G, H)$ can be made into a commutative group by defining $f + g = m_{S,H} \circ (f, g)$. Given a morphism $T \to S$, we have an associated homomorphism $\text{Hom}_S(G, H) \to \text{Hom}_T(G, H)$

given by $f \longmapsto f \times_S T$, so that for given G, H, we get a functor $\underline{\mathrm{Sch}} \to \underline{\mathrm{Sets}}$ given by $S \longmapsto \mathrm{Hom}_S(G, H)$, and this is in fact a commutative group-valued functor when H is commutative.

Now suppose $G = \mathrm{Spec}\ A$ is a finite commutative group scheme and H the multiplicative group scheme $\mathbf{G}_m$. We then assert that the functor $\underline{\mathrm{Sch}} \to \underline{\mathrm{Ab}}$, $S \longmapsto \mathrm{Hom}_S(G, \mathbf{G}_m)$ is represented by $\hat{G}$, that is, there is for each S an isomorphism

$$\underline{\hat{G}}(S) \simeq \mathrm{Hom}_S(G, \mathbf{G}_m),$$

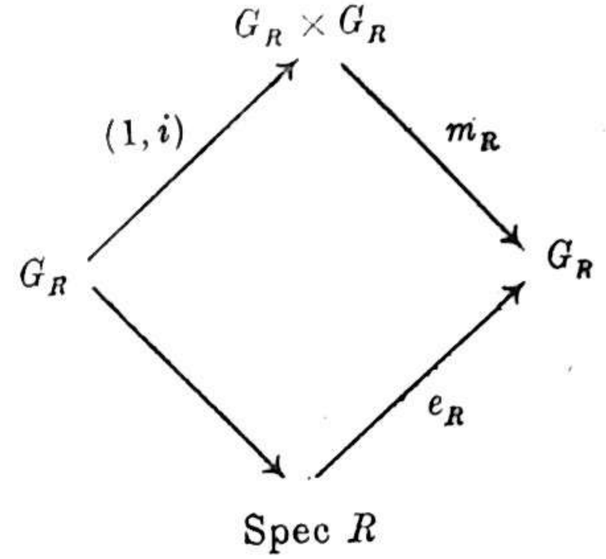
which is functorial in S. Now, if we restrict S to vary in the open subsets of a fixed scheme, it is clear that both sides define sheaves on this scheme. Hence by standard arguments, it suffices to establish the above isomorphism as S varies through affine schemes, $S = \mathrm{Spec}\ R$. Let us denote as usual the objects, morphisms, etc., obtained after base extension to R by a subscript R. Then the coordinate rings of G_R and $\mathbf{G}_{mR}$ become bi-algebras over R, that is, they are algebras with 1 over R, with co-multiplication maps $A_R \to A_R \otimes_R A_R$, etc., satisfying the usual identities, and co-identity maps $A_R \to R$, etc. The notion of homomorphism of bialgebras is then clear. We then have

$$\underline{\hat{G}}(R) = \mathrm{Hom}\,(\mathrm{Spec}\ R, \hat{G}) = \mathrm{Hom}_{k\text{-alg}}(A^*, R) = \mathrm{Hom}_{R\text{-alg}}(R \otimes_k A^*, R)$$
$$= \mathrm{Hom}_{R\text{-alg}}((A_R)^*, R),$$

where $(A_R)^*$ is the R-algebra $\mathrm{Hom}_R(A_R, R)$. Further,

$$\mathrm{Hom}_R(G, \mathbf{G}_m) = \mathrm{Hom}_{R\text{-bialg}}(R[T, T^{-1}], A_R) \xhookrightarrow{i} A_R,$$

where i is the inclusion defined by $i(\phi) = \phi(T)$. Clearly, an element $\alpha \in A_R$ is in the image of i if and only if (i) α is a unit in A_R, and (ii) $\mu_R(\alpha) = \alpha \otimes \alpha$. But in the presence of assumption (ii), (i) is equivalent to (i)′ $\epsilon_R(\alpha) = 1$, where $\epsilon_R : A_R \to R$ is the homomorphism given by the identity. In fact, (i) implies that $\epsilon_R(\alpha)$ is a unit, and on the other hand $(\epsilon_R \otimes \epsilon_R)(\mu_R(\alpha)) = \epsilon_R(\alpha)$, that is, $\epsilon_R(\alpha)^2 = \epsilon_R(\alpha)$, so that $\epsilon_R(\alpha) = 1$; on the other hand, if (i)′ and (ii) hold and $i^* : A_R \to A_R$ is got from the inverse, we have commutativity of the diagram



and taking the pull-back of the function α by these maps, we find $\alpha . i^*(\alpha) = 1$, so that α is a unit. Now, since A_R is R-free of finite rank we have a natural isomorphism

$$A_R \xrightarrow{\sim} \mathrm{Hom}_R((A_R)^*, R)$$

and under this isomorphism, elements α satisfying (i)′ and (ii) go over into element $f \in \mathrm{Hom}_R((A_R)^*, R)$ such that $f(1) = 1$ and $f(XY) = f(X).f(Y)$ for $X, Y \in (A_R)^*$ (since $XY = \mu_R^*(X \otimes Y)$). Thus we have set up a set-theoretic bijection between $\underline{\hat{G}}(R)$ and $\mathrm{Hom}_R(G, \mathbf{G}_m)$ natural in R. We leave it to the reader to check that this is an isomorphism of groups.

In particular, taking $S = \hat{G}$ in the above isomorphism, we get a morphism $\hat{G} \times G \to \mathbf{G}_m$ corresponding to the identity of $\underline{\hat{G}}(\hat{G})$, defined by the homomorphism of k-algebras $k[T, T^{-1}] \to A^* \otimes_k A$, $T \longmapsto \delta$, $\delta =$ the 'diagonal element' of $A^* \otimes_k A$ (which corresponds to $1_A \in \mathrm{Hom}_k(A, A)$ under the natural isomorphism $A^* \otimes_k A \xrightarrow{\sim} \mathrm{Hom}_k(A, A)$). One checks easily from this that this 'universal character' $\hat{G} \times G \to \mathbf{G}_m$ is in fact a bilinear map of group schemes in the obvious sense.

EXAMPLES. (1) Suppose G is a discrete (i.e. reduced) finite group of order n prime to p. By the above, the geometric points of $\hat{G}$ form a group isomorphic to $\mathrm{Hom}(G, k^*)$, which is of order n.

On the other hand, if A is the ring of functions of G, $\dim A = \dim A^* = n$, which shows that $\hat{G}$ is again reduced, and is isomorphic as a discrete group to $\mathrm{Hom}(G, k^*)$.

(2) Next suppose G is reduced and isomorphic to $\mathbf{Z}/p^n\mathbf{Z}$. For any reduced G let $k[G]$ be the group algebra of G. If we identify any $g \in G$ with the linear form $A \to k$ which is evaluation at g, we get an isomorphism of vector spaces $k[G] \xrightarrow{\sim} A^*$, which is trivially seen to be an isomorphism of algebras. Hence $\hat{G}$ has coordinate ring A^* isomorphic to the group algebra of $\mathbf{Z}/p^n\mathbf{Z}$, i.e. $A^* \simeq k(X)/(X^{p^n} - 1)$, where X corresponds to evaluation at the generator $\bar{1} \in \mathbf{Z}/p^n\mathbf{Z}$. On the other hand, for $f, g \in A$, $\bar{1}(f \cdot g) = (fg)(\bar{1}) = f(\bar{1}) \cdot g(\bar{1}) = (\bar{1} \otimes \bar{1})(f \otimes g)$, which shows that the co-multiplication on A^* is given by $X \longmapsto X \otimes X$. Thus we have an isomorphism.

$$\widehat{(\mathbf{Z}/p^n\mathbf{Z})} \simeq \mu_{p^n},$$

hence also

$$\widehat{(\mu_{p^n})} \simeq \mathbf{Z}/p^n\mathbf{Z}.$$

Now, let G be any finite commutative group scheme. We shall say that G is of type l(local) or r(reduced) if the underlying space of G is a single point or if G is reduced respectively. We shall say that G is of type (l, l) (resp. (l, r), (r, l), (r, r)) if G is of type l and $\hat{G}$ is of type l(resp. G of type l, $\hat{G}$ of type r; etc.). We shall show that any group admits a unique decomposition as a product

$$G = G_{r,r} \times G_{r,l} \times G_{l,r} \times G_{l,l}$$

of groups of the indicated types. In fact, if G^0 is the connected component of identity in G, considered as an open and closed subscheme, and if G_{red} is the reduced group, the closed immersions $G^0 \hookrightarrow G$ and $G_{\mathrm{red}} \hookrightarrow G$ induce a homomorphism $G^0 \times G_{\mathrm{red}} \to G$ which is clearly an isomorphism. Further, this decomposition of G into the product of a reduced and a local group is clearly unique. Thus, it suffices to show that each local (resp. reduced) group is uniquely expressible as a product $G_{lr} \times G_{ll}$ (resp. $G_{rr} \times G_{rl}$). Now, if G is reduced, G is uniquely expressible as a product $G_1 \times G_2$ where G_1 is of order prime to p and G_2 is a p-group. By the above, $\hat{G}_1$ is again reduced and $\hat{G}_2$ is local, which proves the assertion for reduced groups. When G is local, split $\hat{G}$ into its local and reduced parts. Dualizing back, this implies a unique decomposition of a local G into groups of type (l, r) and (l, l) respectively. This proves the assertion for local groups.

It follows from our discussion that the only groups of type (r, r) are those reduced groups of orders prime to p, hence direct products of cyclic prime power groups, the primes being distinct from p; that the only groups of type (r, l) are p-groups, hence direct products of $\mathbf{Z}/p^{n_i}\mathbf{Z}$'s; and that the only groups of type (l, r) are duals of p-groups, hence direct products of $\mu_{p^{n_i}}$'s.

There are plenty of examples of local-local groups. For instance, the groups α_{p^n} are local-local. In fact, since Spec $\dfrac{k[X]}{(X^{p^n})}$ cannot be decomposed as a product (the tangent space being one-dimensional), it suffices to see that it is not isomorphic to μ_{p^n}. Since α_p is a quotient of α_{p^n}, it even suffices to see that α_p is not isomorphic to μ_p. But now, if ξ is the linear form on $A = k[X]/(X^p)$ defined by

$$\xi(x^i) = \begin{cases} 0 \text{ if } i \neq p-1 \\ 1 \text{ if } i = p-1 \end{cases} \quad \text{in } A^*,$$

we have $\xi^2(X^i) = (\xi \otimes \xi)((1 \otimes X + X \otimes 1)^i) = 0$ if $i < p - 1$, which shows that A^* has nilpotent elements.

