THE THEORY OF COMMUTATIVE FORMAL GROUPS OVER FIELDS OF FINITE CHARACTERISTIC

1963 Russ. Math. Surv. 18 1

(http://iopscience.iop.org/0036-0279/18/6/R01)

THE THEORY OF COMMUTATIVE FORMAL GROUPS OVER FIELDS OF FINITE CHARACTERISTIC

Yu.I. MANIN

Contents

Introduction

1. The concept of a Lie group in its present-day form is the result of combining two structures: a real or complex analytic manifold G and a group law of composition $G \times G \to G$ on the set of points of G, $(x, y) \to xy^{-1}$, represented by an analytic mapping. It is well known that the theory of Lie groups is fairly sharply divided into two parts. The first part is devoted to the study of local properties of groups. The three classical theorems of Lie allow us to reduce these questions to questions on the structure of Lie algebras: as we should say now, the transformation associating with any local Lie group its Lie algebra is an equivalence of categories. The second part of the theory deals with the connection between local Lie groups and global Lie groups: the central places are occupied by the theorem stating that a simply connected Lie group can be uniquely reconstructed from its Lie algebra (or by what we have said, its local Lie group), and by the notion of a fundamental group, which allows us to develop the exact analogue of Galois theory for the description of the possible global Lie groups having one and the same Lie algebra.

Of the three basic notions studied in the theory of Lie groups - Lie algebras, local Lie groups and global Lie groups - the first is purely algebraic and was studied as such practically the moment it had been formulated. The third concept is not algebraic, because it depends on the notion of an analytic manifold. However, in algebraic geometry there exists the parallel concept of an algebraic variety, on which we can define algebraic groups in the same way as we have defined Lie groups. While algebraic geometry goes beyond the frame-work of real or complex coefficient fields, algebraic groups may be studied as a special case of Lie groups by classical means.

This study was begun by Maurer and was completed in recent years by the work of Chevalley [10], leading to the classification of algebraic Lie algebras, i.e. Lie algebras for which there exists a global algebraic Lie group. The well-known principle of Lefschetz, according to which algebraic geometry over an algebraically closed field of characteristic zero agrees in all respects with algebraic geometry over the complex numbers, allows us even to conclude that the occurrence of new phenomena can be expected only for fields of characteristic $p > 0$.

The study of such groups was begun relatively recently, and for a long time was stimulated by the immediate number-theoretical needs, namely the efforts to prove the Riemann hypothesis for zeta-functions on algebraic curves over finite fields. In these studies a quite exceptional role was played by one class of commutative algebraic groups - the so-called abelian varieties, which form the precise analogue of commutative tori in the classical theory (A. Weil). Later, in papers by C. Chevalley, Barsotti, M. Rosenlicht, A. Borel, linear algebraic groups were studied, realized as matrix groups, and a general structure theorem was proved, according to which every algebraic group is an extension of an abelian variety by a linear group. This cycle of papers clearly confirmed the circumstance noticed earlier that Lie algebras are unsuitable for a complete study of algebraic groups, when one is not dealing with the case of characteristic zero. It was shown that although the concept itself of a Lie algebra of an

algebraic group could be defined in the same general context and the resulting correspondence was functorial, a non-commutative group could correspond to a commutative Lie algebra, a Lie subalgebra need not correspond to a subgroup etc. In place of the apparatus of Lie algebras certain global techniques were developed by A. Weil and A. Borel which enabled them to obtain a number of classical and new results for algebraic groups by purely algebraic means and for any characteristic.

In this connection the attempt, based on habits from classical mathematics, to identify Lie algebras with local Lie groups, had taken such firm root that it needed a certain time to realize that differences between these concepts existed in finite characteristic and that it might be advantageous to algebraicise the latter of the two. This, in very general lines, was the path of the different theories of algebraic groups, rising from its beginnings around 1954 to the concept of a formal Lie group, or simply a formal group. Their investigation was begun roughly at the same time in the papers of M. Lazard [51]-[53] and J. Dieudonné [24], and the first results were summarized in the report by Dieudonné at the Amsterdam Mathematical Congress (cf. [33]). During the past eight years the theory of formal groups has brought forth a wealth of results, problems and perspectives as a branch of algebraic geometry, interest in which shows no signs of flagging (in particular, two reports at the Brussels Colloquium on algebraic groups in June 1962 were devoted to this theory). The connection with the algebraic apparatus (algebras with a diagonal mapping) and that of algebraic topology (cf. Dieudonné [28]), was discovered in current work on the number-theoretical interpretation of the structure of algebroid formal groups; finally the general cohomology theory in algebraic geometry, established by the school of Grothendieck, in which commutative formal groups and their variants appear as coefficient groups, - all these examples show that the theory of formal groups is a living and developing branch whose attraction depends on the interlacing of ideas of analysis and algebra, classical analogies and new technical tools, so characteristic of modern mathematics.

2. The topic of this article is the theory of commutative formal groups over fields of finite characteristic. The papers by Dieudonné in which the basic results on the structure of formal groups were first obtained show clearly that the commutative and non-commutative cases differ sharply in the nature of the results, the methods used, and the degree of parallelism with classical theories.

As we have said, the central part of the classical theory of non-commutative Lie groups – the classification of semisimple Lie algebras – was taken over practically unchanged to the case of formal groups of finite characteristic. This is true at least with respect to the results on the existence of the usual four infinite series and the finite number of exceptional simple algebras (cf. Dieudonné [29]). In the course of these results, long and technical additions, whose derivation was essentially based on the global variant of this classification, were obtained by C. Chevalley for algebraic groups by combining the classical techniques of Killing, E. Cartan, H. Weyl and the algebraic-geometric tools of A.Weil, A. Borel and Chevalley himself.

By contrast, the theory of commutative Lie groups in the classical

case is almost trivial. After the proof of Lie's three theorems on the local part of the theory it reduces to the observation that for each dimension there exists up to isomorphism just one commutative Lie algebra, and globally to the simple description of the discrete subgroups of a vector space. In each case, a local commutative Lie group is determined by its dimension and is isomorphic to a direct sum of additive local groups. For fields of finite characteristic this simple situation no longer holds, and the diversity of commutative formal groups is far greater, as is easily seen by examples. First, however, we must give an exact definition of a formal group. The 'naive' definition, used by Dieudonné and Lazard, is obtained as follows. If in the neighbourhood of the identity of an ordinary Lie group we choose an analytic coordinate system and write down the coordinates of the point $z = xy$ as analytic functions of the coordinates of x and y, lying sufficiently close to the origin, we obtain the system of power series

$$z_i = \varphi_i(x_1, \ldots, x_n; y_1, \ldots, y_n) \quad (i = 1, \ldots, n), \tag{0.1}$$

in terms of which the group axioms may be written as identical relations (for brevity we use vector notation $\varphi = (\varphi_i)$, $x = (x_i)$ etc.)

$$\varphi(x, \varphi(y, z)) = \varphi(\varphi(x, y), z) \tag{0.2}$$

(associativity axiom) and

$$\varphi(0, x) = \varphi(x, 0) = x \tag{0.3}$$

(axiom of a neutral element). The existence of inverses, as is easily seen, follows from (0.3) and the analyticity of the functions.

The commutativity of the group is expressed by the law

$$\varphi(x, y) = \varphi(y, x). \tag{0.4}$$

The system of power series (0.1), convergent in a neighbourhood of the origin of coordinates and satisfying the above axioms, defines a local group law. Two such group laws are said to be equivalent if we can pass from one to the other by an invertible analytic transformation of coordinates near the origin:

$$x_i' = \sum_{\alpha} a_{i\alpha} x^{\alpha}, \quad \alpha = (\alpha_1, \ldots, \alpha_n) \in Z_+^n, \quad x^{\alpha} = x_1^{\alpha_1}, \ldots, x_n^{\alpha_n}. \tag{0.5}$$

Now a local Lie group is defined to be an equivalence class of local group laws.

It is clear that with this definition we retain all essentials, when we replace the field of real or complex numbers by any normed field, for example the p-adic numbers (cf. Dynkin [3] and Igusa [48]). The resulting beautiful theory is useful in certain arithmetical questions, but (in the case of algebraically closed fields of characteristic zero) runs parallel to the classical theory. The definition of a formal group in which we are interested is obtained by discarding the requirement of convergence of the power series occurring and merely regarding them as formal series. It is known that over a field of characteristic zero this relaxation also gives nothing new. Therefore, in what follows we shall exclusively consider

the case when the coefficients of the power series (0.1) belong to a given field of characteristic $p > 0$.

In the first place we shall describe the correspondence between algebraic groups and formal groups, which is analogous to the correspondence between global and local Lie groups. It rests on the fact that the unit element (like any point) of an algebraic group G is a non-singular point. Therefore any algebraic function on the group which is regular at the unit element can be expressed as a formal power series in $n = \dim G$ 'local parameters'. Thus, we obtain a group law in the algebraic group; the formal group G so defined is called the completion of the algebraic group G. Formal groups of this form will be called algebroid.

For every dimension $n > 0$ there exists a commutative algebraic group W_n – the group of additive Witt vectors of length n – whose completion is not only not isomorphic to a direct sum of n additive groups, but which, in general, is indecomposable. This fact already shows that the theory of commutative formal groups differs essentially from the classical theory. Many striking phenomena were discovered independently by Lazard and Dieudonné even in the study of one-dimensional formal groups: they showed that there exist countably many pairwise non-isomorphic such groups whose corresponding algebroid groups reduce to three: the additive group, the multiplicative group and the completion of the one-dimensional abelian variety containing no points of order p (apart from zero).

Later on Dieudonné [27], [30] developed an apparatus which in the theory of commutative formal groups plays the same role as that played by Lie algebras in the theory of local Lie groups. Namely he showed that every commutative formal group G over a field k of finite characteristic corresponds to a module over a certain fixed ring E, which depends only on the field k. The ring E is a complete local ring of characteristic zero with residue class field k. The correspondence mentioned is functorial, non-isomorphic groups have non-isomorphic modules, and although not every E-module corresponds to a group, the modules that do so correspond are fairly readily described. This part of the theory may be used in place of Lie's three theorems.

We thus arrive at the problem of studying E-modules. The difficulty of this problem lies in the fact that the ring E is non-commutative and of (Krull) dimension two; there is little the general theory can say in this case. Dieudonné [30] has remarked that if we pass from E to a certain ring of fractions, the classification problem becomes considerably easier, since the new ring is a principal ideal domain. It turns out that non-isomorphic modules may become isomorphic over the new ring, so the corresponding equivalence relation – isogeny – is much weaker than the usual isomorphism, and this permits an invariant interpretation from the point of view of formal groups. Namely the category of commutative formal groups in the accepted sense is additive, but not abelian: it contains bijective morphisms that are not isomorphisms.

It turns out that the E-modules of two formal groups are isogenous if and only if there is a bijective morphism between the corresponding groups.

In this case the groups themselves are said to be isogenous.

In the paper by Dieudonné [30] a complete classification of commutative

formal groups up to isogeny is given. The result is that for every dimension there exists a countable set of indecomposable groups and every group is isogenous to a direct sum of indecomposable ones. The indecomposable groups (or rather, their modules) and their endomorphism rings are described up to isogeny in full detail.

After the paper [30] there remained the following unsolved basic problems in the theory of commutative formal groups:

A. The classification of commutative formal groups up to isomorphism.

(Raising this question in [30], Dieudonné comments that this is a problem 'whose complexity defies analysis'.)

B. Description of algebroid groups.

In connection with B there naturally arises the following problem

C. The determination of the completion of algebraic groups (up to isogeny).

(It may be noted that it is easy to obtain an invariant of an algebraic group – its Lie algebra –, but this is not enough to determine its completion.)

The aim of the present paper is the solution of these three problems. Our results are almost best possible. Very briefly and in general outline the results are obtained in the following way.

In problem A we confine ourselves to the classification of those groups for which multiplication by p is an isogeny. (This limitation is analogous to considering only semisimple Lie algebras in the classical theory; in the study of abelian varieties we only come across such groups). The result states that in each isogeny class of groups the classification up to isomorphism is carried out by means of parameters from the field k; the space of these parameters is algebraic and finite-dimensional; the dimension of the parameter space and the number of connected components tend to infinity with the dimension of the groups of the class. The construction of the parameter space is carried out completely effectively; in particular, for two-dimensional groups all calculations are carried out in full and the explicit form of the parameter space is obtained.

A qualitative answer to question B is as follows: all commutative formal groups occur as direct summands of algebroid groups.

Much more than this cannot be said: for every dimension there are infinitely many non-algebroid groups.

Question C is non-trivial only for abelian varieties. The basic result is that the structure of the completion of an abelian variety can always be calculated; thus, one obtains a global invariant of the variety, namely its zeta-function. Previously this was known only for dimension one; the first partial results in this direction were obtained by the author [8].

3. The paper consists of four chapters. The first gives the foundations of the theory of formal groups and introduces Dieudonné modules. In the second chapter we carry out the classification of modules up to isogeny; in the main we follow the account by Dieudonné with variations by Gabriel. The second important result of this chapter is Theorem 2, which is used in Chapter IV for the study of algebroid groups. The third and fourth chapters contain the basic results of this paper concerning the classification of commutative formal groups and the determination of the structure of algebroid groups. We shall not here enter into the content of

the paper in greater detail, since each chapter opens with a brief survey of the basic results and points out novelties.

The last section of each chapter is devoted to comments of a bibliographical character and a comparison with the non-commutative case.

The basic results of the last two chapters were briefly announced in notes by the author [4]-[6].

For an understanding of the first chapter the reader should have some acquaintance with the theory of categories, to the extent of the first chapter of the paper by Grothendieck [44], and with the definition of schemata; the language of schemata is described for example in the report by Grothendieck at the Edinburgh Congress. Beyond this we only presuppose standard concepts from modern linear algebra and elementary properties of the Witt group.

The reader who wishes to become acquainted with the basic results of the second chapter may confine himself to scanning the fourth section (with a look at the definition of the ring E_F at the beginning of the chapter). The third chapter in those parts where a detailed discussion of the structure of Dieudonné modules is carried out requires only a knowledge of the classification obtained in the second chapter. In the third and seventh sections we obtain the algebraic-geometric structure of the Witt group (cf. the corresponding reference in the text). The fourth chapter is of a more specialized character and presupposes a knowledge of the theory of abelian varieties.

Chapter I

FORMAL GROUPS AND DIEUDONNÉ MODULES; BASIC CONCEPTS

Schüler. Kann Euch nicht eben
ganz verstehen.
Mephistopheles. Das wird
nächstens schon besser gehen,
Wenn Ihr lernt alles reduzieren
Und gehörig klassifizieren.

GOETHE, FAUST

This chapter has essentially the character of a survey; its basic aim is to give a definition of formal groups and related concepts within the framework of algebraic geometry in the spirit of A. Grothendieck [39], as well as to formulate the basic results giving the relation between commutative formal groups and Dieudonné modules.

The definition of formal groups given in the introduction is unsatisfactory from the conceptual and technical point of view; only the language of schemata allows one to introduce the basic notions of the theory of formal groups in a natural and general manner. The description of these concepts occupies the first two sections; we take our definition of formal group in a sense that does not quite agree with that of Dieudonné, because we allow our local rings to have nilpotent elements. The third section is devoted to a description of the category of commutative artinian groups,

following Gabriel [37]. In contrast to Gabriel we employ the 'geometric' language. Propositions 4 and 5 play a role in the interrelation between the classical Witt operators F and V and give rise to a fundamental duality, cf. Barsotti [13]. In the fourth section an important theorem is stated, giving the reduction of the study of commutative formal groups to the problem of classifying their modules. The results of this section play a fundamental role in the following chapter.

§1. Groups in categories

1. The definition of a group in an abstract category stated below represents a particular case of the concept of an algebraic structure on the objects of a category and may be given under more general conditions (cf. Grothendieck [39], Chapter O_{III}). We shall not develop the theory from a few primitive definitions, but confine ourselves to the case needed for the applications, which is considered here to serve as model and motivation for the later more special considerations.

2. Let C be a category and S an object. Consider the class C_S consisting of all pairs (X, f), where X is an object of C and $f: X \to S$ a morphism in C. By a morphism from the pair (X, f) to the pair (Y, g) we understand any morphism $h: X \to Y$ such that the diagram

$$\begin{array}{ccc} X & \overset{h}{\to} & Y \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle g} & \\ & S & \end{array}$$

commutes. With this definition of morphism the class C_S becomes a category which is called the *category of objects over the object* S or the *category of* S*-objects*.

Sometimes it is useful to consider the following more general situation. Let $\Gamma \subset \mathrm{Hom}\,(S, S)$ be a certain monoid with unit element, i.e. a subset of the set of endomorphisms of the object S that contains with any pair of morphisms their product and contains the identity morphism. Let $\sigma \in \Gamma$. Then a σ-morphism from (X, f) to (Y, g) is a morphism $h: X \to Y$ such that the diagram

$$\begin{array}{ccc} X & \overset{h}{\longrightarrow} & Y \\ {\scriptstyle f}\downarrow & \sigma & \downarrow{\scriptstyle g} \\ S & \longrightarrow & S \end{array}$$

commutes. The product of a σ-morphism by a τ-morphism in an obvious sense is a $\tau \circ \sigma$-morphism. Therefore we may turn the class C_S into a category by defining $\mathrm{Hom}_\Gamma((X, f), (Y, g))$ as the set of all σ-morphisms of (X, f) into (Y, g), where σ ranges over Γ. In the particular case when Γ consists only of the identity morphism we obtain the definition of the category C_S given earlier (for which we retain the notation C_S).