So far we have developed the circle of ideas involving homomorphisms from G to $\mathbf{G}_m$. Next we turn to homomorphisms from G to $\mathbf{G}_a$ and related results. We fix the notations $G = \mathrm{Spec}\ R$, $\hat{G} = \mathrm{Spec}\ R^*$ as above and we let roman letters $x, y, \ldots$ be elements of R; greek letters $\alpha, \beta, \ldots$ be elements of R^*. Let s and s^* be the co-multiplications in R and R^* respectively. We recall that in §11, we saw how R^* operated naturally on the sheaf $\mathcal{O}_G$. In our affine case, this means that there is a natural inclusion

$$R^* \hookrightarrow \mathrm{Hom}_k(R, R).$$

Explicitly, if $\alpha: R \to k$ is an element of R^*, we get a map $D_\alpha: R \to R$ by the composition

$$R \xrightarrow{s} R \otimes_k R \xrightarrow{1 \otimes \alpha} R.$$

In particular, if $\alpha(1) = 0$, $\alpha(\mathfrak{M}_e^2) = (0)$, then D_α is derivation of R over k. The operators D_α are all translation-invariant in the usual sense. Moreover the transposed maps $D_\alpha^*: R^* \to R^*$ are just the compositions

$$\beta \otimes \alpha \longleftarrow \beta$$

$$R^* \xleftarrow{\text{mult.}} R^* \otimes_k R^* \longleftarrow R^*$$

i.e. the maps $\beta \longmapsto \alpha.\beta$, multiplication by α.

As an application, we can interpret $\mathrm{Hom}(\hat{G}, \mathbf{G}_a)$ in a new way:

$$\mathrm{Hom}_{\text{Gp.Sch.}}(\hat{G}, \mathbf{G}_a) \cong \mathrm{Hom}_{\text{bi-algebra}}(k[X], R^*)$$
$$\cong \{\alpha \in R^* \mid s^*\alpha = \alpha \otimes 1 + 1 \otimes \alpha\}$$

(since a homomorphism ϕ from $k[X]$ to R^* is determined by the image $\alpha = \phi(X)$, and ϕ is compatible with co-multiplication if and only if $s^*\alpha = \alpha \otimes 1 + 1 \otimes \alpha$). Such α's are called *primitive* elements of R^*. If we associate to any $\alpha \in R^*$ the map D_α which is the transpose of multiplication by α, we see that primitive elements correspond precisely to invariant derivations of R:

$$\left\{\alpha \in R^* \,\middle|\, s^*\alpha = \alpha \otimes 1 + 1 \otimes \alpha\right\} \cong \left\{D: R \longrightarrow R \,\middle|\, D \text{ an invariant derivation}\right\}$$
$$\cong \mathrm{Lie}(G).$$

The conclusion is that

$$\mathrm{Hom}(\hat{G}, \mathbf{G}_a) \cong \mathrm{Lie}(G).$$

Moreover, the p^{th} power operation in $\mathrm{Lie}(G)$ is obtained by taking D to $\overbrace{D \circ \ldots \circ D}^{p\text{x}}$, which corresponds to raising α to its p^{th} power, which corresponds to composing a map $\phi: \hat{G} \to \mathbf{G}_a$ with the Frobenius $F: \mathbf{G}_a \to \mathbf{G}_a$ (since $F^*(X) = X^p$).

Now look at the following type of group.

DEFINITION. *A group scheme G is of height one if it consists of a single point e, and if $x^p = 0$, for all $x \in \mathfrak{M}_e$.* (*G need not be commutative.*)

It is easy to see that, *as schemes*, such groups G are isomorphic to $\mathrm{Spec}(k[X_1, \ldots, X_n]/(X_1^p, \ldots, X_n^p))$. In fact, choosing $X_1, \ldots, X_n \in \mathfrak{M}_e$ which induce a basis of $\mathfrak{M}_e/\mathfrak{M}_e^2$, and letting $R = \Gamma(\mathcal{O}_G)$, we find that R is a quotient of $k[X_1, \ldots, X_n]/(X_1^p, \ldots, X_n^p)$. On the other hand, if we use the fact that R admits derivations $D_i: R \to R$ such that $D_i(X_j) \equiv \delta_{ij} \pmod{\mathfrak{M}_e}$, then it is easy to see that there can be no relation of linear dependence over k among the monomials

$$\prod_{i=1}^{n} X_i^{a_i}, \quad 0 \leqslant a_i < p.$$

We have already seen in §11 that any group scheme G has a maximal subgroup scheme $G^{(p)} \subset G$ of height one, having the same Lie algebra as G. Then the analog in characteristic $p > 0$ of the classical equivalence of categories between Lie algebras and germs of Lie groups is the following

THEOREM. *The functor $G \longmapsto \mathrm{Lie}\, G$ sets up an equivalence of the categories of finite group schemes of height one and finite-dimensional p-Lie algebras over k (i.e. a finite-dimensional vector space with bracket and p^{th} power map, as in* §11).

We shall prove this only for commutative G, which correspond to p-Lie algebras with trivial bracket.

PROOF. For any k-vector space $\mathfrak{g}$ with a p-linear map $\alpha \to \alpha^{(p)}$, let $U(\mathfrak{g})$ be the k-algebra $S(\mathfrak{g})/I$, where I is the ideal generated in the symmetric algebra $S(\mathfrak{g})$ of $\mathfrak{g}$ by elements of the form $\alpha^{(p)} - \alpha^p, \alpha \in \mathfrak{g}$. Note that if $\alpha_1, \ldots, \alpha_n$ are a basis of $\mathfrak{g}$, then $\prod_{i=1}^{n} \alpha_i^{r_i}, 0 \leqslant r_i < p$ are a basis of $U(\mathfrak{g})$. Define a co-multiplication $s: U(\mathfrak{g}) \to U(\mathfrak{g}) \otimes_k U(\mathfrak{g})$ by putting for $\alpha \in \mathfrak{g}$, $s\alpha = 1 \otimes \alpha + \alpha \otimes 1$ (check that this goes down to $U(\mathfrak{g})$). It is easily verified that $U(\mathfrak{g})$ is a commutative finite-dimensional bialgebra, and is a covariant functor in $\mathfrak{g}$.

Put $R(\mathfrak{g}) = U(\mathfrak{g})^*$, and $G(\mathfrak{g}) = \mathrm{Spec} U(\mathfrak{g})^*$, considered as a group scheme.

We shall prove that the two functors

$$G \longmapsto \mathrm{Lie}\ G$$

$$\mathfrak{g} \longmapsto G(\mathfrak{g})$$

are inverses of each other.

We prove first that for any vector space $\mathfrak{g}$ with a p-linear map, $G(\mathfrak{g})$ is of height one and there is a natural isomorphism $\mathfrak{g} \xrightarrow{\approx} \mathrm{Lie}\, G(\mathfrak{g})$. Now, we have a natural inclusion $\mathfrak{g} \hookrightarrow U(\mathfrak{g})$ of $\mathfrak{g}$ into the primitive elements of $U(\mathfrak{g})$, which gives an injection $\mathfrak{g} \hookrightarrow \mathrm{Lie}\, G(\mathfrak{g})$. To show that $G(\mathfrak{g})$ is of height one, it suffices to show that for $x \in R(\mathfrak{g})$ belonging to the maximal ideal of 0 in $G(\mathfrak{g})$, $x^p = 0$. If we identify $U(\mathfrak{g})$ with a subalgebra of $\mathrm{End}_k R(\mathfrak{g})$ via D, it will suffice to show that if $\alpha \in U(\mathfrak{g})$, $D_\alpha(x^p) = 0$. Since $U(\mathfrak{g})$ is generated by $\mathfrak{g}$, it even suffices to show that for $\alpha \in \mathfrak{g}$, $D_\alpha(x^p) = 0$, which is clear since D_α is a derivation. It only remains to show that $\mathfrak{g} \to \mathrm{Lie}\, G(\mathfrak{g})$ is surjective. But if $n = \dim_k(\mathfrak{g})$, $m = \dim_k \mathrm{Lie}\, G(\mathfrak{g})$, then by our remarks on a basis of $U(\mathfrak{g})$, $p^n = \dim_k U(\mathfrak{g})$, and by our remarks on the structure of $\Gamma(\mathcal{O}_{G(\mathfrak{g})})$, $p^m = \dim_k R(\mathfrak{g})$. Thus $n = m$, so $\mathfrak{g} \xrightarrow{\sim} \mathrm{Lie}\, G(\mathfrak{g})$.

Secondly, let G be a commutative group scheme of height one with coordinate ring R. Let ϕ: $\mathrm{Lie}(G) \to R^*$ be the usual inclusion map. We have seen in §11 that $\phi(\alpha^{(p)}) = \phi(\alpha)^p$, so ϕ extends to a homomorphism

$$\tilde{\phi}\colon U(\mathrm{Lie}\ G) \longrightarrow R^*.$$

Since for $\alpha \in \mathrm{Lie}\,(G)$, α and $\phi(\alpha)$ are primitive with respect to the co-multiplication in $U(\mathrm{Lie}\, G)$ and R^* resp., $\tilde{\phi}$ is a homomorphism of bi-algebras. The transpose of $\tilde{\phi}$ is again a homomorphism of bi-algebras

$$\tilde{\phi}^*\colon R \longrightarrow R(\mathrm{Lie}\ G)$$

and passing to the Spec's, we obtain a homomorphism of group schemes:

$$\phi'\colon G(\mathrm{Lie}\ G) \longrightarrow G.$$

By the first part of the proof, Lie G is the Lie algebra of $G(\mathrm{Lie}\ G)$ and it follows from our construction that the differential of ϕ' induces an isomorphism from the Lie algebra of $G(\mathrm{Lie}\ G)$ to that of G. Now by Nakayama's lemma, any morphism $f\colon X \to Y$ of schemes with one point each, whose differential is injective, is a closed immersion. This applies to ϕ'; in other words, $\tilde{\phi}^*$ is surjective. But if $n = \dim_k \mathrm{Lie}\ G$, then $p^n = \dim_k R = \dim_k R(\mathrm{Lie}\ G)$. Therefore $\tilde{\phi}^*$ and ϕ' are both isomorphisms.

COROLLARY. *If G is a commutative group scheme of height one, the homomorphism p_G (mult. by p in G) is zero.*

PROOF. In fact, multiplication by p kills Lie G, so the result follows from the Theorem.

If $G = \mathrm{Spec}\ R$ is a group scheme of height one, then not only is its structure as a group determined by its p-Lie algebra but also to give an action of G on a scheme X is equivalent to giving an action of Lie G on X, i.e. a k-linear map $\alpha \longmapsto D_\alpha$ from Lie G to derivations $D_\alpha : \mathcal{O}_X \to \mathcal{O}_X$ such that

(i) $[D_\alpha, D_\beta] = 0$, all $\alpha, \beta \in \mathrm{Lie}\ G$,

(ii) $D_{\alpha(p)} = (D_\alpha)^p$, all $\alpha \in \mathrm{Lie}\ G$.

We can see this in several steps.

(I) To give a map $\alpha \longmapsto D_\alpha$ as above is equivalent to giving a homomorphism of algebras:

$$D\colon U(\mathrm{Lie}\ G) \longrightarrow \mathrm{Diff}(\mathcal{O}_X),$$

where $\mathrm{Diff}(\mathcal{O}_X)$ is the algebra of differential operators on $\mathcal{O}_X$, such that D carries Lie G into derivations.

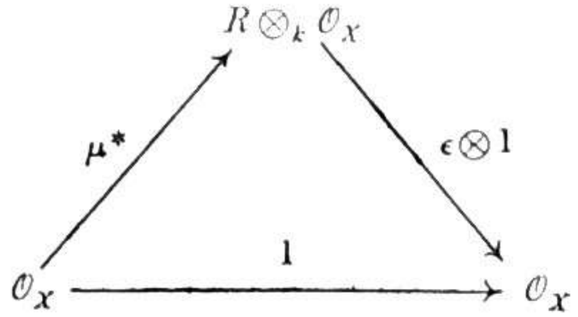
(II) Interpreting D as a map

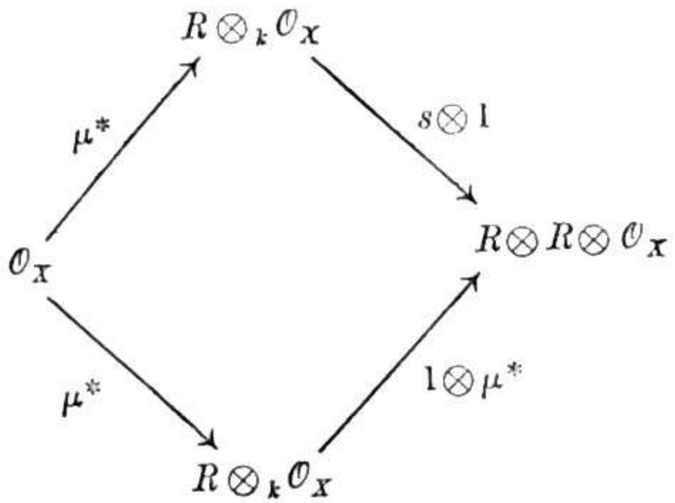
$$\tilde{D}\colon U(\mathrm{Lie}\ G) \otimes_k \mathcal{O}_X \longrightarrow \mathcal{O}_X,$$

and using the fact that the coordinate ring R is the dual of $U(\mathrm{Lie}\ G)$, we see that to give $\widetilde{D}$ is equivalent to giving a transposed map

$$\mu^* : \mathcal{O}_X \longrightarrow R \otimes_k \mathcal{O}_X.$$

The condition that $D(1) = 1$ and $D_{\alpha\beta} = D_\alpha \circ D_\beta$ translate easily into the conditions that





commute. It can also be checked that the condition that D take Lie G to derivations, i.e. D commutes with co-multiplication, means that μ^* is a homomorphism of algebras.

(III) To give a homomorphism μ^* is the same as giving a morphism $\mu: G \times X \to X$ and the two commutative diagrams with μ^* say exactly that μ is an action of G on X.

Finally, let us look at the decomposition into pieces of a commutative finite group scheme G of height one. We get

(*) $$G = G_{l,r} \times G_{l,l}$$

and both $G_{l,r}$ and $G_{l,l}$ are again of height one. Since $G_{l,r}$ is killed by p,

$$G_{l,r} \simeq \mu_p^n$$

for some n. We have seen that Lie (μ_p) is one-dimensional with a generator e such that $e^{(p)} = e$. Now the decomposition (*) induces a decomposition

(**) $$\mathrm{Lie}\ G = \mathrm{Lie}\ G_{l,r} \oplus \mathrm{Lie}\ G_{l,l} = \mathfrak{g}_1 \oplus \mathfrak{g}_2.$$

It follows that $\mathfrak{g}_1$ has a basis $e_1, \ldots, e_n$ such that $e_i^{(p)} = e_i$. On the other hand, since $\widehat{G}_{l,l}$ is again local, and $\mathfrak{g}_2$ is contained in the maximal ideal of $\Gamma(\mathcal{O}_{\widehat{G}_{l,l}})$, it follows that for all $\alpha \in \mathfrak{g}_2$, $\alpha^{(p^n)} = 0$ for n large. In view of the theorem, we deduce a corollary in "p-linear" algebra:

COROLLARY. *If V is any vector space with a p-linear map $x \longmapsto x^{(p)}$, there is a unique decomposition, invariant under $x \longmapsto x^{(p)}$:*

$$V = V_s \oplus V_n,$$

such that V_s has a basis $x_1, \ldots, x_k$ for which $x_i^{(p)} = x_i$, and such that $x \to x^{(p)}$ is a nilpotent map on V_n.

V_s and V_n are called the semi-simple and nilpotent subspaces of V respectively, and in the case of Lie G, *we have:*

$$(\mathrm{Lie}\ G)_s = \mathrm{Lie}\ G_{l,r}$$
$$(\mathrm{Lie}\ G)_n = \mathrm{Lie}\ G_{l,l}.$$

15. Applications to Abelian Varieties.

THEOREM 1. *Let f: $X \to Y$ be an isogeny of abelian varieties, with kernel K. Let $\widehat{f}$: $\widehat{Y} \to \widehat{X}$ be the dual map, with kernel K'. Then there is a canonical isomorphism of K' with the dual $\widehat{K}$ of K.*

PROOF. If L is any line bundle on Y and $x \in X$, then $\phi_{f^*L}(x) \in \widehat{X}$ represents the line bundle $T_x^*(f^*L) \otimes f^*L^{-1}$, and since

$$T_x^*(f^*L) \otimes (f^*L)^{-1} \simeq f^*[T_{fx}^* L \otimes L^{-1}]$$

it follows that

$$\phi_{f^*L}(x) = \widehat{f}(\phi_L(f(x))).$$

In particular, if ϕ_{f^*L} is the zero map, then ϕ_L must be the zero map too; i.e. $f^*L \in \mathrm{Pic}^0 Y \Rightarrow L \in \mathrm{Pic}^0 X$. It follows then that for any scheme S, we have natural isomorphisms:

$$\underline{K}'(S) \simeq \mathrm{Ker}\,[\mathrm{Hom}\,(S, \widehat{Y}) \to \mathrm{Hom}\,(S, \widehat{X})]$$

$$\simeq \mathrm{Ker} \left\{ \left[\begin{array}{l} \text{line bundles on} \\ S \times Y, \text{ trivial on} \\ S \times (0) \end{array} \right] \longrightarrow \left[\begin{array}{l} \text{line bundles on} \\ S \times X, \text{ trivial on} \\ S \times (0) \end{array} \right] \right\}$$

$$\simeq \mathrm{Ker} \left[\left(\begin{array}{l} \text{line bundles on} \\ S \times Y \end{array} \right) \longrightarrow \left(\begin{array}{l} \text{line bundles on} \\ S \times X \end{array} \right) \right].$$

The last isomorphism is correct because if a line bundle on $S \times Y$ becomes trivial on $S \times X$, then it must also be trivial on $S \times (0)$. But now $S \times Y$ is the quotient of $S \times X$ for the free action of K. Thus according to the results in §12, there is a natural isomorphism:

$$\mathrm{Ker} \left[\left(\begin{array}{l} \text{line bundles} \\ \text{on } S \times Y \end{array} \right) \longrightarrow \left(\begin{array}{l} \text{line bundles} \\ \text{on } S \times X \end{array} \right) \right] \simeq \left[\begin{array}{l} \text{Liftings of the} \\ \text{action of } K \text{ on} \\ S \times X \text{ to actions} \\ \text{on } S \times X \times \mathbf{A}^1 \end{array} \right].$$

Now an action of K on $S \times X \times \mathbf{A}^1$ is defined by a morphism μ fitting into a diagram:

$$\begin{array}{ccc} K \times S \times X \times \mathbf{A}^1 & \xrightarrow{\mu} & S \times X \times \mathbf{A}^1 \\ \downarrow{\scriptstyle p_{123}} & & \downarrow{\scriptstyle p_{12}} \\ K \times S \times X & \xrightarrow{\mu_0} & S \times X \end{array}$$

where μ_0 is the translation action of K on X, with S thrown in. If $\lambda = p_3 \circ \mu$ is the induced morphism from $K \times S \times X \times \mathbf{A}^1$ to $\mathbf{A}^1$, then in terms of T-valued points, the lifted action can be described as

$$k\colon (s, x, \alpha) \longmapsto (s, x+k, \lambda(k, s, x, \alpha)),$$

$k \in \underline{K}(T)$, $s \in \underline{S}(T)$, $x \in \underline{X}(T)$, $\alpha \in \underline{\mathbf{A}}^1(T)$. Since the action should be *linear* on $\mathbf{A}^1$,

$$\lambda(k, s, x, \alpha) = \alpha . \lambda(k, s, x, 1).$$

Since X is a complete variety, for any scheme W, $\Gamma(\mathcal{O}_{W \times X}) \simeq \Gamma(\mathcal{O}_W)$, hence all morphisms $W \times X \to \mathbf{A}^1$ factor through W. In particular, λ does not depend on the factor x in X. Thus the action is given by

$$k : (s, x, \alpha) \longmapsto (s, x + k, \lambda(k, s, 0, 1) . \alpha).$$

To be an action, we need

$$\lambda(k_1 + k_2, s, 0, 1) = \lambda(k_1, s, 0, 1) . \lambda(k_2, s, 0, 1)$$

$$\lambda(0, s, 0, 1) = 1.$$

In other words, λ is given by an S-homomorphism $\chi\colon K \times S \to \mathbf{G}_m$. Conversely, any such χ defines an action μ via

$$\mu(k, s, x, \alpha) = (s, x + k, \chi(k, s) . \alpha).$$

Therefore,

$$\left[\begin{array}{l} \text{Liftings of the action of } K \text{ on } S \times X \\ \text{to actions on } S \times X \times \mathbf{A}^1 \end{array} \right] \simeq \mathrm{Hom}_S(K, \mathbf{G}_m) \simeq \underline{\widehat{K}}(S).$$

Putting all this together, $K' \simeq \widehat{K}$.

DEFINITION. *An isogeny $f : X \to Y$ of abelian varieties is said to be of height one if, denoting by $k(Y)$ and $k(X)$ the respective function fields, we have $k(X)^p \subset k(Y)$.*

We shall show that f is of height one if and only if $\ker f$ is a group scheme of height one. In fact, assume f is of height one. $\mathcal{O}_{X,0}$ is the integral closure of $\mathcal{O}_{Y,0}$ in $k(X)$ and $\mathcal{O}_{Y,0}$ is integrally closed. Therefore $\mathcal{O}_{Y,0} = \mathcal{O}_{X,0} \cap k(Y) \supset \{f^p \mid f \in \mathcal{O}_{X,0}\}$, hence $\mathfrak{M}_{Y,0} \supset \{f^p \mid f \in \mathfrak{M}_{X,0}\}$. Since $\ker f \simeq \mathrm{Spec}\,(\mathcal{O}_{X,0}/\mathfrak{M}_{Y,0} \cdot \mathcal{O}_{X,0})$, this shows that $\ker f$ is of height one. Conversely, suppose $K = \ker f$ is of height one, and let R^* be the bialgebra of $\widehat{K}$. Let U be any non-void affine open subset of X with coordinate ring A. The action of K on U is given by a homomorphism of R^* into the algebra of differential operators on A, such that a set of generators of R^* gets mapped into vector fields on U. The elements of A invariant under the

action of K therefore consist precisely of those elements of A which are killed by these derivations; in particular they contain $A^{(p)} = \{f^p \mid f \in A\}$. This proves that $k(X)^p \subset k(Y)$.