The situation described arises, in particular, when we consider linear spaces (possibly provided with additional structure) and their multilinear mappings. Any deviation from linearity in this case is described by an automorphism of the ground field.

Suppose that C_S is a category with a product (to denote the product in

an abstract category we shall use the sign π, and for the sum we use the sign $\amalg$). In this category put $(X, f) \pi (Y, g) = (Z, h)$ (in an obvious notation). Then the object Z is called a *fibre product* of the objects X, Y in the category C and is denoted by $X \underset{S}{\pi} Y$. If for each object S there is a product defined on C_S, we shall say that C is a category with fibre products.

The object $e \in C$ is called a *final object* in C if for each $X \in C$ the set $\mathrm{Hom}(X, e)$ consists of a single element. All final objects are isomorphic, and we may therefore consider the final object to be unique (if there is one). In the category C_S there is a final object: this is the pair $(S, 1_S)$ (the symbol 1_X or simply 1 denotes the identity morphism of the object X). If $e \in C$ is a final object, then the category C_e is equivalent to C.

In what follows we shall assume that categories satisfy two axioms.

I. There exists a final object e in the category C.

II. C is a category with a product.

3. An *internal law of composition* on the object $X \in C$ is a morphism $c\colon X \pi X \to X$; sometimes we denote this by the symbol c_X.

The law of composition is said to be associative if it satisfies the following

ASSOCIATIVITY AXIOM. The diagram

$$\begin{array}{ccc} X\pi X\pi X & \xrightarrow{c\pi 1} & X\pi X \\ {\scriptstyle 1\pi c}\downarrow & & \downarrow{\scriptstyle c} \\ X\pi X & \xrightarrow{\ c\ } & X \end{array}$$

commutes.

In the formulation of the following axioms we denote by $d\colon X \to X \pi X$ the diagonal morphism; $\varepsilon\colon X \to e$ the uniquely determined morphism; and $s\colon X \pi X \to X \pi X$ the morphism interchanging the factors.

An associative law of composition c_X is called a group law if it satisfies the following two axioms.

AXIOM OF A LEFT NEUTRAL. There exists a morphism $\eta\colon e \to X$ such that the diagram

$$\begin{array}{ccc} X\pi X & \xrightarrow{(\eta\circ\varepsilon)\pi 1} & X\pi X \\ {\scriptstyle d}\uparrow & & \downarrow{\scriptstyle c} \\ X & \xrightarrow[1]{} & X \end{array}$$

commutes.

AXIOM OF A LEFT INVERSE. There exists a morphism $a\colon X \to X$ such that the diagram

$$\begin{array}{ccc} X\pi X & \xrightarrow{a\pi 1} & X\pi X \\ {\scriptstyle d}\uparrow & & \downarrow{\scriptstyle c} \\ X & \xrightarrow[\eta\circ\varepsilon]{} & X \end{array}$$

commutes.

We leave as an exercise the formulation in terms of commutative diagrams and the proof of the usual elementary properties of groups: the 'left neutral' morphism is also 'right neutral' and is uniquely determined; the 'left inverse' morphism is also 'right inverse' and is unique.

A group law c is said to be *commutative* or *abelian* if it satisfies the

COMMUTATIVITY AXIOM. The diagram

$$\begin{array}{ccc} X\pi X & \xrightarrow{s} & X\pi X \\ {\scriptstyle c}\searrow & & \swarrow{\scriptstyle c} \\ & X & \end{array}$$

commutes.

The object $X \in C$ together with a group law c defined on it is called a *C-group* (commutative if c is commutative). For brevity we shall denote the C-group so defined simply by X, where the group law c is understood to be fixed.

A morphism of C-groups (X, c_X) into (Y, c_Y) is a morphism $f: X \to Y$ such that the diagram

$$\begin{array}{ccc} X\pi X & \xrightarrow{f\pi f} & Y\pi Y \\ {\scriptstyle c_X}\downarrow & & \downarrow{\scriptstyle c_Y} \\ X & \xrightarrow[f]{} & Y \end{array}$$

commutes. The class of C-groups with these morphisms constitutes a category; the class of commutative C-groups form a subcategory. Starting from the axioms we can show that a morphism of C-groups commutes not only with the group law, but also with the neutral morphism and the inverse.

Groups in categories of sets, topological spaces, analytic manifolds are represented by general groups, topological groups, Lie groups. Groups in categories of proximity spaces, of which examples (in categories of schemata and formal schemata) will occur in profusion below, form an essential extension of the concept of a group.

Another example is given by the H-spaces of Hopf: they are groups in the category whose objects are topological spaces and whose morphisms are the homotopy classes of continuous mappings.

Let X be a C-group; for any object $Y \in C$ the set $\mathrm{Hom}_C(Y, X)$ is itself a group relative to the composition law $fg = c_X \circ (f\pi g)$, and moreover, this group structure depends functorially (in an obvious sense) on X. If, however, Y is also a C-group, then the set of group morphisms $Y \to X$ is, generally speaking, not a group; this is clear already from the example of ordinary non-commutative groups. Nevertheless, if X is commutative, then the set $\mathrm{Hom}(Y, X)$ (in the category of C-groups) is an abelian group relative to the composition law $f + g = c_X \circ (f\pi g)$.

PROPOSITION 1.1. *The category of commutative C-groups is an additive category.*

The proof consists in a verification of the axioms, which may be left to the reader. We remark that by axiom I the class of C-groups is non-empty: it contains in any case the group e (with the only possible composition law).

4. PROPOSITION 1.2. *The category of (all, or only commutative) C-groups is a category with a product.*

PROOF. Let (X, c_X), (Y, c_Y) be two C-groups and put $Z = X \pi Y$; $c_Z = s \circ (c_X \pi c_Y)$, where $s: (X\pi Y) \pi (X\pi Y) \to (X\pi X) \pi (Y\pi Y)$ is the natural mapping.

We claim that (Z, c_Z) is a C-group, the projections $p_1: Z \to X$ and $p_2: Z \to Y$ are C-group morphisms and define the group (Z, c_Z) as a product $(X, c_X) \pi (Y, c_Y)$ in the category of C-groups (all these statements remain true if we assume that all groups occurring are commutative).

The first two statements hold automatically. Now let (T, c_T) be a C-group and $f: T \to X$, $g: T \to Y$ any C-group morphisms. To establish that (Z, c_Z) is the product of (X, c_X) and (Y, c_Y) we must show that there exists one and only one C-group morphism $k: T \to Z$ such that $f = p_1 \circ h$, $g = p_2 \circ h$. But such a morphism exists and is unique in the category C, because $Z = X \pi Y$. The commutativity with the group law follows immediately.

5. The following – and last – general result which we prove gives a convenient description of the kernel in an additive category of commutative groups.

PROPOSITION 1.3. *Let C be a category with fibre products. Then the additive category of commutative C-groups is a category with kernels: the kernel of the morphism $f: X \to Y$ is $p: X \underset{Y}{\pi} e \to X$ (where p is the projection);*

the fibre product being taken relative to the morphisms $f: X \to Y$, $\eta: e \to Y$.

PROOF. We may define a commutative C-group structure on $X \underset{Y}{\pi} e$ such that p becomes a C-group morphism; we show that p is a monomorphism and finally verify that for every C-group morphism $g: Z \to X$ such that $f \circ g = \varepsilon_Y \circ \eta_Z$, there exists a C-group morphism $h: Z \to X \underset{Y}{\pi} e$ such that $g = p \circ h$.

To begin with the monomorphy of p: it is enough to verify this in the category C. Let h_1, $h_2 \in \mathrm{Hom}(Z, X \underset{Y}{\pi} e)$ and assume that $p \circ h_1 = p \circ h_2 \in \mathrm{Hom}(Z, X)$. Then $h_1 = h_2$, for it follows from the definition that the mapping $h \to p \circ h$ defines a one-to-one correspondence between the set $\mathrm{Hom}(Z, X \underset{Y}{\pi} e)$ and the subset of all morphisms $g \in \mathrm{Hom}(Z, X)$ such that the square in the diagram

$$\begin{array}{ccc} Z & \xrightarrow{\varepsilon} & e \\ & \searrow^{g} & \downarrow \eta_Y \\ X \underset{Y}{\pi} e & \longrightarrow & X \xrightarrow{f} Y \end{array} \qquad (1.1)$$

commutes.

This shows p to be monomorphic. The same diagram shows that $p = \ker f$, provided only that a group structure is defined on $X \underset{Y}{\pi} e$.

The group law c' on the object $X \underset{Y}{\pi} e$ may be defined by the commutative diagram

$$\begin{array}{ccc} X \pi X & \xrightarrow{c} & X \\ {\scriptstyle p \pi p} \uparrow & & \uparrow {\scriptstyle p} \\ (X \underset{Y}{\pi} e) \pi (X \underset{Y}{\pi} e) & \xrightarrow{c'} & X \underset{Y}{\pi} e \end{array}$$

Since p is a monomorphism, c' is uniquely defined if it exists at all. To prove the existence it is enough to verify the commutativity of the diagram (1.1), where we have put $Z = (X \underset{Y}{\pi} e) \pi (X \underset{Y}{\pi} e)$, $g = c \circ (p \pi p)$, i.e., we must verify that $f \circ c \circ (p \pi p) = \eta \circ \varepsilon$. But f is a C-group morphism, hence $f \circ c = c_Y \circ (f \pi f)$. Thus, it is enough to verify that $c_Y \circ (f \pi f) \circ (p \pi p) = \eta \circ \varepsilon$, for which in turn it is enough to check the commutativity of the diagram

$$\begin{array}{ccc} X\pi e & \longrightarrow & e \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle \varepsilon} \\ X & \longrightarrow & Y \end{array}$$

which follows from the fact that in (1.1) the commutativity of the triangle and the square are equivalent.

To show that $X \underset{Y}{\pi} e$ with the composition law c is a C-group it is enough to define morphisms $\varepsilon' : e \to X \underset{Y}{\pi} e$ and $a' : X \underset{Y}{\pi} e \to X \underset{Y}{\pi} e$ and show that they satisfy the axioms. We confine ourselves to the definitions and leave the verification to the reader. The morphism ε' is obtained from the diagram (1.1) if we put $Z = e$, $g = \varepsilon$ (the commutativity of the square follows because the group morphism f maps the neutral element to the neutral element). The morphism a' is obtained from the diagram

$$\begin{array}{ccc} X & \xrightarrow{a} & X \\ {\scriptstyle p}\uparrow & & \uparrow{\scriptstyle p} \\ X\pi e & \xrightarrow{a'} & X\pi e \\ {\scriptstyle Y} & & {\scriptstyle Y} \end{array}$$

by commutativity, for the proof of which we need only check the commutativity of the square in (1.1), when $Z = X \underset{Y}{\pi} e$, $g = a \circ p$; since $f \circ a \circ p = a \circ f \circ p$, it follows from this that $f \circ p = \eta \circ \varepsilon$. Here we have used the fact that group morphisms always commute with a.

This completes the proof.

We remark that with appropriate changes in the definition of kernel this proposition remains true in much more general situations, for instance in the category of all C-groups.

§2. Algebraic and formal groups. Bialgebras

1. Below we shall make use of the language and elementary properties of schemata, which is presented in the first chapter of the book by Grothendieck and Dieudonné [39].

Let k be a field. A schema over Spec k will be called a *k-schema*. We recall that a k-schema is said to be *algebraic* if there exists a finite covering by affine k-schemata, each of which is isomorphic to the spectrum of a finitely generated k-algebra. Algebraic k-schemata differ from ordinary algebraic varieties over the field k as defined by Serre in this fundamental respect : that their structure sheaf may admit nilpotent elements: a schema without nilpotent elements in its structure sheaf is said to be *reduced*. An affine k-schema is said to be *artinian* if it is isomorphic to the spectrum of a finite-dimensional k-algebra. Artinian k-schemata, affine k-schemata, algebraic k-schemata all form categories with a fibred product and final object Spec k. Hence we may apply the results and definitions of the last section. A group in such a category is correspondingly called an artinian k-group, affine k-group or algebraic k-group. (In the sequel we shall sometimes omit the reference to the field k.) All these three categories of commutative k-groups are additive

categories with kernel.

Let A be a noetherian complete local ring with residue class field k; assume also that k and A have the same characteristic. By a *formal k-schema* we shall understand here the formal spectrum Spf A (this usage, considerably more restricted than in Grothendieck, is justified by the fact that we shall never have to consider formal schemata other than these). Formal k-schemata again form a category with fibre product and final object. A group in this category is called a formal k-group. The category of commutative formal k-groups is an additive category with kernel. (From results of Gabriel mentioned below it follows that owing to the admission of nilpotent elements in the coordinate rings this category is even abelian. The reduction of commutative formal k-groups considered by Dieudonné results in a non-abelian sub-category.)

2. With every algebraic k-group X a corresponding formal k-group $\hat{X}$ can be associated. This correspondence is functorial and forms the precise analogue of the correspondence between a global Lie group and a local Lie group in the classical theory. It is realized as follows. The structural morphism π: Spec $k \to X$ defines a certain closed point x in the space X (the neutral element in the group of geometric points of this space). The local ring of the structure sheaf of X over this point is denoted by the symbol o_x. Let $\hat{X} =$ Spf $\hat{o}_x$ be the formal spectrum of the completion of the ring o_x relative to the topology defined by the powers of the maximal ideal. $\hat{X}$ is called the formal completion of X (along the point x). The composition law $X \pi X \to X$ induces a composition law $\hat{X} \pi \hat{X} \to \hat{X}$ (defined so that the completion $\hat{o}_{(x,x)}$ of the local ring at the point $(x, x) \in X \pi X$ is naturally isomorphic to $\hat{o}_x \hat{\otimes} \hat{o}_x$), which is a group law. The mapping $X \Rightarrow \hat{X}$ is a covariant functor on the category of algebraic k-groups with values in the category of formal k-groups. A formal group of the form $\hat{X}$ is said to be algebroid.

By the dimension of a formal group Spf A we understand the (Krull) dimension of the ring A.

The basic aim of this paper is to study the structure of commutative formal groups and, in particular, algebroid groups. We recall that in the classical case a commutative local Lie group is completely defined by its dimension, and every local group (not necessarily commutative) is obtained from a certain global Lie group. Both these statements can be carried over, with certain reservations, to k-groups, where k is algebraically closed of characteristic zero, but break down completely when k has finite characteristic, which is essentially the one we shall consider. In particular, in each dimension there exists an infinite set of continuous systems of non-isomorphic commutative formal groups. In general they are non-algebroid, but they contain algebroid groups as direct summands.

3. Let $X =$ Spec A be an affine k-schema and put $X \pi X =$ Spec$(A \underset{k}{\otimes} A)$. It follows that the given composition law on X is equivalent to a k-algebra homomorphism $c: A \to A \underset{k}{\otimes} A$. The associativity axiom for this law consists in the commutativity of the diagram

$$\begin{array}{ccc} A\otimes A\otimes A & \xrightarrow{c\otimes 1} & A\otimes A \\ {\scriptstyle 1\otimes c}\uparrow & & \uparrow{\scriptstyle c} \\ A\otimes A & \xleftarrow{\quad c\quad} & A \end{array} \tag{1.2}$$

The axiom of a left neutral element asserts the existence of a homomorphism $\eta: A \to k$ such that the diagram (where $\varepsilon: k \to A$ is the canonical embedding and $d: A \otimes A \to A$ the homomorphism of multiplication)

$$\begin{array}{ccc} A\otimes A\otimes A & \xrightarrow{(\varepsilon\circ\eta)\otimes 1} & A\otimes A \\ {\scriptstyle c}\uparrow & {\scriptstyle 1_A} & \downarrow{\scriptstyle d} \\ A & \longrightarrow & A \end{array} \tag{1.3}$$

commutes. Finally, the axiom of a left inverse element asserts the existence of an automorphism $a: A \to A$ such that the diagram

$$\begin{array}{ccc} A\otimes A & \xleftarrow{a\otimes 1} & A\otimes A \\ {\scriptstyle d}\downarrow & {\scriptstyle \varepsilon\circ\eta} & \uparrow{\scriptstyle c} \\ A & \longleftarrow & A \end{array} \tag{1.4}$$

commutes. The diagrams (1.2)–(1.4) represent the axioms of a group law of composition on $X = \operatorname{Spec} A$, translated into the language of the coordinate ring A. In the same way the affine group structure on X is equivalent to the provision of the linear space A over k with two linear mappings d and c:

$$A \underset{k}{\otimes} A \xrightarrow{d} A \xrightarrow{c} A \underset{k}{\otimes} A, \tag{1.5}$$

linear homomorphisms ε and η:

$$k \xrightarrow{\varepsilon} A \xrightarrow{\eta} k, \tag{1.6}$$

and a mapping

$$a: A \longrightarrow A, \tag{1.7}$$

together with the axioms imposed on the pair (d, ε) (giving the algebra structure on A) and on the pair (c, η) (giving a coalgebra structure on A induced by the composition law of the schema X), which are mutually dual, since each is obtained from the other by reversing all arrows, while the axiom for a is self-dual. If we take only the case when A is a commutative k-algebra, it follows that complete symmetry prevails only for commutative affine groups, for which the mapping c is symmetric.