THEOREM 2. *For all abelian varieties X, there is a one-one correspondence between isogenies $f: X \to Y$ of height one (up to isomorphism) and sub p-Lie algebras of* Lie X.

PROOF. In fact, isogenies of height one are uniquely determined up to an isomorphism by their kernels, which are subgroup-schemes of height one, or what is the same, subgroup-schemes of the maximal height one subgroup-scheme $X_p = \mathrm{Spec}(\mathcal{O}_{X,0}/\mathfrak{M}_{X,0}^{(p)})$. But by an earlier theorem, subgroup-schemes of X_p are in natural one-one correspondence with p-Lie subalgebras of Lie $X_p = \mathrm{Lie}\, X$.

EXAMPLE. The above theorem enables us to give an example of an abelian variety X admitting an infinity of distinct isogenies $X \to Y$ of height one.

In fact, for every prime $p > 0$, there is an elliptic curve E, unique up to isogeny, such that the p^{th} power map in Lie X is 0 (Deuring; cf. §21). But if E is such a curve, and $X = E \times E$, any 1-dimensional subspace of Lie X is stable for the p^{th} power map, and hence defines an isogeny of height one.

THE p-RANK.

Let X be an abelian variety of dimension g in characteristic $p > 0$, and $n = p^r \cdot m$ an integer > 0, $r \geqslant 0$, $m \geqslant 1$, $(p, m) = 1$. We want to analyze the structure of the finite group *scheme* $X_n = \ker n_X$. Now, X_m and X_{p^r} are subgroup schemes of X_n, and we have a homomorphism $X_m \times X_{p^r} \to X_n$. This is, in fact, an isomorphism since X_m is the (r, r)-part of X_n, and X_{p^r} is the product of the (r, l), (l, r) and (l, l)-parts of X_n. As we saw in §6, X_m is a discrete reduced group isomorphic to $(\mathbf{Z}/m\mathbf{Z})^{2g}$. Thus, it suffices to study the structure of X_{p^n}, which we rename G_n. Suppose now that $(G_1)_{\text{red}} = (\mathbf{Z}/p\mathbf{Z})^r$. Since X is divisible, for any $n \geqslant 1$, we have an exact sequence $0 \to G_{1,\text{red}} \to G_{n+1,\text{red}} \xrightarrow{p} G_{n,\text{red}} \to 0$,

and one deduces by induction that for any $n \geqslant 1$, $(G_n)_{\text{red}} = (\mathbf{Z}/p^n\mathbf{Z})^r$. Now, by Theorem 1 of this section, $\hat{G}_n$ is the kernel of $(p^n)_{\hat{X}}$, so it follows that there is an integer s such that for any $n \geqslant 0$, $(\hat{G}_n)_{\text{red}} = (\mathbf{Z}/p^n\mathbf{Z})^s$. Thus, the decomposition of G_n into its pieces is as follows:

$$G_n = (\mathbf{Z}/p^n\mathbf{Z})^r \times (\mathbf{Z}/\widehat{p^n\mathbf{Z}})^s \times G_n^0$$
$$= (\mathbf{Z}/p^n\mathbf{Z})^r \times \mu_{p^n}^s \times G_n^0,$$

where G_n^0 is local-local. Since G_n is of order p^{2ng}, we deduce that there is an integer $t \geqslant 0$ such that $r + s + t = 2g$, and G_n^0 is of order p^{nt}.

We shall show that the integers $r = r_X$, $s = s_X$ and $t = t_X$ are the same for isogenous abelian varieties. It suffices to prove this for r and s, since $r+s+t=2g$. Further, since $s_X = r_{\hat{X}}$, it even suffices to verify this for r. Let $f: X \to Y$ be an isogeny, with kernel of order k. Since $f(X_{p^n}) \subseteq Y_{p^n}$, we have that the order of $(X_{p^n})_{\text{red}}$ is at most k times that of $(Y^{p^n})_{\text{red}}$, that is, $p^{nr_X} \leqslant k \cdot p^{nr_Y}$ for all n, hence $r_X \leqslant r_Y$. Now, $\ker f$ is a finite group scheme, hence is annihilated by an $N > 0$, which shows that $\ker N_X \supset \ker f$. Therefore, N_X factorizes as $X \xrightarrow{f} Y \xrightarrow{g} X$. Thus, $Y \xrightarrow{g} X$ is an isogeny, and $r_Y \leqslant r_X$. This proves that r, s and t are isogeny invariant. In particular, since for any abelian variety X, X and $\hat{X}$ are isogenous, we deduce that $r_X = r_{\hat{X}} = s_X$. Thus, we have that

$$G_n = (\mathbf{Z}/p^n\mathbf{Z})^r \times (\mu_{p^n})^r \times G_n^0$$

with G_n^0 local-local of order p^{nt}, $2r + t = 2g$. In particular, we see that $r \leqslant g$. The integer r is called the *p-rank* of X, and is an isogeny invariant.

Now, since p_X induces the 0-map on Lie algebras, we see that Lie $X = \mathrm{Lie}\,(\ker p_X) = \mathrm{Lie}\, G_1 = \mathrm{Lie}\,(\mu_p)^r \oplus \mathrm{Lie}\, G_1^0$. Since G_1^0 is local-local, the p^{th} power map on $\mathrm{Lie}\, G_1^0$ is nilpotent, whereas $\mathrm{Lie}(\mu_p)^r$ admits a basis $e_1, \ldots, e_r$ such that $e_i^p = e_i$. We thus see

that the p-rank of X equals the dimension of the semi-simple part of Lie X with respect to the p^{th} power map. The same result holds for Lie $\hat{X}$, since X and $\hat{X}$ have the same p-rank. On the other hand, we have established a canonical isomorphism Lie $\hat{X} \simeq H^1(X, \mathcal{O}_X)$. Let $F: \mathcal{O}_X \to \mathcal{O}_X$ be the Frobenius homomorphism $F(\alpha) = \alpha^p$, and denote the induced p-linear map $H^1(X, \mathcal{O}_X) \to H^1(X, \mathcal{O}_X)$ again by F. We shall establish that under the isomorphism Lie $\hat{X} \simeq H^1(X, \mathcal{O}_X)$, the p^{th} power map in Lie X goes over into F. It follows that the p-rank of X is also the dimension of the semi-simple part of $H^1(X, \mathcal{O}_X)$ with respect to the Frobenius map F. Thus, we need to prove

THEOREM 3. *Under the natural isomorphism* Lie $\hat{X} \simeq H^1(X, \mathcal{O}_X)$, *the p^{th} power operation in* Lie $\hat{X}$ *goes over into the Frobenius map in* $H^1(X, \mathcal{O}_X)$.

PROOF. First we give a description of the p^{th} power operation on vector fields on a scheme X, using the functor $\underline{X}$, analogous to the one given for the Poisson bracket in §11. Let D be a vector field, interpreted now as an automorphism of $X \times \operatorname{Spec} \Lambda$ over $\operatorname{Spec} \Lambda$, where $\Lambda = \dfrac{k[\epsilon]}{(\epsilon^2)}$, which is the identity on the closed fibre $X \hookrightarrow X \times \operatorname{Spec} \Lambda$.

Let $M = k[\epsilon_1, \ldots, \epsilon_p]/(\epsilon_1^2, \ldots, \epsilon_p^2)$, and let $\eta_i : \Lambda \to M$ be the k-algebra homomorphisms defined by $\eta_i(\epsilon) = \epsilon_i$ and let $\phi_i = \operatorname{Spec} \eta_i : \operatorname{Spec} M \to \operatorname{Spec} \Lambda$. By base change using ϕ_i, D induces an automorphism D_i of $X \times \operatorname{Spec} M$ over $\operatorname{Spec} M$, and hence $D' = D_1 \circ D_2 \circ \ldots \circ D_p$ is an automorphism of $X \times \operatorname{Spec} M$ over $\operatorname{Spec} M$. Let s_i $(1 \leqslant i \leqslant p)$ be the elementary symmetric functions in M of degree i in $\epsilon_1, \ldots, \epsilon_p$. One checks trivially that $s_1 s_i = (i+1)s_{i+1}$ $(1 \leqslant i \leqslant p-1)$, so that the subring M' in M generated by $s_1, \ldots, s_p$ is $k[s_1, s_p]$. Let $\psi : \operatorname{Spec} M \to \operatorname{Spec} M'$ be the natural morphism. We then assert that there is a unique automorphism D'' of $X \times \operatorname{Spec} M'$ over $\operatorname{Spec} M'$ which induces D' on base extension to $\operatorname{Spec} M$. Further, the only relations between s_1, s_p in $M' = k[s_1, s_p]$ are $s_1^p = 0$, $s_p^2 = 0$, so that we have a homomorphism $\eta : M' \to \Lambda$, $\eta(s_1) = 0$, $\eta(s_p) = \epsilon$. Let $\phi = \operatorname{Spec} \eta : \operatorname{Spec} \Lambda \to \operatorname{Spec} M'$. We have defined the maps

$$\Lambda \xrightarrow{\eta_i} M \supset M' \xrightarrow{\eta} \Lambda$$

$$\operatorname{Spec} \Lambda \xleftarrow{\phi_i} \operatorname{Spec} M \xrightarrow{\psi} \operatorname{Spec} M' \xleftarrow{\phi} \operatorname{Spec} \Lambda.$$

Then via ϕ, D'' induces an automorphism D''' of $X \times \operatorname{Spec} \Lambda$ over $\operatorname{Spec} \Lambda$ which on the closed fibre $X \hookrightarrow X \times \operatorname{Spec} \Lambda$ is the identity. So D''' may be thought of as a vector field on X. We assert that $D''' = D^{(p)}$.

To verify these assertions, we may assume $X = \operatorname{Spec} A$. Then D_i is obtained by the automorphism of M-algebras $A \otimes_k M \to A \otimes_k M$ determined by $a \longmapsto a + (Da) \cdot \epsilon_i$, and D' by the automorphism of $A \otimes_k M$ over M determined by

$$a \longmapsto \left\{ \prod_i (1 + \epsilon_i D) \right\} a = (1 + s_1 D + s_2 D^2 + \ldots + s_p D^p) a.$$

Our assertions can be read off from this.

Now suppose G is a group scheme and D a left invariant vector field, whose value at the identity is the tangent vector $t \in \underline{G}(\Lambda)$. Then the corresponding automorphism of $G \times \operatorname{Spec} \Lambda$ is just translation by t, and D_i is translation of $G \times \operatorname{Spec} M$ by the image of t under the morphism $\underline{G}(\Lambda) \xrightarrow{\underline{G}(\eta_i)} \underline{G}(M)$. Hence D' is translation by $t' = \prod_{i=1}^{p} \underline{G}(\eta_i)\,(t) \in G(M)$. Now, t' is the image of an element $t'' \in \underline{G}(M')$ by the map $\underline{G}(M') \to \underline{G}(M)$. The homomorphism $\underline{G}(M) : \underline{G}(M') \to \underline{G}(\Lambda)$ maps t'' to $t^{(p)}$.

$$\begin{array}{ccccccc} t & & t' & & t' & & t^{(p)} \\ \in & & \in & & \in & & \in \\ \underline{G}(\Lambda) & \longrightarrow & \underline{G}(M) & \longleftarrow & G(M') & \longrightarrow & \underline{G}(\Lambda). \end{array}$$

Apply these remarks to the situation where X is an abelian variety and $\hat{X}$ its dual, with $G = \hat{X}$. Then for any k-algebra R, $\underline{G}(R)$ is the group of all line bundles L on $X \times \operatorname{Spec} R$ trivial on

$\{0\} \times \operatorname{Spec} R$ such that for any point $P \in \operatorname{Spec} R$, $L|X \times \{P\}$ belongs to $\operatorname{Pic}^0 X$. One sees by definition that if the 1-cocycle $\{f_{ij}\}$ for a covering $\mathfrak{U}$ of X with coefficients in the sheaf $\mathcal{O}_X$ represent a cohomology class ξ in $H^1(X, \mathcal{O}_X)$, the corresponding tangent vector $t_\xi \in \operatorname{Lie} \hat{X} \subset \underline{\hat{X}}(\Lambda) \simeq H^1(X, \mathcal{O}^*_{X \times \operatorname{Spec} \Lambda})$ is represented by the 1-cocycle $\{1 + \epsilon f_{ij}\}$ for the same covering. Hence, the element of $\underline{\hat{X}}(M) \subset H^1(X, \mathcal{O}^*_{X \times \operatorname{Spec} M})$ we obtain is represented by the 1-cocycle $\prod_{r=1}^{p} (1 + \epsilon_r f_{ij}) = (1 + f_{ij} s_1 + f_{ij}^2 s_2 + \ldots + f_{ij}^p s_p)$. It follows that $t_\xi^{(p)} \in \operatorname{Lie} \hat{X} \subset \underline{\hat{X}}(\Lambda)$ is represented by the 1-cocycle $\{1 + f_{ij}^p \epsilon\}$, and hence comes from the 1-cocycle $\{f_{ij}^p\}$ for $\mathcal{O}_X$.

16. Cohomology of Line Bundles. Our first aim in this section is to prove the two following theorems.

THE RIEMANN-ROCH THEOREM. *For all line bundles L on X, if $L \simeq \mathcal{O}_X(D)$, we have*

$$\chi(L) = \frac{(D^g)}{g!},$$

$$\chi(L)^2 = \deg \phi_L,$$

where (D^g) is the g-fold self-intersection number of D.

THE VANISHING THEOREM. *If for a line bundle L on X, $K(L)$ is finite, there is a unique integer $i = i(L)$, $0 \leqslant i(L) \leqslant g$, such that $H^p(X, L) = (0)$ for $p \neq i$ and $H^i(X, L) \neq (0)$. Further, $i(L^{-1}) = g - i(L)$.*

PROOFS. (1) If L_1 and L_2 are two line bundles on X such that $L_1 \otimes L_2^{-1} \in \operatorname{Pic}^0 X$, then $\chi(L_1) = \chi(L_2)$. In fact consider the line bundle $p_1^*(L_1) \otimes P$ on $X \times \hat{X}$. Then the Euler characteristic of its restriction L_y to $X \times \{y\}$, $(y \in \hat{X})$, is independent of y. But L_1 and L_2 are both isomorphic to one of the L_y's, so $\chi(L_1) = \chi(L_2)$. Next, if L is symmetric, $n_X^*(L^m) \simeq L^{mn^2}$, so

$$\chi(L^{mn^2}) = \chi(n_X^* L^m) = \deg n_X \cdot \chi(L^m) = n^{2g} \cdot \chi(L^m). \tag{*}$$

Since any L can be written $L_1 \otimes L_2$ where L_1 is symmetric and $L_2 \in \operatorname{Pic}^0 X$, (*) holds for any line bundle L. Since $\chi(L^k)$ is a polynomial in k, (*) shows that $\chi(L^k)$ (for any L) is a homogeneous polynomial of degree g. Let

$$\chi(L^k) = a(L) \cdot \frac{k^g}{g!},$$

so that $\chi(L) = \dfrac{a(L)}{g!}$, and we have only to establish that $a(L) = (D^g)$ if $L = \mathcal{O}(D)$. Assume this for the moment when L is very ample, and let L_i $(i = 1, 2)$ be very ample. Then

$$P(n_1, n_2) = g! \cdot \chi(L_1^{n_1} \otimes L_2^{n_2})$$

is a polynomial in n_1 and n_2. Since $\chi(L_1^{kn_1} \otimes L_2^{kn_2}) = k^g \cdot \chi(L_1^{n_1} \otimes L_2^{n_2})$, P is homogeneous of degree g. If D_i is the divisor corresponding to L_i, since $L_1^{n_1} \otimes L_2^{n_2}$ is very ample for $n_1, n_2 \geqslant 1$, we see that $P(n_1, n_2) = ((n_1 D_1 + n_2 D_2)^g) = \sum_{i=0}^{g} \binom{g}{i} n_1^i n_2^{g-i} (D_1^i D_2^{g-i})$ if $n_1, n_2 \geqslant 1$, and it follows that the same equality holds for all $n_1, n_2 \in \mathbf{Z}$, in particular for $n_1 = 1, n_2 = -1$. But now any line bundle L on X can be written as $L_1 \otimes L_2^{-1}$ with L_i very ample.

Thus, it only remains to show that $a(L) = (D^g)$ for L very ample. We can then choose sections $\sigma_0, \ldots, \sigma_g$ of L on X such that (i) σ_i have no common zero, and (ii) the divisor of zeros of $\sigma_1, \ldots, \sigma_g$ intersect transversally at (D^g) distinct points. Because of condition (i), we get a morphism $X \xrightarrow{\phi} \mathbf{P}^g$ defined by $x \longmapsto (\sigma_0(x), \ldots, \sigma_g(x))$, and by (ii), the 0-cycle $\phi^{-1}((1, 0, \ldots, 0))$ is of degree (D^g), hence ϕ is of degree (D^g). Hence, by the proposition in the appendix to §6, $a(L)$ is (D^g) times the leading coefficient of $g! \chi(\mathcal{O}_{\mathbf{P}^g}(n))$, i.e. $a(L) = (D^g)$.

Next, we have to show that $\chi(L)^2 = \deg \phi_L$. Suppose first that $K(L)$ is finite. Then, by definition of ϕ_L, we have

$$(1_X \times \phi_L)^* P \simeq m^* L \otimes p_1^* L^{-1} \otimes p_2^* L^{-1}$$

on $X \times X$. Arguing as in §8 and §13, we see that $m^* L \otimes p_1^* L^{-1} \otimes p_2^* L^{-1}$ has higher direct images on the first factor concentrated on the finite set $K(L)$. Therefore,

$$R^ip_{1,*}(m^*L\otimes p_1^*L^{-1}\otimes p_2^*L^{-1}) \simeq R^ip_{1,*}(m^*L\otimes p_2^*L^{-1})\otimes L^{-1}$$
$$\simeq R^ip_{1,*}(m^*L\otimes p_2^*L^{-1}).$$

It follows that

$$\chi(m^*L\otimes p_1^*L^{-1}\otimes p_2^*L^{-1}) = \sum_{i=0}^{g}(-1)^i\chi(R^ip_{1,*}(m^*L\otimes p_1^*L^{-1}\otimes p_2^*L^{-1}))$$
$$= \sum_{i=0}^{g}(-1)^i\chi(R^ip_{1,*}(m^*L\otimes p_2^*L^{-1}))$$
$$= \chi(m^*L\otimes p_2^*L^{-1}).$$

Since $(m,p_2): X\times X\to X\times X$ is an isomorphism, and $(m,p_2)^*[p_1^*L\otimes p_2^*L^{-1}]\simeq m^*L\otimes p_2^*L^{-1}$, we find

$$\chi(m^*L\otimes p_2^*L^{-1}) = \chi(p_1^*L\otimes p_2^*L^{-1})$$
$$= \chi(L)\cdot\chi(L^{-1})$$
$$= (-1)^g.\ \chi(L)^2.$$

Since $X\times\hat{X}$ is the quotient of $X\times X$ by the free action of $K(L)$, we deduce that

$$(-1)^g.\deg\phi_L = \deg\phi_L\cdot\chi(P)$$
$$= \chi((1_X\times\phi_L)^*P)$$
$$= \chi(m^*L\otimes p_1^*L^{-1}\otimes p_2^*L^{-1})$$
$$= (-1)^g.\chi(L)^2.$$

Finally suppose $K(L)$ is not finite. We can choose a finite subgroup $F\subset K(L)$ of arbitrarily large order f. The map $1_X\times\phi_L$: $X\times X\to X\times\hat{X}$ therefore factors as $X\times X\to X\times X/F\to X\times\hat{X}$ so that $m^*L\otimes p_2^*L^{-1}$ being the inverse image by $1_X\times\phi_L$ of $P\otimes p_1^*L$, has Euler characteristic divisible by f. Since this holds for arbitrarily large f, $m^*L\otimes p_2^*L^{-1}$ has Euler characteristic 0. But as before $\chi(m^*L\otimes p_2^*L^{-1}) = (-1)^g\chi(L)^2$. So $\chi(L)=0$ and $\deg\phi_L = 0$.

This proves the Riemann-Roch theorem.

(2) We have the Cartesian diagram

$$\begin{array}{ccc} X\times X & \xrightarrow{p_2} & X \\ \downarrow{\scriptstyle 1\times\phi_L} & & \downarrow{\scriptstyle\phi_L} \\ X\times\hat{X} & \xrightarrow{p_2'} & \hat{X} \end{array}$$

(i.e. the left top corner identifies itself to the fibre product of the lower left and upper right corners), and $m^*L\otimes p_1^*L^{-1}\otimes p_2^*L^{-1}\simeq(1\times\phi_L)^*(P)$. Since ϕ_L is flat, we have by Corollary 5, §5, that

$$\phi_L^*(R^qp_{2,*}'(P))\simeq R^qp_{2,*}((1\times\phi_L)^*(P))$$
$$\simeq R^qp_{2,*}(m^*L\otimes p_1^*L^{-1}\otimes p_2^*L^{-1}).$$

But we have seen in §13 that $R^qp_{2,*}'(P)=(0)$ if $q\neq g$ and $R^gp_{2,*}'(P)$ is the residue field $k(0)$ at $0\in\hat{X}$. Hence, we deduce that

$$R^ip_{2,*}(m^*L\otimes p_1^*L^{-1}\otimes p_2^*L^{-1}) = \begin{cases}(0)\text{ if }q\neq g\\ \mathcal{O}_{K(L)}\text{ if }q=g.\end{cases}\qquad(*)$$

Since $K(L)$ is finite, by arguments which we used in (1), we may replace $m^*L\otimes p_1^*L^{-1}\otimes p_2^*L^{-1}$ by $m^*L\otimes p_1^*L^{-1}$ in (*). Taking cohomologies, we get that

$$\dim H^q(X\times X,\ m^*L\otimes p_1^*L^{-1}) = \begin{cases}0\text{ if }q\neq g\\ \deg\phi_L\text{ if }q=g.\end{cases}$$

In this formula, we may as in (1) replace $m^*L\otimes p_1^*L^{-1}$ by $p_2^*L\otimes p_1^*L^{-1}$, so using the Künneth formula, we see that if $h^i(L)=\dim H^i(X,L)$,

$$\sum_{i=0}^{q}h^i(L)\,h^{q-i}(L^{-1}) = \begin{cases}0\text{ if }q\neq g\\ \deg\phi_L\text{ if }q=g.\end{cases}$$

Since all these h^i's are non-negative, it is easy to see that this can only hold if *only one* of the $h^i(L)$'s is positive and *only one* of the $h^i(L^{-1})$'s is positive, and that the sum of these two i's is g.