In view of this symmetry we define a bialgebra [1] to be an object consisting of a linear space A, provided with the structure consisting of the mappings (1.5)–(1.7), which satisfy the axioms for the laws of composition of the algebra and the coalgebra and the axiom (1.4); we shall also say that the composition laws c, d commute. The class of bialgebras over a field k constitutes a category whose morphisms are linear mappings of the underlying spaces that commute with all the mappings defining the bialgebra structure. The correspondence that associates with the affine k-group $X = \operatorname{Spec} A$ its coordinate ring A with the diagonal mapping (we shall sometimes call A simply the *ring* of the group X) is a functor, which defines a

[1] This term was suggested to the author by M. Lazard in a private conversation. Different variants of this concept, arising from the absence of the commutative law and the introduction of a grading and a filtration, appear in the literature under the names of Hopf algebra and hyperalgebra.

duality between the category of commutative affine k-schemata and the category of bialgebras. In this correspondence artinian groups correspond to finite-dimensional bialgebras and vice versa.

4. In a completely analogous manner it can be shown that there is a correspondence between group laws of composition and the rings of formal k-groups Spf $A = X$. The only difference consists in this: that the product of formal schemata corresponds to the *completion* of the tensor product of their rings and in the diagrams (1.2)–(1.5) the sign $\otimes$ has to be replaced by the sign $\hat{\otimes}$ denoting completion of the product.

5. Let A be a finite-dimensional bialgebra and denote by $A^* = L(A, k)$ the space of linear forms on A. We consider the diagrams of linear mappings dual to (1.5)–(1.6)

$$A^* \underset{k}{\otimes} A^* \xrightarrow{c^*} A^* \xrightarrow{d^*} A^* \underset{k}{\oplus} A^*, \tag{1.5*}$$

$$k \xrightarrow{\eta^*} A^* \xrightarrow{\varepsilon^*} k. \tag{1.6*}$$

We noted in 3. that the symmetry of the axiom relating a to the pairs (d, ε) and (c, η) allows us to conclude that the space A^* with the mappings c^*, d^*, η^*, ε^* constitutes a bialgebra. We shall call this the (linear) dual of the bialgebra A.

Let $X = \mathrm{Spec}\ A$ be an artinian k-group. We shall sometimes call the bialgebra A the ring of the group X and the bialgebra A^* the algebra of the group X. This usage agrees with that generally accepted in the particular case when $A = \mathrm{Map}(G, k)$, where G is any finite group and the diagonal of A is induced by the group law of composition $G \times G \to G$. Clearly in this case A^* is isomorphic to the group algebra $k[G]$.

The artinian group $X^* = \mathrm{Spec}\ A^*$ will sometimes be called the group (linearly) dual to X.

6. Let k be a perfect field of characteristic $p \neq 0$. In algebraic geometry the places where artinian groups occur are as kernels and cokernels of ordinary algebraic groups, as coefficients in different cohomology groups etc. For us they are important, because a formal group over a field of characteristic $p \neq 0$ can be expressed as the union of its artinian subgroups.

LEMMA 1.1. *Let $X = \mathrm{Spf}\ A$ be a formal k-group and m the maximal ideal of the algebra A. Write $X_n = \mathrm{Spec}\ A/m^{p^n}$, $i_n: X_n \to X$ the canonical embedding of k-schemata (X_n may be considered either as formal or as affine schema). Then there exists a composition law $c_n: X_n \pi X_n \to X_n$ which turns X_n into an artinian group and such that i_n is an injective morphism of k-groups. The formal group X with the morphisms $i_n: X_n \to X$ is the inductive limit of the system of artinian formal groups X_n and homomorphisms $X_n \to X_m$ $(n > m)$, induced by the algebra homomorphisms $A/m^{p^n} \to A/m^{p^m}$.*

PROOF. We have to define a diagonal homomorphism $c_n: A_n \to A_n \otimes A_n$, where $A_n = A/m^{p^n}$, so that the diagram

$$\begin{array}{ccc} A & \xrightarrow{c} & A \hat{\otimes} A \\ p\downarrow & & \downarrow p\hat{\otimes} p \\ A_n & \xrightarrow{c_n} & A_n \hat{\otimes} A_n \end{array}$$

remains commutative. (Here c is the composition law of the coalgebra A,

$p: A \to A_n$ is the natural projection.) For any element $a \in A$ we must therefore set $c_n(a) = (p \hat{\otimes} p) \circ c \circ p^{-1}(a)$. To verify that the result is independent of the choice of $p^{-1}(a)$ amounts to verifying the inclusion $c(\ker p) \subset \ker(p \hat{\otimes} p)$. Now $\ker(p \hat{\otimes} p) = mp^n \hat{\otimes} A + A \hat{\otimes} mp^n$; on the other hand, if $x \in mp^n$, then $x = \Sigma a_i x_i p^n$, where $a_i \in A$, $x_i \in m$, so that $c(x) = \Sigma c(a_i) c(x_i) p^n \in mp^n \hat{\otimes} A + A \hat{\otimes} mp^n$, because $c(x_i) - x_i \hat{\otimes} 1 - 1 \hat{\otimes} x_i \in m \hat{\otimes} m$. (Clearly we have $c(x) = a_1 \hat{\otimes} x_1 + x_2 \hat{\otimes} a_2 + \Sigma y_i \hat{\otimes} y_j$, where $a_1, a_2 \in k$; $x_1, x_2, y_k \in m$. From the axiom of left and right neutrals it then follows that $a_1 = a_2 = 1$, $x_1 = x_2 = x$.)

The remaining assertions of the lemma are obtained by verifying the definitions.

7. The lemma just established allows us to define the notion of an *algebra* for an arbitrary (not necessarily artinian) formal group. Thus let $X = \operatorname{Spf} A$, $A = \lim A_n$, where $A_n = A/mp^n$. We put $A^* = \lim(A/mp^n)^*$ and call the bialgebra A^* the algebra[1] of the formal group X. Clearly A^* is the union of finite-dimensional bialgebras. Following Gabriel [37] we shall call a bialgebra with these properties a Dieudonné bialgebra.

8. Let $X = \operatorname{Spec} A$ be an affine k-schema and k' a field containing k. The affine schema $X \underset{k}{\pi} \operatorname{Spec} k' = \operatorname{Spec}(A \underset{k}{\otimes} k')$, considered as k'-schema, is denoted by $X \otimes k'$. Similar definitions apply to algebraic and formal schemata. The transition from the k-schema X to the k'-schema $X \otimes k'$ is called change of base field. Similar definitions apply to formal groups. The operation of change of base field is a covariant functor that preserves tensor products, kernels and cokernels of mappings of linear spaces and thus commutes with the operation $A \Rightarrow A^*$. Hence it follows that the change of base field takes k-groups to k'-groups and commutes with taking direct products, kernels and cokernels of morphisms of commutative k-groups. Further, we can change the base field of a group by taking the tensor product of its algebra by k'. Finally, changing the base field commutes with taking the completion of a local ring and hence with passing from an algebraic group to its completion.

§3. The structure of commutative artinian groups

1. We now give a brief account of the fundamental result of P. Gabriel on the structure of commutative artinian groups over a perfect field k.

Let $X = \operatorname{Spec} A$ be a commutative artinian k-algebra, $\Omega \supset k$ the algebraic closure of k, and Γ the Galois group of Ω over k with the Krull topology. The set $\operatorname{Hom}(\operatorname{Spec} \Omega, X) = G_X$ is a commutative group; this group is finite: for in any artinian k-algebra A there are only a finite number of maximal ideals m, and the field A/m is an extension of finite degree over k. Moreover, the group Γ acts on G_X: for any elements $g \in G_X$ and $\gamma \in \Gamma$ the element $g^\gamma \in G_X$ is defined as the composite morphism $\operatorname{Spec} \Omega \xrightarrow{\gamma} \operatorname{Spec} \Omega \xrightarrow{g} X$. The resulting operation $X \Rightarrow G_X$ is a covariant functor from the category A of artinian commutative groups to the category of finite right Γ-modules. It is not hard to see that this functor is additive.

Conversely, let G be a finite Γ-module. We consider the set

[1] In the literature called hyperalgebra.

$A_G = \mathrm{Map}_\Gamma(G, \Omega)$ consisting of all functions f on G with values in Ω, subject to the condition $f(g^\gamma) = f(g)^\gamma$ for any $g \in G$ and $\gamma \in \Gamma$. Clearly this set A_G is a k-algebra. It is finite-dimensional, for given any $g \in G$, the values $f(g)$, for all f, lie in a finite extension of the field k, corresponding to the stabilizer of g in Γ. The diagonal mapping $A_G \to A_G \underset{k}{\otimes} A_G$ induces a composition law $G \times G \to G$ and we shall make the identification $A_{G \times G} = A_G \underset{k}{\otimes} A_G$. It is easily verified that $X_G = \mathrm{Spec}\, A_G$ is a commutative artinian group. Clearly this group is reduced. The covariant additive functor $G \rightrightarrows X_G$ from the category of finite right Γ-modules to the category of reduced commutative artinian groups A_{red} is an equivalence of these categories.

This construction provides a description of reduced groups and shows in particular that the category A_{red} is abelian.

2. We recall that for any schema X the symbol X_{red} denotes the maximal reduced subschema $X_{red} \subset X$.

Since over a perfect field $(X \pi Y)_{red} = X_{red} \pi Y_{red}$, it follows that for any group X the schema X_{red} is a subgroup; Gabriel shows that this subgroup is a direct factor: $X = X_{red} \pi X_{loc}$, where X_{loc} is the spectrum of a bialgebra which qua algebra is local; this decomposition is unique and gives rise to a natural identification $\mathrm{Hom}(X, Y) = \mathrm{Hom}(X_{red}, Y_{red}) \times \mathrm{Hom}(X_{loc}, Y_{loc})$. This proves that the category A is equivalent to the direct product of the category A_{red} and the category A_{loc} of local groups (the spectra of locally finite-dimensional bialgebras).

Let $X = \mathrm{Spec}\, A \in A_{red}$; we consider the linear dual group X^*. Its decomposition into reduced and local components $X^* = X^*_{red} \pi X^*_{loc}$ induces a dual decomposition $X = X_r \pi X_{rl}$, where the groups X_r and X_{rl} are defined so that $X_r \in A_{red}$, $X_r^* \in A_{red}$ and $X_{rl} \in A_{red}$, $X_{rl}^* \in A_{loc}$. Similarly, for any group $X \in A_{loc}$ we obtain a canonical decomposition $X = X_{lr} \pi X_l$, where $X_{lr} \in A_{loc}$, $X_{lr}^* \in A_{red}$, and $X_l \in A_{loc}$, $X_l^* \in A_{loc}$.

Summing up we have the following result: the category A is equivalent to the product of four subcategories:

A_r – the category of reduced groups $X \in A$ such that X^* is reduced,

A_{rl} – the category of reduced groups $X \in A$ such that X^* is local,

A_{lr} – the category of local groups $X \in A$ such that X^* is reduced,

A_l – the category of local groups $X \in A$ such that X^* is local.

The structure of the first three categories is obtained by the construction under 1. A_r is equivalent to the category of finite Γ-modules whose order is prime to the characteristic p of the field k; A_{rl} is equivalent to the category of finite Γ-modules whose order is a power of p; A_{lr} is equivalent to A_{rl}° (the equivalence being defined by the functions of the linear dual). All three categories are abelian.

EXAMPLE. Let k be an algebraically closed field. Then the group Γ is trivial. It follows that A_r consists of the spectra of group algebras of finite groups of order prime to p, and A_{lr} of the spectra of group algebras of p-groups. The unique simple object in A_{lr} is $G_p = \mathrm{Spec}\, k[Z/Zp] = \mathrm{Spec}\, k[x]/(x^p)$, with composition law $c(x) = x \otimes 1 + 1 \otimes x$. Every object in A_{rl} has a composition series whose factors are isomorphic to G_p.

3. Let A, B be finite-dimensional bialgebras over k and σ an

automorphism of k; then a σ-morphism of bialgebras $f: A \to B$ is a multilinear mapping of linear spaces satisfying

$$f(\alpha a) = \alpha^{\sigma} f(a), \quad a \in A, \quad \alpha \in k$$

and compatible with multiplication and the diagonal mapping:

$$f(ab) = f(a)\, f(b), \quad (f \otimes f)(c_A(a)) = c_B(f(a)).$$

For any σ-morphism f we define the dual σ^{-1}-morphism $f^*: B^* \to A^*$ by setting

$$\langle a, f^*(b)\rangle = \langle f(a), b\rangle^{\sigma^{-1}}, \quad a \in A, \quad b \in B^*,$$

where the brackets $\langle\ \rangle$ denote the canonical bilinear form defined by duality on A, A^* and B, B^*. The verification that the correspondence $f^*(b)$ so defined is a linear function on B, i.e. an element of B^*, and that f^* is compatible with multiplication and the diagonal mapping on B^* and A^*, is an exercise in duality.

Let $m > 0$ be an integer and A a bialgebra. The endomorphism $m1_X$ of multiplication by m in the group $X = \operatorname{Spec} A$ is defined as the composite mapping

$$X \xrightarrow{d_m} \underbrace{X\pi \ldots \pi X}_{m \text{ factors}} \xrightarrow{c_m} X,$$

where d_m is the diagonal in the m-fold product and c_m the $(m-1)$-fold iteration of the composition law $c = c_2: X\pi X \to X$.

The endomorphism $m1_X$ induces on A an endomorphism $m1_A$ of the bialgebra A:

$$A \xrightarrow{c_m} \underbrace{A \otimes \ldots \otimes A}_{m \text{ factors}} \xrightarrow{d_m} A,$$

where $d_m(\alpha_1 \otimes \ldots \otimes \alpha_m) = \alpha_1 \ldots \alpha_m$ is the product, and c_m is defined by induction by

$$c_m = (c_2 \otimes \underbrace{1_A \otimes \ldots \otimes 1_A}_{m-1 \text{ factors}}) \circ c_{m-1}.$$

Let $p > 0$ be the characteristic of the field k and $\sigma: x \to x^p$ the Frobenius automorphism of k. For every bialgebra A over k we define a σ-morphism $F_A: A \to A$ by the formula

$$F_A(a) = a^p, \quad a \in A,$$

and a σ^{-1}-morphism $V_A: A \to A$ by duality:

$$V_A = (F_{A^*})^*.$$

PROPOSITION 1.4. *For any finite bialgebra A the morphism $p1_A$ of multiplication by p can be expressed as the product of the σ-morphism F_A and the σ^{-1}-morphism V_A, taken in either order.*

PROOF. Firstly we have, for any elements $a \in A$, $a' \in A^*$,

$$\langle a', V_A \circ F_A a\rangle = \langle F_{A^*} a', F_A a\rangle^{1/p} = \langle a'^p, a^p\rangle^{1/p} =$$
$$= \langle d_p(a' \otimes \ldots \otimes a'), a^p\rangle^{1/p} = \langle a' \otimes \ldots \otimes a', (c_p a)^p\rangle^{1/p}.$$

Let $a_1, \ldots, a_n$ be a k-basis of A. Then

$$c_p(a) = \sum \alpha_{i_1 \ldots i_p} a_{i_1} \otimes \ldots \otimes a_{i_p},\ \alpha_{i_1 \ldots i_p} \in k,$$

where $\alpha_{i_1 \ldots i_p} = \alpha_{s(i_1 \ldots i_p)}$ for any permutation s of the indices, because the composition law is commutative. The number of different permutations is one if $i_1 = \ldots = i_p$ and otherwise is divisible by p. Hence

$$c_p(a) = \sum_{i=1}^{N} \alpha_{i \ldots i} a_i \otimes \ldots \otimes a_i$$

and

$$\langle a' \otimes \ldots \otimes a',\ (c_p a)^p \rangle^{1/p} = \langle a' \otimes \ldots \otimes a',\ \sum_{i=1}^{N} \alpha_{i \ldots i}^p a_i^p \otimes \ldots \otimes a_i^p \rangle^{1/p} =$$

$$= \sum_{i=1}^{N} \alpha_{i \ldots i} \langle a',\ a_i^p \rangle = \langle a',\ (d_p \circ c_p)\, a \rangle = \langle a',\ (p 1_A)\, a \rangle.$$

Thus, $V_A \circ F_A = p 1_A$; hence $V_{A^*} \circ F_{A^*} = p 1_{A^*}$ and so by duality, $F_A \circ V_A = p 1_A$, which establishes the proposition.

4. The result just proved may be used to give a simple description in terms of groups of the categories A_r, A_{rl}, A_{lr}, A_l introduced under 2. The morphism Spec $k \to$ Spec k induced by σ will be denoted by the same letter σ and the $\sigma^{\pm 1}$-morphisms of the group $X =$ Spec A induced by F_A and V_A will be denoted by F_X and V_X respectively. We shall say that the τ-morphism $f: A \to A$ is nilpotent if for sufficiently high $n > 0$ we have $f^n(A) = k \subset A$ in the set-theoretical sense. (We say in this case that f^n annihiliates A or $X =$ Spec A respectively.) Similarly we say that the τ-morphism f is an automorphism if $f(A) = A$.

PROPOSITION 1.5. (a) *The group $X \in A$ lies in A_r if and only if F_X and V_X are both automorphisms.*

(b) *The group $X \in A$ lies in A_{rl} if and only if F_X is nilpotent and V_X is an automorphism.*

(c) *The group $X \in A$ lies in A_{lr} if and only if F_X is an automorphism and V_X is nilpotent.*

(d) *The group $X \in A$ lies in A_l if and only if F_X and V_X are both nilpotent.*

The verification of these statements is not difficult and may be left to the reader.

We note the following important fact: when the group X is defined over the prime field, then F_X and V_X are ordinary endomorphisms.

§4. The Dieudonné module of a formal group

1. In what follows we shall be concerned chiefly with the categories A_r and A_l, both of which consist of formal artinian groups. The first, as we have seen, is abelian and its structure, at any rate over an algebraically closed field, is fairly clear.

Gabriel proved first of all that the category A_l is also abelian. The proof is of a rather technical character: with the help of Proposition 1.3 we can explicitly determine the image and co-image of any morphism in the category of bialgebras, and from the specific properties of the groups in

A_l we can immediately infer the isomorphism of the image and the coimage.

Lemma 1.1 shows that any formal group is an inductive limit of artinian formal groups. The category A_{loc} is not closed with respect to inductive limits; however, there is a general construction that allows us to embed an arbitrary abelian category C in an abelian category Ind C in which inductive limits exist and the limit of an exact sequence is an exact sequence (cf. Grothendieck [46], Gabriel [35], [37]). In particular, if the category C is equivalent to the product of two abelian subcategories C_1 and C_2, then Ind C is equivalent to the product of Ind C_1 and Ind C_2. The application of this general argument to the category $A_{loc} = A_{lr} \pi A_l$ yields the following result, which in a much weaker form was first proved by Dieudonné [25]. To formulate it we require the following definition.

A commutative formal group X is called a *toroidal* group if X belongs to the category Ind A_{lr}. A group X that belongs to the category Ind A_l is called a Dieudonné group.

We note that if we change the field of constants, a toroidal group goes over into a toroidal group and a Dieudonné group into a Dieudonné group, as long as we limit ourselves to perfect fields.

THEOREM 1.1. *The category of commutative formal k-groups is equivalent to the product of the category of toroidal groups and the category of Dieudonné groups. All are abelian categories.*

This shows, in particular, that every commutative formal group is essentially uniquely decomposable into a direct product of a toroidal group and a Dieudonné group, and that there are no non-trivial morphisms between Dieudonné groups and toroidal groups.

Every subgroup of a toroidal group and every product of toroidal groups is again toroidal.

If the field k is algebraically closed, then by the results under 1. and 2. the category A_{lr} is equivalent to the category of finite abelian p-groups. The structure of the latter is well known; if we translate the information on finite p-groups and their projective limits into the language of the category of toroidal formal groups we reach the following conclusions.

Set $X = \operatorname{Spf} k[[x]]$ and let the composition law be defined by the diagonal mapping $c(x) = x \hat{\otimes} 1 + 1 \hat{\otimes} x + x \hat{\otimes} x$. The formal group T thus described is said to be *multiplicative*. If the field k is algebraically closed, then T is just the injective hull of the simple artinian group G_p (cf. § 3.2 example). Further we have

THEOREM 1.2. *Every toroidal group over an algebraically closed field is isomorphic to a subgroup of a direct sum of a finite number of multiplicative groups. A reduced toroidal group over an algebraically closed field is isomorphic to a direct sum of a finite number of multiplicative groups.*

This result justifies the use of the word 'toroidal'. It was first obtained by Dieudonné.

2. It remains to investigate formal Dieudonné groups. They constitute a subcategory of Ind A_l, and for a description of the latter Gabriel has introduced a general technique for reducing abelian categories to categories of modules.

As already stated, Ind A_l is an abelian category admitting inductive limits, and the inductive limit of an exact sequence is again an exact

sequence. Moreover, Ind A_l has a class of generators of finite length (the objects of A_l). Gabriel calls an abelian category with these properties locally finite. (We note that Ind A_l admits a convenient realization as the category of Dieudonné bialgebras; cf. § 2.7)

A general result of Gabriel [37] states that on a locally finite category a certain variant of Pontrjagin duality can be defined.

Namely, let C be a locally finite category, (S_α) the family of all simple objects of C (in which each simple object occurs just once) and I_α the injective hull of S_α. We set $I = \varkappa I_\alpha$; I represents in a certain sense a 'universal' injective object. Denote by E the endomorphism ring of I. In E we can introduce a natural topology by taking as a base of neighbourhoods of zero the system of all left ideals $l \subset E$ of finite colength ($\operatorname{long}_E E/l < \infty$). E is complete with respect to this topology. We denote by M_E the category of complete topological left E-modules, whose topology is linear and has a base of neighbourhoods of zero consisting of all submodules of finite colength. Then Gabriel's result can be formulated as follows:

THEOREM 1.3. *The contravariant functor* $X \Rightarrow \operatorname{Hom}(X, I)$ *defines a duality between the categories* C *and* M_E.

3. To apply Gabriel's theorem to the category Ind A_l we have to compute the ring $E = E_k$ (where k is the base field).

Firstly, in Ind A_l there is just one simple object S_k, which occurs as kernel of the Frobenius endomorphism of the additive group. Explicitly,

$$S_k = \operatorname{Spec} k[x]/(x^p), \qquad c(x) = x \otimes 1 + 1 \otimes x.$$

The object S_k is obtained from the analogous object S defined over the prime field by changing the field of constants. The injective hull I_k of S_k is isomorphic to $I \otimes k$, where I is the injective hull of S. The object I can be computed explicitly. Thus, consider the formal group $W_n = \operatorname{Spec} A_n$ (completion of the algebraic group of additive Witt vectors of length n). Let $m_n \subset A_n$ be the maximal ideal. Denote by $W^{(n)}$ the artinian formal group $\operatorname{Spec} A_n/m_n^p$ and consider the morphism

$$\gamma_n : \hat{W}^{(n)} \longrightarrow \hat{W}^{(n+1)},$$

where γ_n is induced by the composition of the morphism V of W_{n+1} (we recall that W_n is defined over the prime field!) and the natural mapping $A_{n+1} \to A_n$ of the rings of the Witt groups (restriction). Clearly $W^{(1)} \approx S$; it can be shown that the injective hull I of S is isomorphic to the inductive limit $\varinjlim W^{(n)}$ with respect to the morphisms γ_n. After this the complete calculation of the ring E_k presents no difficulties.

We summarize the result obtained for formal groups.

THEOREM 1.4. (1) *The ring* E_k *is isomorphic to the ring of non-commutative formal power series of the form*

$$a = w + \sum_{r=1}^{\infty} a_r F^r + \sum_{s=1}^{\infty} b_s V^s, \qquad w,\ a,\ b \in W(k)$$

with multiplication rules

$$VF = FV = p, \qquad Fw = w^\sigma F, \qquad wV = Vw^\sigma,$$

where $W(k)$ is the ring[1] *of infinite Witt vectors over the field k*

$$(w_1, w_2, w_3, \ldots)^\sigma = (w_1^p, w_2^p, w_3^p, \ldots).$$

(2) *The functor $X \Rightarrow \mathrm{Hom}(X, I_k)$ defines a duality between the category of Dieudonné k-groups and the category of finitely generated left E-modules M for which the module M/FM has finite length. The group X is reduced if and only if $Fx = 0$, $x \in M(X)$, implies that $x = 0$.*

(3) *If $k' \subset k$ is any perfect field, then $X_{k'} = X \otimes k'$. The functor $X \Rightarrow X_{k'}$ changing the field of constants is dual to the functor $M \Rightarrow E_{k'} \underset{E_k}{\otimes} M$ changing rings. (In other words, there is an isomorphism $M(X \otimes k') \approx E_{k'} \underset{E_k}{\otimes} M(X)$ which is compatible with morphisms)*

We shall not give a complete proof of this theorem, but confine ourselves to some comments. Firstly, on the determination of the ring E_k. The elements F, V of this ring are defined so that on the group $\hat{W}^{(n)} = X$ they induce the corresponding endomorphisms F_X, V_X (cf. end of § 3). $W(k)$ acts on $\hat{W}^{(n)} \otimes k$ by multiplication of Witt vectors. Further, on every group $\hat{W}^{(n)} = X$ the endomorphisms F_X, V_X are nilpotent. Therefore, in E_k the powers F^n, V^n tend to zero in the topology generated by the ideals $\mathrm{Hom}(I \otimes k/\hat{W}^{(n)} \otimes k, I \otimes k) \subset \mathrm{Hom}(I \otimes k, I \otimes k)$, consisting of the endomorphisms whose kernels contain the canonical image of $\hat{W}^{(n)} \otimes k$ in $I \otimes k$. Thus, the ring $E = W(k)_\sigma[[F, V]]$ with the given commutation rule is represented in a natural way in E_k; this representation turns out to be a ring isomorphism.

The assertion that for the formal group X the module M/FM is of finite length is equivalent to the ring of X being noetherian. For if $X = \mathrm{Spf}\, A$ and $m \subset M$ is the maximal ideal, then it is easily verified that $M/FM = \mathrm{Hom}(\mathrm{Spec}\, A/m^p, I)$. The module $\mathrm{Hom}(\mathrm{Spec}\, A/m^p, I)$ has finite length if and only if the algebra A/m^p is finite-dimensional; this last condition, as is well known, is equivalent to A being noetherian. We remark here that if X is reduced, then its dimension agrees with the length of the E-module M/FM.

If the group X is not reduced, then it follows from the exact sequence $0 \to X_{red} \to X \to X/X_{red} \to 0$ that the module $M(X)$ has a submodule $\mathrm{Hom}(X/X_{red}, I_k)$ of finite length, because X/X_{red} is artinian. Such a submodule is annihilated by a certain power of F. Conversely, let $Fx = 0$, $x \in M(X)$, $x \neq 0$, then the submodule $E_k x$ of $M(X)$ has finite length, and we find that X has an artinian factor group; but then the ring of this factor group is embedded in the ring of X, and therefore X cannot be reduced.

The final statement of the theorem can be verified without difficulty.

4. Theorem 1.4 shows that E_k-modules play the same role in the theory of commutative formal groups that Lie algebras play in the theory of local Lie groups.

A large part of the subsequent exposition is devoted to the study of Dieudonné modules: the further basic results can without difficulty be

[1] $W(k)$ is a complete local ring of zero characteristic with maximal ideal $pW(k)$ and residue class field $W(k)/pW(k) \approx k$. These properties of $W(k)$ determine it uniquely; σ is the unique automorphism inducing the automorphism of raising to p-th powers in the residue class field k.

translated into the language of formal groups. We shall provide here a small dictionary for such a translation.

The general principle of the terminology consists in this: that we employ the same word to denote corresponding concepts of groups and their Dieudonné modules.

In particular, the *dimension* of a module is the dimension of the corresponding group; a module is said to be *reduced* if the corresponding group is reduced; a module is *unipotent* if the group is unipotent etc. Following Barsotti [13], we shall call a formal group X *equidimensional* if the kernel of the endomorphism of multiplication by p on X is artinian. Thus, a Dieudonné module M is equidimensional if and only if M/pM has finite length (and is therefore artinian).

In the sequel an important role will be played by the category of formal groups over modules of the subcategory A_{loc}, consisting of artinian formal groups. We shall not define here the concept of a factor category, which is described in the works of Grothendieck [44] and Gabriel [36], but confine ourselves to the following remarks. We shall call the formal groups X, Y *isogenous* if their images in the factor category mod A_{loc} are isomorphic. A morphism $X \to Y$ is called an *isogeny* if its image in the factor category mod A_{loc} is an isomorphism.

In terms of the category of formal groups, to say that X and Y are isogenous amounts to asserting the existence of subgroups $X_0 \subset X$, $X' \subset X$ and $Y_0 \subset Y$, $Y' \subset Y$ satisfying the following conditions:

(a) the groups X_0, Y_0 and X/X', Y/Y' are artinian,

(b) the groups X'/X_0 and Y'/Y_0 are isomorphic.

It is clear that isogeny is an equivalence relation. The formulation of the corresponding concept for Dieudonné modules may be left to the reader. The relation of isogeny (modules and groups) will henceforth be denoted by the symbol $\sim$, and the relation of isomorphism by $\approx$.

The notion of isogeny for algebraic groups is defined in exactly the same way as for formal groups. A morphism between algebraic groups is an isogeny if and only if the corresponding morphism between formal groups is an isogeny. Algebroid formal group may be isogenous (and also isomorphic) without the corresponding algebraic groups being isogenous. Nevertheless we have the following result on the extension of 'local' isogenies to global isogenies (which is known to be false for general morphisms of formal groups).

PROPOSITION 1.6. *Let $\hat{X}$ be the completion of an algebraic group X and $\varphi: X \to X'$ an isogeny-epimorphism of formal groups. Then there exists an isogeny $f: X \to Y$ of algebraic groups such that X' is isomorphic to the completion $\hat{Y}$ and the isogeny φ is the isomorphic completion $\hat{f}$ of f.*

In the case when X is reduced this result follows from the Barsotti-Serre theory of inseparable isogenies. In the general theory it is a consequence of the theorem on the existence of a factor-group X/X_0, where $X_0 \subset X$ is an algebraic subgroup (in particular, a locally artinian subgroup; cf. the report by Grothendieck [43] and the paper by Cartier [16]). For the locally artinian subgroup $X_0 = \ker \varphi$ of the formal group $\hat{X}$ may also be regarded as a subgroup of X, and setting $Y = X/X_0$ it is sufficient to consider the natural epimorphism $f: X \to Y$.

§ 5. Comments

The fundamental working tool in the series of papers by Dieudonné is the algebra of a formal group (called a hyperalgebra there). Dieudonné introduced it in [33] as the algebra of invariant differential operators in analogy with the classical case. Cartier [18]–[20] characterized hyperalgebras axiomatically and was the first to turn his attention to the fundamental role of the linear duality. A full 'symmetrization' of the theory from this point of view was first achieved in the paper by Gabriel [37] (*cf.* also the report by Cartier [20] in Brussels), where not only the hyperalgebras of reduced formal groups were studied, as Dieudonné had done, but also artinian bialgebras and their inductive and projective limits, which lead to a considerable simplification of the theory.

In the paper [13] by Barsotti and also in his report [14] there is an interesting study of duality on the level of Dieudonné modules. In the application to abelian varieties this provides a 'symmetry condition' which is established by other methods in the fourth chapter of the present paper. Besides, Barsotti introduces new variants of the Witt formalism and new operations on generalized Witt vectors, and he states that in this way he can transfer the classical theory of differentials of the third kind to the case of a base field of finite characteristic.

In the papers of Gabriel and Barsotti only commutative groups are considered; while non-commutative groups are indispensable for various theories, results on their bialgebras are given only in the paper [29] by Dieudonné, and at an inadequate technical level. Apparently the complication of the study of non-commutative bialgebras is connected with the fact that in place of the diagonal mapping of the algebra into the tensor product with itself, the natural object of study in this case is the diagonal mapping of the algebra into its free product which is much less amenable. (Cf. the construction of the Hausdorff formula in finite characteristic in the paper [28] by Dieudonné.) All the same, the study of non-commutative bialgebras, which includes as particular cases finite groups (possibly with operators) and restricted Lie algebras, presents a definite interest. New facts can be obtained here even near the surface: thus, in the note [7] the author has shown that the translation of Cayley's theorem to the case of non-commutative bialgebras is obtained immediately from the theorem on the embedding of restricted Lie algebras in Jacobson algebras; the latter play here the role of the symmetric group.

Dieudonné modules were introduced by Dieudonné in the papers [27] and [30], where he also established the fundamental theorem on the connection between modules and groups. It should be noted that the Dieudonné module appears here as covariant and not as contravariant functor, because instead of an injective object he considers a projective object ('free commutative hyperalgebra'). In the paper [13] Barsotti gives a connected account of this part of the theory from a point of view very close to that of Dieudonné.

The results on the multilinear duality of the operators F and V are not clear in the Barsotti duality [13], while they make the classification of artinian abelian groups by Gabriel and the structure of the ring E_k considerably more transparent.