REMARKS. Consider the case $k = \mathbf{C}$, $X = V/U$ where V is a g-dimensional complex vector space and U a lattice in V. Let $L = L(H, \alpha)$ be a line bundle on X and $E = \operatorname{Im} H$ so that E is a skew symmetric real bilinear form on V and $E(U \times U) \subset \mathbf{Z}$. We consider V as an oriented vector space by means of the complex structure. If $u_1, \ldots, u_{2g}$ is a basis of U, we call $\det(E(u_i, u_j))$ the determinant of E; this is independent of choice of basis for U and is always positive. Further, we have seen that $K(L)$ is finite if and only if E is non-degenerate, and that

$$\deg \phi_L = \text{Order } K(L) = \text{order } (U^\perp/U),$$

where $U^\perp = \{x \in V \mid E(x, u) \in \mathbf{Z}, \forall\ u \in U\}$. Now, the elements λ_i defined by $\lambda_i(x) = E(x, u_i)$ form a basis of the dual, $\operatorname{Hom}(U^\perp, \mathbf{Z})$, of $U^\perp$, so that we have

$$\text{order } (U^\perp/U) = \det(\lambda_i(u_j)) = \det(E(u_i, u_j)).$$

Hence we obtain that $|\chi(L)| = +\sqrt{\det(E(u_i, u_j))}$. Now, given any skew symmetric matrix A of degree $2g$, it is well known that there is a uniquely determined polynomial function $\operatorname{pf}(A)$, the Pfaffian of A, in the entries of A, such that $\operatorname{pf}(A)^2 = \det A$ and $\operatorname{pf}((E_0)) = 1$ where E_0 is the matrix

$$E_0 = \left[\begin{array}{cc|cc|c} 0 & -1 & & & \\ 1 & 0 & \multicolumn{2}{c|}{\multirow{2}{*}{\Large 0}} & \multirow{2}{*}{\Large 0} \\ \cline{1-2} & & \multicolumn{2}{c|}{} & \\ \multicolumn{2}{c|}{\multirow{2}{*}{\Large 0}} & 0 & -1 & \multirow{2}{*}{\Large 0} \\ \multicolumn{2}{c|}{} & 1 & 0 & \\ \hline \multicolumn{2}{c|}{\multirow{2}{*}{\Large 0}} & \multicolumn{2}{c|}{\multirow{2}{*}{\Large 0}} & \multirow{2}{*}{\Large $\ddots$} \\ \multicolumn{2}{c|}{} & \multicolumn{2}{c|}{} & \end{array}\right].$$

Now, if X runs through $SL(2g, \mathbf{C})$, $\operatorname{pf}(X'AX)^2 = \det X'AX = \det A = \operatorname{pf}(A)^2$ and since $SL(2g, \mathbf{C})$ is connected, we deduce that $\operatorname{pf}(X'AX) = \operatorname{pf}(A)$ if $X \in SL(2g, \mathbf{C})$. Now, two different bases $u_1, \ldots, u_{2g}$ of U such that $u_1 \wedge \ldots \wedge u_{2g}$ is *positive* differ by a matrix in $SL(2g, \mathbf{R})$, so that for such $u_1, \ldots, u_{2g}$, $\operatorname{pf}(E(u_i, u_j))$ is independent of the choice of basis, i.e. it is determined by E, the lattice U and the orientation of V induced by the complex structure on V. We then assert that we have actually

$$\chi(L) = \operatorname{pf}(E(u_i, u_j)). \qquad (*)$$

Since both sides extend to functions on $\mathbf{Q} \otimes_{\mathbf{Z}} \operatorname{Pic} X$ which on any finite-dimensional subspace is a polynomial function, we see that either $\chi(L) = \operatorname{pf}(E(u_i, u_j))$ for all L or $\chi(L) = -\operatorname{pf}(E(u_i, u_j))$ for all L. If we show that for L ample, $\operatorname{pf}(E(u_i, u_j))$ is positive, it would follow that only the first alternative can hold. But then, $L = L(H, \alpha)$ with H positive definite hermitian. Thus, we have only to show that if H is positive definite hermitian on a complex vector space V and $u_1, u_2, \ldots, u_{2g}$ is any real basis with $u_1 \wedge \ldots \wedge u_{2g}$ positive, $\operatorname{pf}(\operatorname{Im} H(u_i, u_j)) > 0$. By our earlier remark, if this holds for one such basis, it holds for any other such. Thus we may use a $\mathbf{R}$-basis $u_1, iu_1, u_2, iu_2, \ldots, iu_g$ where $H(u_i, u_j) = \delta_{ij}$. But now, the matrix of $\operatorname{Im} H$ with respect to this basis equals E_0 and the Pfaffian of this matrix is 1.

This proves the assertion.

THE INDEX OF LINE BUNDLES.

The purpose of the rest of this section is to prove that $i(L)$ can be computed as follows.

THEOREM. *Let L be an ample line bundle on an abelian variety X, and M a non-degenerate line bundle†. Let $P(t)$ be the polynomial defined by $P(n) = \chi(L^n \otimes M)$. Then P has all its g roots real and the index of M equals the number of positive roots, counted with multiplicity, of $P(t)$.*

The proof will be given in a series of steps. We make heavy use of the next lemma. Before stating the lemma, let us introduce some notations. For $a = (a_1, \ldots, a_k) \in \mathbf{Z}^k$, we write $|a| = \sum_{i=1}^{k} |a_i|$, and if $L_1, \ldots, L_k$ are k-line bundles, we denote the line bundle $L_1^{a_1} \otimes L_2^{a_2} \otimes \ldots \otimes L_k^{a_k}$ by L^a.

† By definition, this means $K(M)$ is finite.

LEMMA. *Let X be a projective variety of dimension r and $L_1, \dots, L_k$ line bundles on X. Then there is a constant c depending only on the L_i such that*

$$\dim H^i(L^a) \leqslant c(1 + |a|^r)$$

for $i > 0$ and $a \in \mathbf{Z}^k$.

PROOF. We can easily reduce ourselves to the case when the L_i are all very ample. In fact, choose a very ample L_{k+1} such that $L_i \otimes L_{k+1}$ are very ample for $1 \leqslant i \leqslant k$, and put $L_i' = L_i \otimes L_{k+1}$, $L_{k+1}' = L_{k+1}$. Then there is a linear automorphism T of $\mathbf{Z}^{k+1}$ such that for $a = (a_1, \dots, a_{k+1}) \in \mathbf{Z}^{k+1}$, $L_1^{a_1} \otimes \dots \otimes L_{k+1}^{a_{k+1}} = (L')^{Ta}$ and $\alpha^{-1}|a| \leqslant |Ta| \leqslant \alpha|a|$ for a suitable $\alpha > 0$.

Thus we assume all L_i $(1 \leqslant i \leqslant k)$ very ample. We proceed by induction on the integer $\nu = \dim X + k$. When $\nu = 0$, the assertion is trivial. Thus we may assume $\nu > 0$ and that the assertion holds for smaller values of ν. If now $k = 0$, the assertion is again clear. Thus suppose $k > 0$, and let L' be the system of line bundles $\{L_1, \dots, L_{k-1}\}$ and for $a = (a_1, \dots, a_k) \in \mathbf{Z}^k$, set $a' = (a_1, \dots, a_{k-1}) \in \mathbf{Z}^{k-1}$. Then the existence of a constant c for all $a \in \mathbf{Z}^k$ with $a_k = 0$ follows by induction hypothesis. For any $\mu \in \mathbf{Z}$, we have an exact sequence

$$0 \longrightarrow L'^{a'} \otimes L_k^{\mu} \longrightarrow L'^{a'} \otimes L_k^{\mu+1} \longrightarrow L'^{a'} \otimes L_k^{\mu+1}|_H \longrightarrow 0$$

where H is a hyperplane section for the projective imbedding of X given by L_k. Suppose now that $a_k > 0$. We have the exact sequence

$$H^i(L'^{a'} \otimes L_k^{\mu}) \longrightarrow H^i(L'^{a'} \otimes L_k^{\mu+1}) \longrightarrow H^i(H, L'^{a'} \otimes L_k^{\mu+1}|_H)$$

from which we have

$$\dim H^i(L'^{a'} \otimes L_k^{\mu+1}) - \dim H^i(L'^{a'} \otimes L_k^{\mu}) \leqslant \dim H^i(H, L'^{a'} \otimes L_k^{\mu+1}|_H) \leqslant c(|a|^{r-1} + 1)$$

for $0 \leqslant \mu < a_k$ and a suitable constant c, by induction hypothesis. Summing over all μ with $0 \leqslant \mu < a_k$, we obtain

$$\dim H^i(L'^{a'} \otimes L_k^{a_k}) \leqslant C.|a_k|(|a|^{r-1} + 1) + \dim H^i(L'^{a'}) \leqslant C'(|a|^r + 1).$$

Similarly, if $a_k < 0$, the exactness of

$$H^{i-1}(H, L'^{a'} \otimes L_k^{\mu+1}|_H) \longrightarrow H^i(X, L'^{a'} \otimes L_k^{\mu}) \longrightarrow H^i(X, L'^{a'} \otimes L_k^{\mu+1})$$

gives, for $0 > \mu \geqslant a_k$, the inequalities

$$\dim H^i(L'^{a'} \otimes L_k^{\mu}) - \dim H^i(L'^{a'} \otimes L_k^{\mu+1}) \leqslant \dim H^{i-1}(H, L'^{a'} \otimes L_k^{\mu+1}|_H) \leqslant C(1 + |a|^{r-1})$$

and summing over μ with $0 > \mu \geqslant a_k$, we get as before the required inequality.

STEP A. Let L be any non-degenerate line bundle on an abelian variety X and H a very ample line bundle on X, and let P be the polynomial in two variables defined by $P(m, n) = \chi(L^m \otimes H^n)$. If $P(1, t) \neq 0$ for $0 \leqslant t \leqslant 1$, then $i(L) = i(L \otimes H)$.