A question that arises naturally is the study of formal groups over rings, and not merely over fields. In this direction there are only some results by Lazard [51]–[53] concerning the case of commutative groups. His fundamental result, which is not covered in the subsequent investigation, consists in the proof of the existence of a 'universal group law'. Namely, there exists a ring A and a diagonal mapping

$$c\colon A[[x_1, \ldots, x_n]] \longrightarrow A[[x_1, \ldots, x_n]] \hat{\otimes}_A A[[x_1, \ldots, x_n]],$$

such that for any integral domain B with a 'group law'

$$c'\colon B[[x_1, \ldots, x_n]] \longrightarrow B[[x_1, \ldots, x_n]] \hat{\otimes}_B B[[x_1, \ldots, x_n]],$$

on the schema $\operatorname{Spf} B[[x_1, \ldots, x_n]]$ over $\operatorname{Spec} B$, the law c' is obtained as the image of c under a certain homomorphism $A \to B$. In other words, the functor on the category of reduced affine schemata $\operatorname{Spec} B$ that associates with every schema the set of formal group laws over this schema is representable (cf. Grothendieck [41]). Unfortunately, the discussion of group laws (i.e. groups with a 'fixed coordinate system') instead of the groups themselves makes this result almost inapplicable.

In the paper [52] Lazard shows that all one-dimensional reduced formal groups are commutative.

§ Chapter II

DIEUDONNÉ MODULES; CLASSIFICATION UP TO ISOGENY

The basic aim of this chapter is the classification of E-modules up to isogeny. For this purpose the ring E can be replaced by a certain principal ideal ring E_F (cf. § 1) over which the classification of modules can be carried out completely. In the first section we shall carry out the reduction to the ring E_F, and in the second the classification of modules (over a certain more general ring, which is necessary for technical reasons). The second basic result of this chapter – Theorem 2.2 in § 3 – is new. It will only be needed in the fourth chapter and may be omitted on a first reading. In the fourth section we summarize the results of the classification in the language of formal groups.

§1. Reduction of the problem

1. Let E be the ring defined in the preceding chapter; we shall take the field k to be fixed, unless the contrary is expressly stated, and we may therefore omit the index k. A finitely generated E-module M with the further condition that M/FM is of finite length, is called a Dieudonné module. The basic aim of this chapter is the classification of Dieudonné modules up to isogeny. The method of classification is due to Dieudonné and rests on the fact that the isogeny of modules is equivalent to the isomorphism of the extended modules relative to a certain other ring. This new ring turns out to be a principal ideal ring.

More precisely, consider the ring $E_F = W(k)\sigma((F))$ consisting of all formal series of the form

$$\sum_{i>-\infty} a_i F^i, \quad a_i \in W(k),$$

with multiplication rule $Fa = a^\sigma F$. The ring E_F is a right E-module; for any E-module M the tensor product $M_F = E_F \underset{E}{\otimes} M$ may be considered as a left E_F-module.

PROPOSITION 2.1. (1) *The Dieudonné E-modules M', M'' are isogenous if and only if the E_F-modules M'_F, M''_F are isomorphic.* (2) *For any Dieudonné E-module M the E_F-module M_F is periodic.*

PROOF. (1) Let $M' \sim M''$; we shall show that $M'_F \approx M''_F$. It is sufficient to consider two cases: (a) M' is a submodule of finite colength in M''; (b) $M' = M''/M_0$, where M_0 is a submodule of finite length. In case (a) it is clear that $M'_F \subset M''_F$. The opposite inclusion follows from the fact that for a certain $k \geqslant 1$ we have $F^k M'' \subset M'$ (because long $M''/M' < \infty$) and so $M'' \subset M'_F$. In case (b) the epimorphism $h: M'' \to M'$ induces an epimorphism $h_F: M''_F \to M'_F$. Let $x \in \ker h_F$, $x = F^{-k}y$, $y \in M''$, $k \geqslant 0$; then $h_F(x) = F^{-k}h(y) = 0$, hence $F^l h(y) = 0$ and so $F^l y \in M_0$. Since M_0 has finite length, y is annihilated by a certain power of F and so $x = F^{-k}y = 0$, which shows that h_F is an isomorphism.

(Clearly the proof consists in repeating the argument used to show that localization is an exact functor.)

Conversely, let $M'_F \approx M''_F$, where the modules M' and M'' may be taken to be reduced, because every noetherian E-module is isogenous to its maximal reduced factor-module. Then the natural mappings $M' \to M'_F$ and $M'' \to M''_F$ are inclusions. We shall identify M'_F and M''_F by means of the given isomorphism and regard M' and M'' as submodules of M'_F. Since M' and M'' are finitely generated, it follows that there exist integers k, l such that $F^k M' \subset M''$ and $F^l M'' \subset M'$. (For let $(x_1, \ldots, x_N)$ be any finite generating set of M''; any element of this set may be written in the form $x_i = F^{-l_i} y_i$, where $y_i \in M'$; put $l = \max l_i$. The existence of k follows similarly.) From the inclusions $F^k M' \subset M''$, $F^l M'' \subset M'$ there follows the isogeny of the modules M' and M'' because long $M'/F^k M \leqslant \infty$ and long $M''/F^k M' \leqslant$ long $M''/F^{k+l}M' < \infty$.

(2) Let us show that the E_F-module M_F is periodic. Clearly it is enough to show that for any element x belonging to the image of M in M_F there exists an element $g \in E_F$ such that $gx = 0$. We shall denote this image by the same letter M. Since $FV = p$, it follows that $(pF^{-1})M \subset M$. Now assume that the annihilator of the element x vanishes. We denote by E_F^+ the ring of all series with non-negative exponents for F. The set M' of all elements $a \in E_F$ for which $ax \in M$ is an E_F^+-submodule of E_F isomorphic to the E_F^+-module M (the isomorphism being given by the mapping $a \to ax$). But M is a finitely generated E_F^+-module; it is generated by the inverse images of the non-zero elements generating M/FM over E. It follows that M' is finitely generated. Since $(pF^{-1})^i \in M'$, we have for some $n \geqslant 1$,

$$(pF^{-1})^n = \sum_{i=0}^{n-1} a_i (pF^{-1})^i, \quad a_i \in E_F^+,$$

and so $p^n \in FE_F^+$, which is impossible.

Hence M_F is a periodic module and the proposition is established.

§ 2. Modules over the ring A

1. In this section we denote by A a ring of a more general form than E_F in § 1. The precise definition follows.

Let k be a perfect field of characteristic $p > 0$, $W(k)$ the ring of infinite Witt vectors over k, $e \geqslant 1$ an integer, $U = W(k)[\pi]$, where $\pi^e = p$, $\sigma: U \to U$ an automorphism of U such that $\pi^\sigma = \pi$, and $A = U_\sigma((T))$ the ring of Hilbert power series with coefficients from U; this consists of all elements of the form $\sum_{i>-\infty} a_i T^i$, $a_i \in U$, with the multiplication of terms carried out by the commutativity rule $Ta = a^\sigma T$, where $a \in U$.

The aim of this section is to study finitely generated A-modules; it turns out that A is a principal ideal ring, and in the case of an algebraically closed field k this enables us to obtain a complete classification of A-modules. These results, concerning the case of a finite field k, will be needed later on for computations on the formal structure of abelian varieties.

2. PROPOSITION 2.2. *All right and left ideals of the ring A are principal.*

PROOF. We confine our attention to left ideals; the case of right ideals is precisely analogous. For any element $f = \sum_{i=m}^{\infty} a_i T^i$, $a_i \in U$, $a_m \neq 0$, we put $s(f) = \nu(a_m)$, where ν is the π-adic exponent in the ring U. We shall prove that A is euclidean relative to the function s. This means that for any pair of elements $f, g \in A$ there exist q, $r \in A$ such that

$$f = gq + r, \quad s(r) < s(g) \quad \text{or} \quad r = 0.$$

For the proof we can restrict ourselves to the case $s(f) \geqslant s(g)$ and assume that $f \notin gA$. Set $d(f) = m$ (suffix of the first non-zero coefficient); then there exists q_1 such that $d(f - gq_1) \geqslant m + 1$. For we may put $f = f' + f''$, where

$$f' = \pi^{s(f)} T^{d(f)} e,$$

and the element e is invertible and $d(e) = 0$; similarly we put $g = g' + g''$, where $g' = \pi^{s(g)} T^{d(g)} h$, h is invertible and $d(h) = 0$; moreover $d(f'') \geqslant d(f) + 1$ and $d(g'') \geqslant d(g) + 1$. Then $f' = g' q_1$ for some q_1, and it is not hard to see that $d(f - gq_1) \geqslant m + 1$. Now if $s(f - gq_1) \geqslant s(g)$, the process may be repeated; it cannot continue indefinitely, because $d(q_{i+1}) \geqslant d(q_i) + 1$; therefore the series $\sum_i q_i$ converges in A and by an unlimited repetition of the process we would obtain $g \sum_i q_i = f$, which was excluded.

COROLLARY 1. *The ring A is noetherian* (Jacobson [2], Ch. 3, 2).

COROLLARY 2. *Every finitely generated periodic left A-module is isomorphic to a direct sum of cyclic A-modules of the form A/Aq, where either $q = \pi^i$, $i \geqslant 1$, or*

$$q = \sum_{i=0}^{h-1} a_i T^i + cT^h, \quad c \in A, \quad d(c) = 0, \quad s(c) = 0, \quad a_i \in \pi U \tag{2.1}$$

PROOF. In fact every periodic module over a principal ideal ring is a

direct sum of cyclic modules. It therefore suffices to show that the generators can be chosen to have the form indicated.

Let $M = A/Aq$; if $d(q) \neq 0$, $q = T^{d(q)}q'$, then A/Aq' is isomorphic to M, so we may assume that $d(q) = 0$. Put $q = \pi^m q_1$, where $q_1 \in A$ and $m \geqslant 0$ is the greatest integer for which such a decomposition is possible. The element q_1 can then be expressed in the form subject to the given condition: in the decomposition $q_1 = \sum_{i=0}^{\infty} a_i T^i$ we put $h = \min\{i \mid v(a_i) = 0\}$, $c = \sum_{i=h}^{\infty} a_i T^{i-h}$.

Therefore it is enough to show that

$$A/A\pi^m q_1 \approx A/A\pi^m \oplus A/Aq_1.$$

(Direct sums in the category of modules will be denoted by the symbol $\oplus$.) This follows from Fitting's Lemma (cf. Jacobson [2], Ch.1, 5), applied to the endomorphism of multiplication by π (we recall that π belongs to the centre of A). Thus, Corollary 2 is established.

3. The module $A/\pi^m A = M$ is indecomposable, and any submodule of M is of the form $\pi^i M$, $0 \leqslant i \leqslant m$. This follows from the fact that every divisor of π^m is of the form π^i, to within unit factors.

The modules A/Aq, where q is of the form (2.1), yield to further analysis. We shall make use of the fact that if $u \in A$ is any invertible element, then A/Auq is isomorphic to A/Aq. We shall show now that by such a transformation q may be reduced to the form (2.1), where $c = 1$; this is analogous to the well known 'Weierstrass preparation theorem'.

LEMMA 2.1. *There exists an invertible element $u \in A$ such that*

$$uq = \sum_{i=0}^{h-1} b_i T^i + T^h, \qquad b_i \in \pi U.$$

PROOF. If we put $u_1 = c^{-1}$, then $u_1 q \equiv T^h \bmod \pi A$. Suppose that we have already found an element $u_n \in A$ such that

$$u_n q \equiv \sum_{i=0}^{h-1} b_i^{(n)} T^i + T^h \bmod \pi^n A,$$

where $b_i^{(n)} \in \pi U$. We try to determine $u_{n+1} = u_n + \pi^n v$ from the conditions

$$(u_n + \pi^n v)\, q \equiv \sum_{i=0}^{h-1} b_i^{(n+1)} T^i + T^h \bmod \pi^{n+1} A, \quad b_i^{(n+1)} \equiv b_i^{(n)} \bmod \pi^n.$$

For this purpose it is sufficient to find $v \bmod \pi$ from the equation

$$\pi^{-n}\Big(u_n q - \sum_{i=0}^{h-1} b_i^{(n)} T^i - T^h\Big) + vcT^h \equiv t_{h-1}(T) \bmod \pi,$$

where $t_{h-1}(T)$ is a polynomial of degree $h-1$ in T, but otherwise arbitrary. This congruence can always be solved, because c is invertible. Thus the lemma is established.

A polynomial of the form $\sum_{i=0}^{h-1} a_i T^i + T^h$, where $a_i \equiv 0 \bmod \pi$, is said to be *distinguished*. A further reduction of a cyclic A-module whose annihilator is generated by a distinguished polynomial can be obtained if we

assume that the field k is algebraically closed and the automorphism σ is induced by a certain non-zero power of the Frobenius endomorphism

$$(a_1, a_2, \ldots)^\sigma = (a_1^{p^k}, a_2^{p^k}, \ldots), \qquad k \neq 0.$$

The first result states that a non-commutative distinguished polynomial can then be decomposed into linear factors over a certain purely ramified extension ring. For the proof we shall make use of the Newton polygon.

4. LEMMA 2.2. *Let the field k be algebraically closed and let $q = \sum_{i=0}^{h-1} a_i T^i + T^h$ be a distinguished polynomial. Then there exists an integer $m > 0$ such that over the ring $U' = U[\pi^{1/m}]$, $(\pi^{1/m})^\sigma = \pi^{1/m}$ (in the ring $A[\pi^{1/m}]$, by definition, $T\pi^{1/m} = \pi^{1/m}T$), we have an equation of the form*

$$q = \prod_i (T - \pi^{ni/m} u_i),$$

where the elements $u_i \in U[\pi^{1/m}]$ are invertible.

PROOF. It is sufficient to show that over the given purely ramified extension of U any distinguished polynomial has a linear factor: the assertion then follows by induction on the degree of the polynomial.

A splitting criterion can be given in the following form: the equation

$$q(T) = \sum_{i=0}^{h} a_i T^i = q_1(T)(T - a) \tag{2.2}$$

is equivalent to the relation

$$\sum_{i=0}^{h} a_i a^{1+\sigma+\ldots+\sigma^{i-1}} = 0 \qquad (a^{1+\ldots+\sigma^{i-1}} = 1 \text{ for } i = 0).$$

The proof follows by equating coefficients in (2.2) and eliminating the coefficients of $q_1(T)$ from the resulting system of equations.

Using this criterion we shall show that if the integer s defined by the condition

$$\frac{r}{s} = \min \frac{\nu(a_i)}{h - i}, \qquad (r, s) = 1,$$

is 1, then a linear factor can be found already in A itself. For this purpose it is enough to prove the solubility of the equation

$$\sum_{i=0}^{h} a_i \pi^{ri} x^{1+\sigma+\ldots+\sigma^{i-1}} = 0 \tag{2.3}$$

for an invertible element $x \in U$. We have $\nu(a_i) \geqslant r(h - i)$; if we put $a_i = \pi^{r(h-i)} b_i$, then (2.3) is equivalent to the relation

$$\sum_{i=0}^{h} b_i x^{1+\sigma+\sigma^2+\ldots+\sigma^{i-1}} = 0, \qquad b_i \in U, \tag{2.4}$$

in which at least two coefficients b_i do not lie in πU. The equation (2.4) has a non-zero solution mod π. Assume that we have already found an invertible solution of this equation mod π^n:

$$\sum_{i=0}^{h} b_i x_n x_n^\sigma \ldots x_n^{\sigma^{i-1}} = \pi^n c, \qquad x_n \notin \pi U, \qquad c \in U.$$

Put $x_{n+1} = x_n = \pi^n y$; clearly

$$\prod_{k=0}^{i-1} x_{n+1}^{\sigma^k} \equiv \prod_{k=0}^{i-1} x_n^{\sigma^k} + \pi^n \sum_{k=0}^{i-1} x_n \dots x_n^{\sigma^{k-1}} y^{\sigma^k} x_n^{\sigma^{k+1}} \dots x_n^{\sigma^{i-1}} \mod \pi^{n+1}$$

(we recall that $x_n \not\equiv 0 \bmod \pi$). Therefore the condition

$$\sum_{i=0}^{h} b_i x_{n+1} x_{n+1}^{\sigma} \dots x_{n+1}^{\sigma^{i-1}} \equiv 0 \mod \pi^{n+1}$$

gives

$$c + \sum_{i=0}^{h} b_i \sum_{k=0}^{i-1} x_n \dots x_n^{\sigma^{k-1}} y^{\sigma^k} x_n^{\sigma^{k+1}} \dots x_n^{\sigma^{i-1}} \equiv 0 \mod \pi.$$

This is a non-linear equation in y and the coefficient of the power $y^{\sigma^{h-1}}$ is not zero. Its solubility therefore follows from the fact that k is algebraically closed. Consequently $q(T)$ is divisible on the right by a factor of the form $T - \pi^r u$, where $u \in U$ is invertible.

If however $\frac{r}{s} = \min \frac{\nu(a_i)}{h - i}$ is not an integer, we reach our object by going over to the ring $U[\pi^{1/s}]$ (ν is understood to be the normalized exponent taking all integer values). The lemma follows.

REMARK. For the applications it is convenient to have the following somewhat more precise variant of the condition for the splitting into linear factors. Namely, in the notation of the proof of Lemma 2.2, let $s = 1$ and let j be the least value for which $\frac{\nu(a_i)}{h - j} = r$. Then we may at once split $h - j$ linear factors from $q(T)$ with the same exponent for the root:

$$q = q'(T - \pi^r x_1) \dots (T - \pi^r x_{h-j}),$$

where $x_i \in U$ is invertible.

For the proof it is enough to verify that if

$$q = \sum_{i=0}^{h} a_i T^i = \Big(\sum_{i=0}^{h-1} b_i T^i\Big)(T - \pi^r x),$$

then $\min \frac{\nu(b_i)}{h - 1 - i} = r$ and $\frac{\nu(b_i)}{h - 1 - i} < r$ for $i < j$, and the required result is now obtained by induction on h. Indeed,

$$a_i = b_{i-1} - b_i \pi^r x^{\sigma^i} \quad (i \geqslant 1), \qquad a_0 = -\pi^r b_0 x,$$

so that $\nu(b_0) = \nu(a_0) - r \geqslant r(q - 1)$. Using the fact that $\nu(a_i) \geqslant r(q - i)$ and that strict inequality holds for $i < j$, we may proceed by induction on i. Suppose that we have shown that $\nu(b_{i-1}) \geqslant r(q - i)$ (with strict inequality for $i < j$); then $\nu(b_i) \geqslant r(q - i - 1)$ (with strict inequality for $i < j$). But then we obtain an equality for $i = j$, because this holds for the coefficients a_i. Thus, everything is proved.

5. LEMMA 2.3. *Let* $M = A/Ap(T)$, *where*

$$p(T) = \sum_{i=0}^{h-1} a_i T^i + T^h, \qquad a_i \in \pi U.$$

Denote by K the quotient field of U. Then there exists on M a vector space structure over K which is compatible with the U-module structure. This structure is unique and the dimension of M over K is h. (Here we do not assume that the field k is algebraically closed.)

PROOF. For the existence proof it is sufficient to define multiplication by $\pi^{-1}: M \to M$ and to show that this is compatible with the action of U.

Let us put

$$-p(T) = T^h(\pi q(T) - 1), \qquad q(T) \in A.$$

It is clear that $q(T)$ is uniquely defined by this condition. Then $\pi q(T) \equiv 1 \bmod Ap(T)$. We put $\pi^{-1}x = q(T)x$ for the generating element $x = 1 \bmod Ap(T)$. It is not hard to convince oneself that this gives the required result. The uniqueness of the linear space structure is clear. The dimension of this space is h, because we may take as basis the images of the elements $1, T, \ldots, T^{h-1}$.

6. LEMMA 2.4. *Let $M = A/Abc \supset N = Ac/Abc$. Then the submodule N is a direct summand, $M = N \oplus P$, if and only if the equation $xb + cy = 1$ is soluble (in the ring A). In this case $P \approx A(1 - yc)/Abc \approx A/Ac$.*

PROOF. We verify first that $N \approx A/Ab$. Let $\xi = 1 \bmod Abc \in M$. Then the ideal Abc is the annihilator of ξ, $M = A\xi$, $N = Ac\xi$. The annihilator of $c\xi$ is the ideal Ab, so that $N \approx A/Ab$.

Let $M = N \oplus P$, $\xi = \xi_N + \xi_P$ the corresponding decomposition, and $\xi_P = d\xi$, where $d \in A$. Then the element ξ_P generates P and $a\xi_P = 0$, i.e. $a\xi \in N$, so that $a \in Ac$, and it follows that $P \approx A/Ac$.

Put $\xi_N = yc\xi$, then $1 - yc - d \in Abc$, because $\xi = yc\xi + d\xi$, and the element d is defined up to an element from Abc, so that we may assume that $d = 1 - yc$. From the equation $c(1 - yc)\xi = 0$ it follows that $c(1 - yc) = xbc$, so that $1 - cy = xb$. The reasoning may also be reversed: from the equation $xb + cy = 1$ it follows that $N + Ad\xi = M$, where $d = 1 - yc$; if $zc\xi = vd\xi \in N \cap Ad\xi$ and $zc - vd = wbc$, $zc - v + vyc = wbc$, $v \in Ac$, then $cd \in Acd = A(c - cyc) = Axbc$, i.e. $vd\xi = 0$, so that $N \cap Ad\xi = 0$. Thus the lemma is proved.

7. The next step consists in the study of modules of the form $A/A(T - a)$.

LEMMA 2.5. *The module $A/A(T - a)$ is simple and isomorphic to the module $A/A(T - \pi^r)$, where $r = \nu(a)$. Moreover, any extension of two such modules is trivial.*

PROOF. Consider the module $A/A(T - a)$; it is zero if $\nu(a) = 0$, so let $\nu(a) \neq 0$. We denote the quotient field of U by K and on K define a left A-module structure by putting $Tx = x^{\sigma}a$ (cf. Lemma 2.3). The mapping $A/A(T - a) \to K$ in which $1 \bmod A(T - a)$ corresponds to the unit element of K is an A-module isomorphism. Now K and $A/A(T - b)$ are isomorphic as A-modules if and only if there exists an element $y \in K$ such that $Ty = by$, i.e. $y^{\sigma}a = by$. If this equation has a solution, then $\nu(a) = \nu(b)$; the converse also holds, namely that the given extension has a solution mod π, as in the preceding lemma.

Now let $0 \to M_1 \to M \xrightarrow{f} M_2 \to 0$ be an exact sequence of A-modules, and let $M_1 = A/A(T - a)$, $M_2 = A/A(T - b)$. Let $x \in M_1$ be the image of the unit element of A and $y \in M$ an element such that $f(y)$ represents the image of the unit element of A in M_2. It is clear that x, y form a K-basis for the

space M. To establish the result it is enough to find an element x' such that the pair x, x' is a K-basis for M and $Tx' = bx'$. We shall write x' in the form $x' = y + \xi x$, where $\xi \in K$; then

$$Tx' = Ty + \xi^{\sigma} ax = by + cx + \xi^{\sigma} ax = by + b\xi x.$$

Hence ξ must satisfy the equation $b\xi - \xi^{\sigma} a = c$, where a, b, c are given elements of the field K. This equation can always be solved by the method of successive approximations.

The lemma is now proved.

COROLLARY. *Let* $p(T) = \prod_i (T - \pi^{r} u_i)$; *then*

$$A/Ap(T) \approx \bigoplus_i A/A(T - \pi^{r}).$$

LEMMA 2.6. *Every cyclic module* A/Aa, $a \notin \pi A$, *is semisimple.*

PROOF. In any case the module A/Aa becomes semisimple if we replace the ring A by $A[\pi^{1/s}]$, since the equation $xb + cy = 1$ (cf. Lemma 2.4), where $b, c \in A$, is soluble in $A[\pi^{1/s}]$. We set

$$x = \sum_{i=0}^{s-1} \pi^{i/s} x_i; \quad y = \sum_{i=0}^{s-1} \pi^{i/s} y_i,$$

then $x_0 b + c y_0 = 1$ and $x_0, y_0 \in A$; by Lemma 2.4 this establishes the result.

8. The final result is a consequence of the preceding ones.

LEMMA 2.7. *Let* $M = A/Ap(T)$, *where* $p(T)$ *is a distinguished polynomial. Then* $M \approx \bigoplus_i A/A(T^{s_i} - \pi^{r_i})$, *where* $(s_i, r_i) = 1$ *and* s_i, r_i *are integers. The modules* $A/A(T^{s} - \pi^{r})$ *are simple and for different pairs* (s, r) *are pairwise non-isomorphic.*

PROOF. Put $A_s = A[\pi^{1/s}]$. For a given s the A_s-module $M_s = A_s \underset{A}{\otimes} M$ is isomorphic to the direct sum $\bigoplus_r A_s/A_s(T - \pi^{r/s})$. Let $x \in M_s$ be an element such that $(T - \pi^{r/s})x = 0$, $x = \sum_{i=0}^{s-1} \pi^{i/s} x_i$, $x_i \in M$. Then $(T^s - \pi^r)x = 0$ and hence $(T^s - \pi^r)x_i = 0$, because the submodule $Ax_i \subset M$ is a factor module of $A/A(T^s - \pi^r)$. We shall show that the latter module is simple if $(s, r) = 1$. For otherwise we have a simple submodule $M' \subset A/A(T^s - \pi^r)$, where $M' \approx A/Aq(T)$, with a distinguished polynomial $q(T)$. The degree of $q(T)$ must be less than s, because the dimension of M' as K-space is less than that of $A/A(T^s - \pi^r)$, which is equal to s (cf. Lemma 2.3). Therefore over some ring A_t the decomposition of M will contain a factor of the form $A_t/A_t(T - \pi^{r'/s'})$, $s' \leqslant s$, which is impossible, because $A_s/A_s(T - \pi^{r/s})$ remains simple over any extension of A of the form $A[\pi^{1/m}]$.

It has already been shown that an extension of simple modules is trivial. Thus the lemma is established.

We can now formulate the classification theorem for periodic A-modules.

THEOREM 2.1. *Let* k *be an algebraically closed field of characteristic* $p > 0$, $\pi^{e} = p$, $\sigma: W(k)[\pi] \to W(k)[\pi]$ *an automorphism that leaves* π *fixed and on* k *induces a certain non-zero power of the Frobenius endomorphism; and let* $A = W(k)[\pi]_{\sigma((T))}$. *Then any periodic* A*-module is isomorphic to a direct sum of modules of the form* $\bigoplus_i A/A\pi^{k_i} \bigoplus_j A/A(T^{r_j} - \pi^{s_j})$. *The module*

$A/A\pi^k$ is indecomposable; the modules $A/A(T^r - \pi^s)$ are simple and pairwise non-isomorphic for $(r, s) = 1$; if $(r, s) = d$, $r = r_0 d$, $s = s_0 d$, then

$$A/A\,(T^r - \pi^s) \approx dA/A\,(T^{r_0} - \pi^{s_0}).$$

(Here and in the sequel we shall use the symbol dM to indicate the direct sum of d modules isomorphic to M.)

§ 3. A technical result

1. With the same assumptions as before, let M be an A-module without π-torsion of the form $A \otimes M_0$, where M_0 is a (periodic) $W(k_a)[\pi]_\sigma((T))$-module, $k_a \subset k$ being the field of p^a elements. Let K_a be the quotient field of the ring $W(k_a)[\pi]$. Since T^a lies in the centre of the ring $W(k_a)[\pi]_\sigma((T))$, it follows that multiplication by T^a induces a certain endomorphism Λ on the linear space M_0 over K_a. Let $P(\lambda) = \sum_{i=0}^{n-1} a_i\lambda^i + \lambda^n$ be the characteristic polynomial of Λ, where $a_i \equiv 0 \bmod \pi$. We shall assume that $P(\lambda)$, as commutative polynomial, splits into linear factors over a ring of the form $W(k_b)[\pi^{1/k}]$, where $b = 0 \bmod a$, $k \geqslant 1$: $P(\lambda) = \prod_{i=1}^{n} (\lambda - \tau_i)$, $\tau_i \in W(k_b)[\pi^{1/k}]$. Under these conditions we have

THEOREM 2.2. *Let r_c be the number of roots τ_i of $P(\lambda)$ such that $\nu(\tau_i) = ac$ (ν is the exponent for which $\nu(\pi) = 1$). Set $s_c = cr_c$. Then*

$$M \approx \bigoplus_c A/A\,(T^{r_c} - \pi^{s_c}).$$

2. We preface the proof by the following lemma.

LEMMA 2.8. *For $k, a \geqslant 1$, put $A_{k,a} = W(k)[\pi^{1/k}]_{\sigma^a}((T^a))$, $T^a x = x^{\sigma^a} T^a$, $A = A_{1,1}$. If two A-modules without π-torsion M_1, M_2 are such that the $A_{k,a}$-modules $M_1[\pi^{1/k}]$ and $M_2[\pi^{1/k}]$ are isomorphic, then $M_1 \approx M_2$, quâ A-modules (where we have put $M[\pi^{1/k}]$ in place of $A[\pi^{1/k}] \underset{A}{\otimes} M$).*

PROOF. Clearly it is sufficient to examine the cases $k = 1$ and $a = 1$.

1) $k = 1$. Let $M = A/A(T^r - \pi^s)$, $(r, s) = 1$. By the classification theorem the $A_{1,a}$-module M is isomorphic to $\bigoplus_i A_{1,a}/A_{1,a}(T^{ar_i} - \pi^{si})$. We shall now compute the (r_i, s_i). Let $(a, r) = d$, $a = a_0 d$, $r = r_0 d$. The elements $x_i = T^i$ mod $A(T^r - \pi^s)$ of M at any rate generate it as $A_{1,a}$-module. On the other hand, $T^r x_i = \pi^s x_i$, whence $T^{a_0 r} x_i = \pi^{a_0 s} x_i$. Therefore $(T^{ar_0} - \pi^{a_0 s})x_i = 0$, and so the $A_{1,a}$-module M is periodic and homogeneous (= isotypic) of type $A_{1,a}/A_{1,a}(T^{ar_0} - \pi^{a_0 s})$, $(r_0, a_0 s) = 1$. The dimension of this simple module, as space over the quotient field of $W(k)[\pi]$, is r_0, therefore the number of components is $rr_0^{-1} = d$. Thus,

$$M \approx A_{1,a}/A_{1,a}(T^{ar} - \pi^{as}) \approx dA_{1,a}/A_{1,a}(T^{ar_0} - \pi^{a_0 s}) \tag{2.5}$$

(isomorphism of $A_{1,a}$-modules). Now the assertion of the lemma in the case when M is simple is an immediate consequence. The general case is obtained if we observe that the equation $M = M_1 \oplus M_2$ for A-modules remains true when we regard it as an equation for $A_{1,a}$-modules, and that homogeneous

modules of a given type remain homogeneous of a given type under passage to the ring $A_{1,a}$, as follows from the relation (2.5).

2) $a = 1$. The argument is very similar, but even simpler. Put $\pi_1 = \pi^{1/k}$, $(r,k) = d$, $r = r_0 d$, $k = k_0 d$; then the $A_{k,1}$-module $M[\pi_1]$, where $M = A/A(T^r - \pi^s)$, is isomorphic to $A_{k,1}/A_{k,1}(T^r - \pi_1^{ks})$. Clearly the $A_{k,1}$-module $M[\pi_1]$ is generated by the element $x = 1 \bmod A(T^r - \pi^s)$, for which $(T^{r_0} - \pi_1^{k_0 s})x = 0$, therefore $M[\pi_1] \approx dA_{k,1}/A_{k,1}(T^{r_0} - \pi_1^{k_0 s})$. The rest of the argument is as for the case $k = 1$.

3. Proof of Theorem 2.2. By the preceding lemma it is enough to establish the isomorphism for $A_{k,b}$-modules:

$$M[\pi^{1/k}] = \bigoplus_c A_{k,b}/A_{k,b}(T^{br_c} - \pi^{bs_c}).$$

Note that we may assume that $b = a$, because a can be replaced by any multiple of itself without changing the statement of the theorem.

Over the ring $W(k_a)[\pi]((T^a)) = B$ the module M_0 is isomorphic to $\bigoplus_i B/BP_i(T^a)$, where $\prod_i P_i(\lambda) = P(\lambda)$ is the given decomposition of the commutative polynomial $P(\lambda)$ into its factors. Hence the $A_{1,a}$-module M is isomorphic to $\bigoplus_i A_{1,a}/A_{1,a}P_i(T^a)$. We adjoin $\pi^{1/k}$ and decompose $P_i(T^a)$ into (commuting) linear factors: $P_i(T^a) = \prod_l (T^a - \tau_{li})$, where τ_{li} are the roots of $P_i(\lambda)$. Now the essential point is that any non-commutative factorization under our assumptions coincides with the commutative factorization, because T^a lies in the centre of the ring $W(k_a)[\pi^{1/k}]_\sigma((T))$. Hence it follows that the $A_{k,a}$-module $M[\pi^{1/k}]$ is isomorphic to a direct sum

$$\bigoplus_i A_{k,a}/A_{k,a}(T^a - \tau_i) \approx \bigoplus_c r_c A_{k,a}/A_{k,a}(T^a - \pi^{a^\wedge})$$

by Lemma 2.5, i.e.

$$\bigoplus_c A_{k,a}/A_{k,a}(T^{ar_c} - \pi^{acr_c}).$$

It only remains to verify that after the adjunction of $\pi^{1/k}$ the module $A/A(T^{rc} - \pi^{sc})$, quâ $A_{k,a}$-module, remains isomorphic to $A_{k,a}/A_{k,a}(T^{ar_c} - \pi^{as_c})$, but this can be established as in the proof of Lemma 2.8.

§4. Classification of formal groups up to isogeny

1. We shall now summarize the results of § 2 and apply them to the ring E_F. In this case $\pi = p$, $T = F$ and any periodic E_F-module is isomorphic to a direct sum of the form

$$M' = \bigoplus_i E_F/E_F(F^{r_i} - p^{s_i}) \bigoplus_t E_F/E_F p^t, \qquad (r_i, s_i) = 1.$$

We shall show that M' is isomorphic to M_F, where M is a given Dieudonné E-module, if and only if $r_i > s_i$ for all i. The sufficiency of the condition follows from the fact, which is easily verified, that for $r > s$

$$E_F/E_F(F^r - p^s) \approx E_F \bigoplus_E (E/E(F^{r-s} - V^s))$$

and

$$E_F/E_F p^l \approx E_F \bigoplus_E (E/EV^l).$$

This condition is also necessary. In fact, assume that $M' = M_F$, $M \subset M'$. Let $r_1 \leqslant s_1$, say, and let $F^{-h}x (x \in M)$ be the image of 1 mod $E_F(F^{r_1} - p^{s_1})$ in the first direct summand of the decomposition M'. Let $\alpha = 1 - F^{s_1 - r_1} V^{s_1} \in E$; then it is easy to see that $\alpha x = 0$, which is impossible, because $x \neq 0$ and α is invertible. This contradiction shows that $r_i \leqslant s_i$ cannot hold.