PROOF. The following remark is essential to what follows. If $f: X \to Y$ is an isogeny of abelian varieties of degree prime to p and L a line bundle on Y with $\chi(L) \neq 0$, $i(f^*(L)) = i(L)$. In fact, we know by Cor. to Prop. 3, §7 that L is a direct summand of $f_*(f^*(L))$, and $H^i(X, f^*(L)) \simeq H^i(Y, f_*(f^*(L)))$, so that $H^i(L) \neq (0) \Rightarrow H^i(f_*(f^*L)) \neq (0) \Rightarrow H^i(f^*(L)) \neq (0)$. Also if $L_0 \in \mathrm{Pic}^0 X$, then $i(L) = i(L \otimes L_0)$. In fact, for some $x \in X$, $L \otimes L_0 \simeq T_x^* L$, hence $H^i(L) \neq (0) \Rightarrow H^i(T_x^* L) \neq (0) \Rightarrow H^i(L \otimes L_0) \neq (0)$. In particular, since $n_X^*(L) = L^{n^2} \otimes L_0$ with $L_0 \in \mathrm{Pic}^0 X$, we see that $i(L^{n^2}) = i(L)$ for any $n > 0$, with $p \nmid n$.

Suppose then that N is a large square prime to p. If $i(L) \neq i(L \otimes H)$, then $i(L^N) \neq i(L^N \otimes H^N)$, so there is a least integer a in $0 < a \leqslant N$ with $i_1 = i(L^N \otimes H^a) \neq i(L^N \otimes H^{a-1}) = i(L^N)$. (Note that since $P(1,t)$ has no rational zeroes, $0 \leqslant t \leqslant 1$, all the bundles $L^N \otimes H^a$ are non-degenerate so $i(L^N \otimes H^a)$ is well defined.) The exact sequence $0 \to L^N \otimes H^{a-1} \to L^N \otimes H^a \to L^N \otimes H^a|_V \to 0$, where V is a hyperplane section of X for the imbedding given by H, gives us that

$$0 \longrightarrow H^{i_1}(L^N \otimes H^a) \longrightarrow H^{i_1}(L^N \otimes H^a|_V)$$

is exact so that

$$\dim H^{i_1}(V, L^N \otimes H^a|_V) \geq \dim H^{i_1}(L^N \otimes H^a)$$
$$= |\chi(L^N \otimes H^a)|$$
$$= N^g . P\left(1, \frac{a}{N}\right).$$

But there is a lower bound

$$P(1, t) \geq c > 0 \text{ if } 0 \leq t \leq 1,$$

and since this holds for arbitrarily large N, while V is of dimension $g-1$, we get a contradiction to the lemma.

STEP B. If L_1 and L_2 are two line bundles on an abelian variety and $F(s, t)$ is the homogeneous polynomial defined by $F(m, n) = \chi(L_1^m \otimes L_2^n)$, and if $F(t, 1-t) \neq 0$ for $0 \leq t \leq 1$, then $i(L_1) = i(L_2)$.

PROOF. Choose a very ample L_3 such that $L_1 \otimes L_3 \otimes L_2^{-1}$ is also very ample. Set $f(a, b, c) = \chi(L_1^a \otimes L_2^b \otimes L_3^c)$, so that $f(a, b, 0) = F(a, b)$. Since $F(t, 1-t) \neq 0$ for $0 \leq t \leq 1$, by continuity, we can choose a square N, prime to p, so large that for $0 \leq r \leq N-1$, $0 \leq t \leq 1$,

$$f(N-r, r, t) = N^g f\left(1 - \frac{r}{N}, \frac{r}{N}, \frac{t}{N}\right) \neq 0,$$

$$f(N-r-1+t, r+1-t, t) = N^g f\left(1 - \frac{r+1-t}{N}, \frac{r+1-t}{N}, \frac{t}{N}\right) \neq 0.$$

The first equation coupled with Step A gives us that for $0 \leq r \leq N-1$, r an integer,

$$i(L_1^{N-r} \otimes L_2^r) = i(L_1^{N-r} \otimes L_2^r \otimes L_3)$$

and the second gives us that

$$i(L_1^{N-r} \otimes L_2^r \otimes L_3) = i(L_1^{N-r-1} \otimes L_2^{r+1})$$

for $0 \leq r \leq N-1$, r an integer. Taken together, we get that for r in the same range,

$$i(L_1^{N-r} \otimes L_2^r) = i(L_1^{N-r-1} \otimes L_2^{r+1}),$$

so that we obtain

$$i(L_1) = i(L_1^N) = i(L_2^N) = i(L_2).$$

COROLLARY. *If L is non-degenerate and n any integer > 0,*

$$i(L) = i(L^n).$$

STEP C. If L_1, L_2, and $L_1 \otimes L_2$ are non-degenerate,

$$i(L_1 \otimes L_2) \leq i(L_1) + i(L_2).$$

PROOF. Let $\nu: X \times X \to X$ be the morphism $(x, y) \longmapsto x - y$, and set $L = p_1^*(L_1) \otimes p_2^*(L_2)$. Then $\nu^{-1}(0)$ is the diagonal of $X \times X$, and if we identify it with X, $L \mid \nu^{-1}(0)$ becomes isomorphic to $L_1 \otimes L_2$, which shows that $L|_{\nu^{-1}(x)}$ is non-degenerate for any $x \in X$ and has index $i = i(L_1 \otimes L_2)$. Hence, the direct images $R^j\nu(L)$ vanish for $j < i$, and by the Leray spectral sequence, $H^p(X \times X, L) = 0$ for $p < i$. But now,

$$H^{i(L_1)+i(L_2)}(X \times X, p_1^*(L_1) \otimes p_2^*(L_2)) = H^{i(L_1)}(X, L_1) \otimes H^{i(L_2)}(X, L_2) \neq 0,$$

so that $i(L_1) + i(L_2) \geq i = i(L_1 \otimes L_2)$.

STEP D. Let L_1 and L_2 be non-degenerate line bundles on an abelian variety X such that $L_1 \otimes L_2^{-1}$ is ample. If $f(m,n) = \chi(L_1^m \otimes L_2^n)$, suppose $f(t, 1-t)$ has a unique zero τ in $[0, 1]$ of multiplicity λ. Then

$$0 \leq i(L_2) - i(L_1) \leq \lambda.$$

PROOF. By Step C, we have

$$i(L_1) = i(L_1 \otimes L_2^{-1} \otimes L_2) \leq i(L_1 \otimes L_2^{-1}) + i(L_2) = i(L_2)$$

which proves the first inequality.

Since f is homogeneous and $i(L^n) = i(L)$ for $n > 0$, we may replace L_1 and L_2 by suitable powers to suppose $L_1 \otimes L_2^{-1}$ very ample. Let us denote by $H, H^2, \ldots$, respectively a hyperplane section of X, a hyperplane section of this section, etc. for the projective imbedding given by $L_1 \otimes L_2^{-1}$.

Let N be any large integer, which we suppose coprime to the denominator of τ if τ is rational. Then there is a unique integer r with $0 < r \leq N$ such that $\frac{r-1}{N} < \tau < \frac{r}{N}$. Put $s = N - r$, $i(L_1) = i_1$ and $i(L_2) = i_2$.

We first propose to show by induction on α that for $k < r-1$, $l = N-k$, we have

$$H^p(H^\alpha, L_1^k \otimes L_2^l) = (0) \text{ if } p < i_2 - \alpha - 1.$$

The assertion is obvious for $\alpha = 0$, since by Step B,

$$i(L_1^{r-1} \otimes L_2^{s+1}) = i(L_1^{r-2} \otimes L_2^{s+2}) = \ldots = i(L_2^N) = i_2.$$

Suppose then that $\alpha > 0$ and the above holds for $\alpha - 1$ instead of α. From the exact sequence

$$0 \longrightarrow L_1^{k-1} \otimes L_2^{l+1}|_{H^{\alpha-1}} \longrightarrow L_1^k \otimes L_2^l|_{H^{\alpha-1}} \longrightarrow L_1^k \otimes L_2^l|_{H^\alpha} \longrightarrow 0$$

we get the exactness of

$$H^p(L_1^k \otimes L_2^l|_{H^{\alpha-1}}) \longrightarrow H^p(L_1^k \otimes L_2^l|_{H^\alpha}) \longrightarrow H^{p+1}(L_1^{k-1} \otimes L_2^{l+1}|_{H^{\alpha-1}})$$

and the assertion follows by induction hypothesis. But now, the exactness of

$$H^p(L_1^{r-1} \otimes L_2^{s+1}|_{H^{\alpha-1}}) \longrightarrow H^p(L_1^r \otimes L_2^s|_{H^{\alpha-1}}) \longrightarrow H^p(L_1^r \otimes L_2^s|_{H^\alpha})$$

coupled with the above fact gives us that the map

$$H^p(L_1^r \otimes L_2^s|_{H^{\alpha-1}}) \longrightarrow H^p(L_1^r \otimes L_2^s|_{H^\alpha})$$

is injective for $p \leqslant i_2 - \alpha$. Taking $p = i_1$, we deduce that

$$H^{i_1}(X, L_1^r \otimes L_2^s) \longrightarrow H^i(H^{i_2-i_1}, L_1^r \otimes L_2^s|_{H^{i_2-i_1}})$$

is injective. Thus we deduce that

$$\dim H^{i_1}(L_1^r \otimes L_2^s|_{H^{i_2-i_1}}) \geqslant \dim H^{i_1}(L_1^r \otimes L_2^s) =$$

$$= |\chi(L_1^r \otimes L_2^s)| = N^g \left| f\left(\frac{r}{N}, \frac{s}{N}\right)\right|.$$

By the first lemma, we therefore deduce that there is a constant $c > 0$ such that for all large N (prime to the denominator of τ if τ is rational),

$$N^g \left| f\left(\frac{r}{N}, \frac{s}{N}\right)\right| < c.\, N^{g-(i_2-i_1)},$$

or

$$\left| f\left(\frac{r}{N}, \frac{s}{N}\right)\right| < \frac{c}{N^{i_2-i_1}}.$$

Now, $f(t, 1-t) = (t-\tau)^\lambda g(t)$ where g is non-vanishing at τ. Thus for all large N as above, there is a $c' > 0$ such that

$$\left|\frac{r}{N} - \tau\right|^\lambda < \frac{c'}{N^{i_2-i_1}},$$

or

$$\left|\frac{r}{N} - \tau\right| < c'' N^{-(i_2-i_1)/\lambda}.$$

If τ were rational and N coprime to the denominator q of τ, we must have $\left|\frac{r}{N} - \tau\right| > \frac{1}{Nq}$ for all r, so that we must have $\frac{i_2-i_1}{\lambda} < 1$, hence $i_2 < i_1 + \lambda$. If τ were irrational, by Kronecker's theorem on the density of fractional parts of $N\tau$ for τ irrational, for a sequence N_i of integers $\to \infty$, the distance of $N_i\tau$ from the nearest integer tends to $\frac{1}{2}$, so that we again deduce that $\frac{i_2 - i_1}{\lambda} < 1$, hence $i_2 < i_1 + \lambda$.