2. Denote by $G_{n,m}$ the formal group whose Dieudonné module is isomorphic to $E/E(F^m - V^n) = M_{n,m}$. Clearly this group is reduced. For $(n,m) = 1$ it is simple in the sense that any epimorphism is either an isogeny or the trivial mapping $G_{n,m} \to \operatorname{Spec} k$. This group is defined over the prime field. Its dimension is given by a simple calculation:

$$\dim G_{n,m} = \log \ker F_{G_{n,m}} = \log M_{n,m}/FM_{n,m} = n.$$

Further, it is convenient to denote the multiplicative group by the symbol $G_{1,0}$ and the group of the Dieudonné module E/EV^n by $G_{n,\infty}$. It is not hard to verify that $G_{n,\infty}$ represents the completion of the algebraic group W_n of Witt vectors of length n under addition. We shall confine ourselves to verifying this up to isogeny. In fact, W_n is annihilated by the homomorphism of multiplication by p^n, but not by p^{n-1}. The same holds for $\hat{W}_n$, and hence $\hat{W}_n \sim \bigoplus_i G_{n_i,\infty}$, where the equality $n = n_i$ holds for at least one i. But the dimension of $\hat{W}_n$ is n, therefore $\hat{W}_n \sim G_{n,\infty}$. Thus, we have obtained the following result.

CLASSIFICATION THEOREM FOR FORMAL GROUPS UP TO ISOGENY. (a) *Any formal commutative group is isogenous to a direct sum of its maximal toroidal subgroups, unipotent groups and groups in which multiplication by p is an isogeny. This decomposition is unique up to isogeny.*

(b) *Any toroidal group is isogenous to a group of the form*

$$fG_{1,0},\ f \geqslant 1.$$

(c) *Any unipotent group is isogenous to a direct sum of indecomposable unipotent groups* $G_{n,\infty}$, $n \geqslant 1$.

(d) *Any group in which the morphism of multiplication by p is an isogeny, is isogenous to a direct sum of simple groups* $G_{n,m}$, $n \geqslant 1$, $m \geqslant 1$, $(n,m) = 1$.

REMARK. The introduction of the unifying notation $G_{n,m}$ is convenient, because for arbitrary values of n and m subject to the conditions

$$1 \leqslant n < \infty, \quad 0 \leqslant m \leqslant \infty, \quad (n,m) = 1$$

(we take $(n,\infty) = 1$ for all n) the group $G_{n,m}$ is determined up to isogeny by the following conditions:

(a) the dimension of $G_{n,m}$ is n;

(b) $G_{n,m}$ is indecomposable up to isogeny;

(c) the degree of the endomorphism of multiplication of G by p is p^{n+m} (where $p^\infty = 0$).

§ 5. Comments

For non-commutative formal groups no analogue of the Dieudonné module is known, and the whole apparatus set up here does not carry over to the non-commutative case. Regarding this case see also the comments to Ch. IV.

The classification of periodic E_F-modules was given by Dieudonné [30]; it has been reprinted without essential changes in the papers by Barsotti [13] and Gabriel [37]. We have followed the version of Gabriel, in which it is technically more convenient to state and prove our Theorem 2.2. The basic aim of Theorem 2.2 consists in replacing the determination of non-commutative factorizations of polynomials by commutative factorizations. Its interest lies in the fact that it makes it possible to carry out an analogous replacement without having to presuppose that the roots of the commutative factorization are 'not too badly' ramified. See also Theorem 4.1 of Ch. IV.

Chapter III

DIEUDONNÉ MODULES; CLASSIFICATION UP TO ISOMORPHISM

The basic aim of this chapter is the construction of the 'module space' (in the terminology of Riemann) for equidimensional commutative formal groups. A fundamental role in the construction of this space is played by the concept of a special E-module to be introduced in § 2. A special module serves as point of support for the classification: every module M can be regarded as the extension of a module of finite length by a maximal special submodule $M_0 \subset M$. If we first confine ourselves to modules M with a fixed special submodule M_0 and such that the length long M/M_0 does not exceed a given constant, then it can be shown that these modules are classified by the orbits of a finite group that acts on a constructive algebraic set over the base field; this is established in § 3. In §§ 4, 5, 6 it is shown that in any isogeny class of modules there are only a finite number of special modules up to isomorphism (first finiteness theorem) and that long M/M_0 is bounded by a constant depending only on the class (second finiteness theorem). The representation of a simple module M_F as the tensor product of the ring $W(k)$ with the endomorphism ring of this module, which will be introduced in § 4, occupies an important place in the proofs. The end of § 6 contains an extension of the finiteness theorems to the widest possible class of modules; these turn out to be the reductive modules, isogenous to a direct sum of equidimensional modules and a module annihilated by V.

The representation of the module M_F to be introduced in § 4 also turns out to be very useful for the better determination of the module space in certain special cases. In § 7 such a determination is carried out for cyclic isosimple modules, and in § 8 for all two-dimensional modules, which can be completely classified.

It should be remarked that we are constantly using the algebraic and quasi-algebraic structure on rings of the form $W_h(k)$ (Witt vectors of length h over k) and modules over rings of this form. The necessary technical introduction to these structures is set out in the papers of

Greenberg [38] and Serre [57], [58].

Throughout this chapter the base field k is assumed to be algebraically closed.

§1. Statement of the problem

1. The basic result obtained in Ch. II states that every E-module of a Dieudonné group is isogenous to an E-module of the form

$$\bigoplus_i E/E(F^{m_i} - V^{n_i}) \bigoplus_j E/EV^{r_j},$$

where $(m_i, n_i) = 1$ and m_i, n_i, r_j are natural numbers. The module E/V^rE is the Dieudonné module for the completion of the additive group of Witt vectors of dimension r. This group is unipotent; therefore an E-module isogenous to a module of the form $\bigoplus_r E/V^rE$ will also be called unipotent, while an E-module isogenous to a module without components of the form E/V^rE is called a module without unipotent components, or an equidimensional module (cf. Ch. I, §4, 4).

2. The task of classifying E-modules up to isomorphism is solved in this chapter for modules without unipotent components. This limitation is due to the fact, already mentioned, that the basic result of the classification, according to which the reduced E-modules without unipotent components that are isogenous to a fixed E-module are parametrized by the orbits of a finite group acting on a constructive algebraic set over the base field, in general no longer holds for modules with unipotent components. From the global point of view our limitation may be expressed by saying that we discuss only completions of abelian varieties, leaving aside the unipotent (commutative) linear groups, which form a class about which little appears to be known. An analogous situation obtains in the classical theory, where semisimple Lie algebras lend themselves to a complete classification, which is very much more than can be said for algebras with a radical.

§ 2. Auxiliary results

(The word 'module' always refers to a Dieudonné E-module here, unless the contrary is expressly stated.)

1. For every module M the symbol M_F denotes the E_F-module $E_F \underset{E}{\otimes} M$ defined in Ch. II, § 1. Let us agree to define the action of the automorphism σ on E by putting $F^\sigma = F$, $V^\sigma = V$. The elements of M_F are the expressions $F^{-k}x$, $x \in M$, with which we operate according to the following natural rules:

$$aF^{-k}x = F^{-k}a^{\sigma^k}x,\ a \in E; \quad F^{-k}x + F^{-l}y = F^{-k}(x + F^{k-l}y),\ k \geqslant l; \quad F^{-k}x = F^{-l}y$$

if and only if $V^s(F^l x - F^k y) = 0$ for some $s \geqslant 0$.

An E-submodule M' of M_F is said to be *dense* if M'_F coincides with M_F; sometimes we shall also say that $M' \subset M$ is a dense submodule; this means that $M'_F = M_F$.

LEMMA 3.1. *A reduced E-module M' is isogenous to an E-module M if and only if it is isomorphic to a dense E-submodule of M_F.*

PROOF. The sufficiency of the condition follows immediately from Proposition 2.1. The necessity follows by considering the composition mapping $M' \xrightarrow{i} M'_F \xrightarrow{j} M_F$, where i is the canonical homomorphism, which is an embedding if M' is reduced, and j is an isomorphism whose existence follows from the isogeny of M' and M by Proposition 2.1. Thus the lemma is proved.

In order to classify the reduced modules isogenous to M it is therefore enough to consider the dense submodules of M_F.

REMARK. Lemma 3.1 can be strengthened as follows: under the conditions of the lemma there always exists an embedding $M' \to M_F$ such that the image of M' contains $M \subset M_F$ (or an embedding such that M' is contained in M). For we may confine ourselves to the case when $M \approx \bigoplus E/E(F^{m_i} - V^{n_i}) \bigoplus E/EV^{r_j}$. In this case the submodule $F^k M$ of M_F is isomorphic to M, for any integer k, and so the assertion follows.

2. In the sequel we shall simply write W instead of $W(k)$.

LEMMA 3.2. *Let $M = \bigoplus_i E/E(F^{m_i} - V^{n_i})$. Then an E-submodule M' of M_F is dense if and only if its rank, as W-module, is $\sum_i (m_i + n_i)$.*

PROOF. The W-module $E/E(F^m - V^n)$ is free and its rank is $m + n$, because the elements $x_0 = 1 \bmod E/E(F^m - V^n)$, $Fx_0, \ldots, F^{m-1}x_0$, $Vx_0, \ldots, V^n x_0$ form a W-basis. On the other hand, for any dense submodule M' of M_F and any given integers $k, l \geqslant 0$ we have the inclusions $p^k M' \subset M$ and $p^l M \subset M'$ (cf. the proof of Prop. 2.1), hence M and M' have the same W-rank. This proves the necessity.

Now let $M' \subset M_F$ have the rank $\sum_i (m_i + n_i)$, as W-module. Choose k such that $p^k M' \subset M$. The factor module $M/p^k M'$ has finite length as W-module, and a fortiori as E-module. Therefore $p^k M$ is a dense submodule and the lemma follows.

REMARK. The limitation to equidimensional modules is essential: in fact, the W-module E/EV^r, $r \geqslant 1$, has infinite rank.

COROLLARY. *Equidimensional modules that are isogenous have the same rank.*

In what follows all modules are assumed to be reduced, unless the contrary is expressly stated.

3. *DEFINITION.* An equidimensional module M isogenous to a module of the form $kE/E(F^m - V^n)$, $(m, n) = 1$ (such a module will for brevity be called *homogeneous of type* (m, n)) is said to be *special* if $F^m M = V^n M$.

An arbitrary equidimensional module M is said to be *special* if it is isomorphic to a direct sum of homogeneous special modules.

EXAMPLE. The module $\bigoplus_i E/E(F^{m_i} - V^{n_i})$ is special.

DEFINITION. Let M be a homogeneous module of type (m, n). An element $x \in M$ is said to be *special* if $F^m x = V^n x$.

An element x of an arbitrary equidimensional module M is said to be special if its components in the homogeneous components of M are special in the latter.

LEMMA 3.3. *A homogeneous module M of type (m, n) is special if and only*

if, as W-module, it has a basis consisting of special elements (called a special basis).

PROOF. Let $x_1, \ldots, x_N$ be a special W-basis and $y = \sum_{i=1}^{N}{}' a_i x_i$, $a_i \in W$ any element of M. Clearly

$$F^m y = \sum_i a_i^{\sigma^m} F^m x_i = \sum_i a_i^{\sigma^m} V^n x_i = V^n \sum_i a_i^{\sigma^{m+n}} x_i \in V^n M.$$

and similarly $V^n y \in F^m M$. Therefore M is special.

Conversely, let M be a homogeneous special module. Starting from an arbitrary free W-basis $x_1^{(1)}, \ldots, x_N^{(1)}$ we construct a special W-basis by the following simple method. The operator $V^{-n}F^m$ induces a σ^{m+n}-semilinear automorphism on the factor module M/pM, considered as k-linear space of dimension N. It is well known (Fitting) that for such an automorphism there always exist N linearly independent eigenvectors for the eigenvalue 1. We may therefore assume that

$$V^{-n} F^m x_i^{(1)} = x_i^{(1)} \mod pM \qquad (i = 1, \ldots, N).$$

Now assume that we have already found elements $x_i^{(k)}$ such that $V^{-n}F^m x_i^{(k)} \equiv x_i^{(k)} \mod p^k M$. We are looking for an element $x_i^{(k+1)}$ of the form $x_i^{(k+1)} = x_i^{(k)} + p^k \xi_i$. In vector notation we have $x^{(k)} = (x_i^{(k)})$, $\xi = (\xi_i)$, $V^{-n}F^m x^{(k)} - x^{(k)} = p^k y$. The condition on ξ can be written as

$$V^{-n} F^m (x^{(k)} + p^k \xi) \equiv x^{(k)} + p^k \xi \mod p^{k+1} M,$$

whence

$$y + V^{-n} F^m \xi \equiv \xi \mod pM.$$

It is easy to see that this congruence is soluble: put $\xi = x^{(k)}A$, $y = x^{(k)}B$, where A and B are $N \times N$ matrices with elements in W; then $V^{-n}F^m \xi \equiv x^{(k)} A^{\sigma^{m+n}} \mod pM$, and the equation for $A = \| a_{ij} \|$

$$A - A^{\sigma^{m+n}} \equiv B \mod p$$

reduces to N^2 non-linear equations for the elements $a_{ij} \mod p$, which have a solution, because k is algebraically closed.

This completes the proof of the lemma.

THEOREM 3.1. *Let M be an equidimensional module. Then among the special submodules of M there exists a unique maximal one, $M_0 \subset M$. The factor module M/M_0 is of finite length.*

PROOF. We express M_F as a direct sum of submodules of the form $\bigoplus (M_i)_F$, where M_i are the homogeneous components of pairwise different types. The submodules $(M_i)_F$ of M_F are defined uniquely up to order. We embed M in M_F.

The module $M \cap (M_i)_F$ is homogeneous. Let $M_{0i} \subset M \cap (M_i)_F$ be the W-module generated by all the special elements of this intersection. Then it is clear that M_{0i} is a homogeneous special module, and hence $M_0 = \bigoplus_i M_{0i}$ is a special module. Let $M' = \bigoplus M_i'$ be any special submodule of M, where $M_i' = M' \cap (M_i)_F$. By Lemma 3.3, M_i' is generated by special elements over W, and so $M_i' \subset M_{0i}$. Therefore $M' \subset M_0$ and M_0 is the required maximal special submodule.

The module $\bigoplus_i E/E(F^{m_i} - V^{n_i})$ is special, therefore in any case M contains a dense special submodule (cf. the remark to Lemma 3.1). A fortiori the maximal special submodule M_0 is dense in M, hence M/M_0 has finite length. This proves the theorem.

REMARK. It is not hard to see that the notion of a special element for any equidimensional module M (not necessarily homogeneous) can be characterized as follows. Let $M_0 \subset M$ be the maximal special submodule, $M_0 = \bigoplus_i M_{0i}$ its decomposition as a direct sum of special homogeneous submodules (of pairwise different types). Then the element x of M is special if it belongs to one of the M_{0i} and is special in it. With this definition Lemma 3.3 remains true for not necessarily homogeneous modules.

§3. The algebraic structure on the module space

1. Let M_0 be a special module. We shall say that a given module M *belongs* to M_0 if the maximal special submodule of M is isomorphic to M_0. When M_0 is already a submodule of M, the terminology "M belongs to M_0" signifies that M_0 is the special submodule of M.

Any module M belonging to M_0 can be realized as a certain dense submodule of $(M_0)_F$ containing M_0. For every such submodule there exist natural numbers h and g such that

$$M_0 \subset M \subset p^{-h} M_0, \qquad M_0 \subset M \subset F^{-g} M_0.$$

Let $x \in M_F$; then the *p-height* (respectively, *F-height*) of x over the dense submodule M' of M_F is defined as the least number h such that $p^h x \in M'$ ($F^h x \in M'$); the height of a module $M'' \supset M'$ is defined as the maximum of the heights of the elements of M'' over M'.

For any special module M_0 we consider the class of modules M belonging to M_0 and isomorphic to modules $M \supset M_0$ of p-height at most h over M_0. Later we shall show that for sufficiently large h this class contains all modules belonging to M_0. The aim of this section is to introduce into this class the structure of an algebraic set (for a more precise formulation see below).

2. THEOREM 3.2. *There is a one-to-one correspondence between the set of all E-modules M belonging to a fixed special module M_0 and satisfying the condition*

$$M_0 \subset M \subset p^{-h} M_0, \tag{3.1}$$

where $h \geqslant 1$ is a fixed natural number, and the points of a certain constructive algebraic set [1] *over the field k.*

PROOF. We shall construct the required algebraic set in several steps.