This completes the proof of Step D.

PROOF OF THE THEOREM. We are given an ample L and a non-degenerate M. Let $P(n, m) = \chi(L^n \otimes M^m)$. We must prove that all the g zeroes of $P(t,1) = 0$ are real, and that $i(M)$ is the number of positive ones ($t = 0$ is not a zero, since M is non-degenerate). Choose a positive integer q so that the real zeroes $t_1, \ldots, t_k$ of $P(t, 1)$ are divided up as follows:

$$r_1 < \ldots < r_k, r_i \in \mathbf{Z},$$

$$q^{-1}(r_i - 1) < t_i < q^{-1} r_i.$$

Let λ_i be the multiplicity of the root t_i. Then by Steps B and D, we conclude that if $i(r) = i(L^r \otimes M^q)$, then

$$i(R) = i(r_k) < i(r_k - 1) = i(r_{k-1}) < i(r_{k-1} - 1) = \ldots$$

$(R > r_k)$

$$\ldots = i(r_2) < i(r_2 - 1) = i(r_1) < i(r_1 - 1) = i(S),$$

$(S < r_1 - 1)$

and

$$i(r_l - 1) - i(r_l) < \lambda_l.$$

But for large r, $L^r \otimes M^q$ is ample, hence $i(r) = 0$. And for large *negative* r, $(L^r \otimes M^q)^{-1}$ is ample, hence $i(r) = g$ by the last statement of the vanishing theorem. Therefore

$$g = i\begin{pmatrix}\text{very}\\ \text{negative}\\ r\end{pmatrix} - i\begin{pmatrix}\text{very}\\ \text{positive}\\ r\end{pmatrix} = \Big[\sum_{l=1}^{k} i(r_l - 1) - i(r_l)\Big] < \sum_{i=1}^{k} \lambda_l.$$

But $\Sigma\lambda_l$, the number of real zeroes of $P(t, 1) = 0$ is at most g, so equality holds everywhere, and $i(0) = i(M)$ is just the sum of the λ_l's for which the corresponding root t_l is positive.

COROLLARY. *Let V be a complex vector space of dimension g and U a lattice in it such that $X = V/U$ is an abelian variety. Let $L = L(H, \alpha)$ be a non-degenerate line bundle on X, so that H is a non-degenerate hermitian form on V. Then $i(L)$ equals the number of negative eigenvalues of H.*

PROOF. Choose a basis $u_1, u_2, \ldots, u_{2g}$ of U over $\mathbf{Z}$ such that $u_1 \wedge u_2 \ldots \wedge u_{2g}$ defines the orientation of V. Let $L_0 = L(H_0, \alpha_0)$ be an ample line bundle on X, so that H_0 is positive definite. We set $E = \operatorname{Im} H$ and $E_0 = \operatorname{Im} H_0$. We then have

$$\chi(L_0^n \otimes L) = \operatorname{pf}(nE_0 + E)$$

where E_0 and E are considered as skew symmetric matrices, using the above basis of U. Now, if we use any other positively oriented real basis of V, the Pfaffian gets multiplied by a positive scalar. Thus, if $e_1, \ldots, e_g$ is a $\mathbf{C}$-basis of V, we can utilize the basis $e_1, ie_1, e_2, ie_2, \ldots, e_g, ie_g$ to compute the sign of the above Pfaffian. Choose e_i such that $H_0(e_i, e_j) = \delta_{ij}$ and $H(e_i, e_j) = \lambda_i \delta_{ij}$, $\lambda_i \in \mathbf{R}^*$. Then $nE_0 + E$ has the matrix

$$\left[\begin{array}{cc|cc|c} 0 & -n-\lambda_1 & & & \\ n+\lambda_1 & 0 & & \mathbf{0} & \mathbf{0} \\ \hline & & 0 & -n-\lambda_2 & \\ & \mathbf{0} & n+\lambda_2 & 0 & \mathbf{0} \\ \hline & & & & \\ \mathbf{0} & & \mathbf{0} & & \ddots \end{array}\right]$$

and the Pfaffian of this matrix is $\prod_{i}^{g}(n+\lambda_i)$, (since its square is the determinant and it takes the value $\lambda_1 \ldots \lambda_g$ for $n = 0$, hence the value 1 if all $\lambda_i = +1$). Thus, the index of L is the number of negative λ_i.

This corollary can also be deduced from the results of Andreotti and Grauert [A-G].

17. Very ample line bundles. The object of this section is to prove the following theorem.

THEOREM. *For any ample line bundle L on an abelian variety X, L^n is very ample, if $n \geqslant 3$.*

PROOF. For simplicity, we shall prove L^3 is very ample. If $n > 3$, the same proof works. Since $\dim H^0(X, \underline{L}) = \chi(L) > 0$, we can choose an effective divisor D such that $\mathcal{O}_X(D)$ is isomorphic to the sheaf of sections of L. Further, D can be chosen so as not to have any multiple components, for if $k.E$ occurs in D with E irreducible and $k > 1$, kE is linearly equivalent to $\sum_{i=1}^{k} T_{x_i}^*(E)$ for $\sum_{1}^{k} x_i = 0$, and for suitable choice of the x_i, the $T_{x_i}^*(E)$ are all distinct and distinct from the other components of D.

Thus we assume D without multiple components. Note that for any $x, y \in X$, $T_x^*(D) + T_y^*(D) + T_{-x-y}^*(D) \in |3D|$. We have now to establish the following statements.

(1) Given $x_0, x_1 \in X$ with $x_0 \neq x_1$, there is a $D' \in |3D|$ such that $x_0 \in \operatorname{Supp} D'$, $x_1 \notin \operatorname{Supp} D'$.

(2) Given any tangent vector t to X at x_0, there is a $D' \in |3D|$ such that $x_0 \in \operatorname{Supp} D'$ and t is not tangential to D' (i.e. if $\phi = 0$ is a local equation of D' at x_0, $\langle t, d\phi \rangle \neq 0$).

Since we are making these assertions for any ample L, it suffices to prove (1) and (2) for any ample L with $x_0 = 0$, since the general case follows by applying the result to a translate of L.

Thus, if (1) were not true (with $x_0 = 0$), we would have that for any D as above and any $x, y \in X$,

$$0 \in \text{Supp } D - x \Rightarrow x_1 \in (\text{Supp } D - x) \cup (\text{Supp } D - y) \cup (\text{Supp } D + x + y).$$

Since we may clearly choose y such that x_1 does not belong to the last two members, we deduce that $x \in \text{Supp } D$ implies $x \in \text{Supp } D - x_1$, that is, $\text{Supp } D = \text{Supp } D - x_1$. Since the divisor D has no multiple components, this means that $T_{x_1}(D) = D$. In particular, $x_1 \in K(L)$, hence x_1 has finite order. Let x_1 generate the finite group F. We then have an étale morphism $\pi: X \to X/F$, and $D_1 = \pi(\text{Supp } D)$ is a closed subset pure of codimension one in X/F, which we may consider as a divisor with all components of multiplicity one. Since π is étale, $\pi^*(D_1)$ is again a divisor with all components of multiplicity one and has the same support as D, so that $D = \pi^*(D_1)$ and $\underline{L} \simeq \pi^*(\mathcal{O}_{X/F}(D_1))$. But note that

$$\begin{aligned}\dim H^0(X, \underline{L}) &= \chi(L) \\ &= (\text{Order } F).\chi(\mathcal{O}_{X/F}(D_1)) \\ &= (\text{Order } F).\dim H^0(X/F, \mathcal{O}_{X/F}(D_1)) \\ &> \dim H^0(X/F, \mathcal{O}_{X/F}(D_1)).\end{aligned}$$

Since the set of all divisors D_1 such that $\underline{L} \simeq \pi^*(\mathcal{O}_{X/F}(D_1))$ fall into a finite set of linear equivalence classes, this proves that all sections $s \in \Gamma(\underline{L})$ either define multiple divisors, or lie in one of a finite number of lower-dimensional subspaces $\pi^*\Gamma(\mathcal{O}_{X/F}(D_1))$. This is a contradiction, so (1) holds.

Similarly, suppose (2) is not true for a non-zero tangent vector t at 0, and let T be the invariant vector field defined by t. If (2) is false for all the divisors $T_x^*(D) + T_y^*(D) + T_{-x-y}^*(D)$, it follows immediately that for all $x \in \text{Supp } D$, the vector T_x is tangent to D at x. Since D has no multiple components, this is equivalent to the property:

(*) $\quad \forall\, U \subset X$ open, $\forall$ local equations $\phi = 0$ for D on U,

$$T(\phi) = \alpha.\phi, \text{ some } \alpha \in \mathcal{O}_X(U).$$

In terms of the $k[\epsilon]/(\epsilon^2)$-valued automorphism of X defined by T, (*) just says that the divisor D – a subscheme of X – is invariant. This implies that the $k[\epsilon]/(\epsilon^2)$-valued point of X defined by t is in the subgroup $K(L)$ of points leaving L invariant. Now in characteristic 0, all group schemes are reduced, so $K(L)$ is finite and discrete and this cannot hold unless $t = 0$. On the other hand, in characteristic p, let H be the smallest subgroup of $K(L)$ containing t; then $H \subset X^{(p)}$ and will be determined by its Lie algebra $\mathfrak{h}$ which will be the span of t and its p^{th} powers. It is easy to see that D will be invariant under translations by all points of H. [In fact, if $H = \text{Spec}(R)$, the action of H gives a homomorphism of R^* into the ring of differential operators on X, mapping elements of $\mathfrak{h}$ into the corresponding invariant derivations. Since $\mathfrak{h}$ generates R^*, and the sheaf of ideals $\mathcal{O}_X(-D)$ is stable under $\mathfrak{h}$ by (*), it is also stable under R^*, hence we get a homomorphism $R^* \to \text{Diff}(\mathcal{O}_D)$, i.e. an action of H on D.] Let $X' = X/H$, $D' = D/H$. From the results of §12, we find that $\pi: X \to X'$ is flat and surjective, that D' is a closed subscheme of X' and $D \simeq D' \times_{X'} X$. Therefore if $\mathscr{I}'$ is the sheaf of ideals of D',

$$\mathcal{O}_X(-D) \simeq \mathscr{I}' \otimes_{\mathcal{O}_{X'}} \mathcal{O}_X.$$

Since D is a divisor, $\mathcal{O}_X(-D)$ is a locally free sheaf, so by Part (B), Theorem 1, §12, $\mathscr{I}'$ is a locally free sheaf, i.e. D' is a divisor too. Now $D = \pi^*(D')$, so we compute, as before:

$$\begin{aligned}\dim H^0(X, \underline{L}) &= \deg \pi.\dim H^0(X/H, \mathcal{O}_{X/H}(D')) \\ &> \dim H^0(X/H, \mathcal{O}_{X/H}(D')).\end{aligned}$$

Exactly as before, this implies that all sections $s \in \Gamma(\underline{L})$ either define multiple divisors, or lie in one of a finite set of proper subspaces –a contradiction.