Let N be the rank of the W-module M_0. As a first step we shall parametrize the set of all W-modules M satisfying (3.1). For each such module there exist a W-basis $(x_1, \ldots, x_N)$ of M_0 and integers $0 \leqslant e_1 \leqslant e_2 \leqslant \ldots \leqslant e_N \leqslant h$ such that the elements $p^{-e_1}x_1, \ldots, p^{-e_N}x_N$ constitute a W-basis for M. The system of numbers $e = (e_1, \ldots, e_N)$ defines the module M uniquely; we

[1] By a constructive algebraic set we understand the union of a finite number of subsets of a projective space that are locally closed in the Zariski topology.

shall call it the *index* of M over M_0. There exists only a finite number of admissible indices (but the number increases with h).

Any module M such that $M_0 \subset M \subset p^{-h}M_0$ is completely determined by its image in $p^{-h}M_0/M_0$ under the natural homomorphism $M \to M/M_0 \to p^{-h}M_0/M_0$. The index of M is $(e_1, \ldots, e_N)$ if and only if the corresponding submodule of $p^{-h}M_0/M_0$ is isomorphic to $\bigoplus_{i=1}^{N} W_h(k)/(p^{e_i})$, where $W_h(k)$ is the W-module of Witt vectors of length h. On the space A_e of such modules the group of automorphisms of $p^{-h}M_0/M_0$ acts transitively; by choosing a basis of this module we can identify this group with $G_k = GL(N, W_h(k))$. This group G_k represents the group of geometric points of a certain linear algebraic group G defined over the prime field of characteristic p; this follows from well-known facts on the composition law of Witt vectors. (In this connection cf. the paper [38] by Greenberg and the beginning of the paper [58] by Serre.) The action may be transferred to M as follows: let $M \supset M_0$ and $g \in G_k$. We fix a right action of G_k on the factor module $p^{-h}M_0/M_0$; then

$$Mg = \{x \mid x \bmod M_0 \in (M/M_0)\, g\}.$$

We shall show that the stabilizer $G_0 \subset G$ of any given module M of index e is closed. Indeed, let $(x_1, \ldots, x_N)$ be a W-basis of M_0, $(p^{-e_1}x_1 \ldots, p^{-e_N}x_N)$ a W-basis of M, and $\bar{x}_i = x_i \bmod M_0$. Let $g_{ij}^{(k)}(g)$, $1 \leqslant i, j \leqslant N$, $1 \leqslant k \leqslant h$, be functions on G determined by the conditions

$$\begin{pmatrix} \bar{x}_1 g \\ \vdots \\ \bar{x}_N g \end{pmatrix} = \| g_{ij} \| \begin{pmatrix} \bar{x}_1 \\ \vdots \\ \bar{x}_N \end{pmatrix}, \qquad g \in G_k,$$

$$g_{ij} = (g_{ij}^{(1)}(g), \ldots, g_{ij}^{(h)}(g)) \in W_h(k).$$

To say that g belongs to the stabilizer G_0 of M means that

$$p^{h-e_k} \bar{x}_k\, g = \sum_{i=1}^{N} p^{h-e_k} g_{ki} \bar{x}_i \in M/M_0,$$

i.e., that

$$v_p(p^{h-e_k} g_{ki}) = v_p(g_{ki}) + h - e_k \geqslant h - e_i.$$

This condition is equivalent to the system of equations

$$g_{ki}^{(l)}(g) = 0, \qquad l \leqslant e_k - e_i, \qquad 1 \leqslant k, i \leqslant N,$$

defining a closed subgroup in G whose set of geometric points coincides with G_0.

It follows that there is a natural structure on A_e, and this allows us to identify this set with the set of geometric points of the homogeneous space of right cosets G/G_0 (it is not hard to see that our construction is formed by analogy with flag manifolds in an ordinary affine space; cf. Grothendieck [46]). This concludes the first step.

The second step consists in selecting from the set A_e those W-modules that are also E-modules. It remains to show that this is an algebraic condition. Let F_0 and V_0 be the semilinear mappings of the W-module M_0 into itself that are induced by multiplication by the elements F and V,

respectively, of the ring E. Let e be a given index and $M \supset M_0$ a module of index e with basis $(p^{-e_1}x_1, \ldots, p^{-e_N}x_N)$. We shall identify F_0 and V_0 with the matrices that describe their action relative to the basis $(\bar{x}_1, \ldots, \bar{x}_N)$:

$$\begin{pmatrix} F\bar{x}_1 \\ \vdots \\ F\bar{x}_N \end{pmatrix} = F_0 \begin{pmatrix} \bar{x}_1 \\ \vdots \\ \bar{x}_N \end{pmatrix}, \qquad \begin{pmatrix} V\bar{x}_1 \\ \vdots \\ V\bar{x}_N \end{pmatrix} = V_0 \begin{pmatrix} \bar{x}_1 \\ \vdots \\ \bar{x}_N \end{pmatrix}.$$

The conditions expressing that Mg is an E-module read

$$F(Mg) \subset Mg, \qquad V(Mg) \subset Mg. \tag{3.2}$$

As before, let $\| g_{ij} \|$ be the matrix corresponding to $g \in G_k$ in the basis $(\bar{x}_1, \ldots, \bar{x}_N)$. We have

$$F(Mg) = (FM)\, g^{\sigma}, \quad V(Mg) = (VM)\, g^{\sigma^{-1}};$$

Now condition (3.2) means that $(FM)g^{\sigma}g^{-1} \subset M$, $(VM)g^{\sigma^{-1}}g^{-1} \subset M$, i.e.

$$\| g_{ij} \|\, \| g_{ij}^{\sigma} \| F_0 \begin{pmatrix} p^{h-e_1}\bar{x}_1 \\ \vdots \\ p^{h-e_N}\bar{x}_N \end{pmatrix} \subset M/M_0; \quad \| g_{ij} \|^{-1}\, \| g_{ij}^{\sigma^{-1}} \| V_0 \begin{pmatrix} p^{h-k_1}\bar{x}_1 \\ \vdots \\ p^{h-e_N}\bar{x}_N \end{pmatrix} \subset M/M_0.$$

Let us denote by $\bar{G}$ the variety of all $N \times N$ matrices with elements in $W_h(k)$, identify G_k with a subset of $\bar{G}$, and denote by $\bar{G}_0$ the closure of G_0 in $\bar{G}$. Then Mg is an E-module if and only if

$$\| g_{ij} \|^{-1}\, \| g_{ij}^{\sigma} \| F_0 \in \bar{G}_0, \quad \| g_{ij} \|^{-1}\, \| g_{ij}^{\sigma^{-1}} \| V_0 \in \bar{G}_0.$$

The mappings φ_1: $G \to \bar{G}$ and φ_2: $G \to \bar{G}$ defined by the equations

$$\varphi_1(\| g_{ij} \|) = \| g_{ij} \|^{-1}\, \| g_{ij}^{\sigma} \| F_0,$$
$$\varphi_2(\| g_{ij} \|) = \| g_{ij} \|^{-1}\, \| g_{ij}^{\sigma^{-1}} \| V_0,$$

are morphisms of the quasi-algebraic structure[1] of G. Therefore the set $H_k = \varphi_1^{-1}(\bar{G}_0) \cap \varphi_2^{-1}(\bar{G}_0) \subset G_k$ represents the set of geometric points of a certain closed subvariety $H \subset G$. The image of H under the projection $G \to G/G_e$ is a constructive algebraic set whose geometric points are in one-to-one correspondence with the set of E-modules $M \supset M_0$ of index e. This concludes the second step.

The third and last step consists in choosing from the set H_k the points corresponding to those modules that contain no special elements apart from those belonging to M_0.

Let $x \in p^{-h}M_0$ be a special element. The condition that this lies in Mg means that

$$(x \mod M_0)\, g^{-1} \in M/M_0.$$

But the mapping of k-varieties φ_x: $G \to p^{-h}M_0/M_0$ defined by the formula

$$\varphi_x(g) = (x \mod M_0)\, g^{-1},$$

is a morphism[2]. Now Mg contains x if and only if g belongs to

[1] For the definition of a quasi-algebraic structure see the paper [57] by Serre.

[2] We regard here $p^{-h}M_0/M_0$ as an affine variety whose geometric points are in one-to-one correspondence with the elements of this factor module.

$F_x = \varphi^{-1}(M/M_0)$. This set is closed, as inverse image of the closed set $M/M_0 \subset p^{-h}M/M_0$. From H_k we have to discard the points contained in the union $\bigcup_x F_x$, taken over all special elements $x \in p^{-h}M_0$, $x \notin M_0$. The image of $P \setminus \bigcup_x F_x$ under the projection $G \to G/G_0$, by what has been said above, is in one-to-one correspondence with the set of E-modules $M \supset M_0$ of height at most h, index e, and belonging to M_0. To complete the proof of the theorem it remains to verify that $\bigcup F_x$ is closed.

LEMMA 3.4. *The special elements $x \in p^{-h}M_0$ belong to a finite number of cosets* mod M_0.

PROOF. Clearly it is enough to verify the lemma in the case when M_0 is a homogeneous module of type (m, n). Let $(y_1, \ldots, y_N)$ be a special basis of $p^{-h}M_0$. The element $x = \sum_{i=1}^{N} a_i y_i$, $a_i \in W$, is special if and only if $F^m V^n x = x$, i.e. if $a_i^{\sigma^{m+n}} = a_i$. Now the cosets of special elements $x \bmod M_0$ are in one-to-one correspondence with the sets $(a_1, \ldots, a_N)$ of elements of $W_h(k)$ satisfying the condition $a_i^{\sigma^{m+n}} = a_i$. Clearly these sets are finite in number; thus the lemma is established.

The proof of Theorem 3.2 is now complete.

3. Let us denote by $A(M_0, h)$ the constructive algebraic set obtained in the proof of Theorem 3.2. Its points are in one-to-one correspondence with the E-modules M, $M_0 \subset M \subset p^{-h}M_0$, belonging to the given special submodule M_0. Clearly any two E-modules belonging to non-isomorphic special submodules cannot be isomorphic. It therefore remains to clarify the distribution of the points in $A(M_0, h)$ that correspond to isomorphic E-modules.

THEOREM 3.3. *There exists a finite group $\Gamma(M_0, h)$ of automorphisms of $A(M_0, h)$ such that two points correspond to isomorphic E-modules if and only if they belong to the same orbit relative to $\Gamma(M_0, h)$.*

PROOF. Let us identify each module with the corresponding point.

We first define the action of the group Γ of automorphisms of M_0 on $A(M_0, h)$. The group Γ acts in an obvious way on the set A_e (with the same meaning as in the proof of Theorem 3.2). We need only verify that it maps $A(M_0, h)$ into itself; but this is clear, because the condition for M to belong to $A(M_0, h)$ is invariant under the action of Γ. Moreover, any modules transformed into each other by Γ are clearly isomorphic.

Conversely, let M', $M'' \in A(M_0, h)$ be isomorphic modules. Any isomorphism $M' \to M''$ induces an isomorphism of the corresponding special submodules. Now M', M'' have the same maximal special submodule, namely M_0, therefore any isomorphism $M' \to M''$ induces a certain automorphism of M_0.

As we shall see below, the group Γ is infinite. However, its action on $A(M_0, h)$ is very ineffective, and there is a normal subgroup of finite index leaving $A(M_0, h)$ elementwise fixed. Clearly any element of Γ that does not move the coset of x mod M_0 for all special elements $x \in p^{-h}M_0$, leaves all points of $A(M_0, h)$ fixed. But by Lemma 3.4 there are only finitely many such cosets. Hence we may take for $\Gamma(M_0, h)$ the permutation group of these cosets induced by the action of Γ.

It only remains to verify that the action of $\Gamma(M_0, h)$ is compatible with the algebraic set structure on $A(M_0, h)$. This is a routine argument similar to that which was used in the proof of Theorem 3.2. We allow

ourselves to omit the details.

This completes the proof of Theorem 3.3.

4. We shall now summarize in qualitative terms the structure of the set of isomorphism classes of modules, isogenous to a fixed equidimensional module M. First, however, we formulate the two finiteness theorems which will be proved below.

THEOREM 3.4 (First finiteness theorem). *The number of non-isomorphic special modules isogenous to a fixed module is finite.*

THEOREM 3.5 (Second finiteness theorem). *The height of a module M over its maximal special submodule M_0 is bounded by a number H that depends only on the isogeny class of the module M.*

CLASSIFICATION THEOREM. *Every equidimensional E-module M is determined by the following collection of invariants:*

1) *the system of pairs of coprime integers $((m_i, n_i))$ which define the isogeny class of M:*

$$M \sim \bigoplus_i E/E\,(F^{m_i} - V^{n_i});$$

2) *the maximal special submodule $M_0 \subset M$ (this is a discrete invariant to which we may adjoin, for example, the index of M over M_0, changing slightly the formulation of the following point);*

3) *the $\Gamma(M_0, H)$-orbit of the space $A(M_0, H)$, where H by the second finiteness theorem depends only on the collection $((m_i, n_i))$.*

Two E-modules are isomorphic if and only if all these invariants coincide.

5. We add a few remarks on the nature of the results obtained. First of all we note that they provide an effective construction[1] of a complete system of invariants in the sense that it is possible in principle to construct, for any isogeny class of equidimensional modules, a finite set of algebraic systems of modules, containing up to isomorphism all modules of the given class, and containing any given module only a finite number of times. The identification of isomorphic modules, as we shall see later, is also fully effective.

This construction enables us, for example, to carry out the explicit classification in a very clear form for all modules corresponding to two-dimensional formal groups. The results so obtained will be given later, in §9 of this chapter.

Further, for cyclic modules isogenous to simple ones a complete enumeration will be obtained for the components of the highest dimension of the space corresponding to this class. This result and a number of others, of a more partial nature, on the structure of the module space, will be given below.

In all cases that have been checked the space $A(M_0, H)$ with a 'good' subdivision turned out to be the union of affine varieties invariant under the action of the group $\Gamma(M_0, H)$, so that the quotient space $A(M_0, H)/\Gamma(M_0, H)$ is an algebraic (even affine) variety. We have not been able to prove this in the general case.

---

[1] Because as we shall see below, both finiteness theorems allow in principle an effective enumeration of the special modules and the bound for H.

The space $A(M_0, H)$ can be interpreted as the solution of a certain universal problem à la Grothendieck [42]: the assignment of a special basis of M/M_0 amounts to introducing 'rigidity'. We shall not enter into the details. Nor are we able to touch on the question of specializations in the module space. The possible 'jumps' from one component to another under specializations seem to possess a very complex character. With some definitions, specialization may even change the isogeny class of the group; thus, the group $G_{1,0} = X$ specializes to the group $G_{1,1}$ under the passage to the super-singular invariants of the elliptic curve X (cf. Ch. IV, §5).

§4. The structure of isosimple modules; subsidiary reduction

1. Let m, n be coprime natural numbers, $k_{m+n} \subset k$ the subfield of p^{m+n} elements, and $E_{n,m}$ the 'cyclic local algebra' defined as $E_{n,m} = W(k_{m+n})[\theta]$, where θ is an element satisfying the following commutation law for the coefficients:

$$\theta c = c^{\sigma^{-(a+b)}}\theta, \quad c \in W(k_{m+n}), \qquad am - bn = 1,$$

as well as satisfying the identity $\theta^{m+n} = p$.

The quotient field of the algebra $E_{n,m}$ is denoted by $K_{n,m}$.

Consider the left $W(k)$-module

$$M_{n,m} = W(k) \underset{W(k_{m+n})}{\otimes} K_{n,m}$$

($W(k)$ is a right $W(k_{m+n})$-module relative to the inclusion $W(k_{m+n}) \subset W(k)$, while K_{m+n} is a left $W(k_{m+n})$-module by definition).

Let K be the quotient field of the ring $W(k)$. Then the module M_{m+n} can be regarded as a linear space over K, by putting $p^{-1}(a \otimes \xi) = a \otimes p^{-1}\xi$. The dimension of $M_{n,m}$ is $m + n$; as a basis we may take the elements $1 \otimes 1$, $1 \otimes \theta$, ..., $1 \otimes \theta^{m+n-1}$. Henceforth we shall sometimes omit the sign $\otimes$ and use an expression of the form $\sum a_i \theta^i$, $a_i \in W(k)$, for the elements of $M_{n,m}$.

We now introduce two further structures on $M_{n,m}$.

In the first place $M_{n,m}$ can be regarded as a right $K_{n,m}$-module by setting

$$(a \otimes \xi)\tau = a \otimes \xi\tau; \quad a \in W(k); \quad \xi, \tau \in K_{n,m}.$$

Secondly, we define an E_F-module structure on $M_{n,m}$. Since the action of W on $M_{n,m}$ has already been given, it only remains to specify the action of F. We shall put

$$F\theta^i = \theta^{i+n} \qquad (i \text{ any integer}).$$

2. LEMMA 3.5. 1) $M_{n,m} \approx (E/E(F^m - V^n))_F$, *quâ* E_F*-modules.*

2) *Any finitely generated non-zero* E*-submodule of* $M_{n,m}$ *is dense.*

PROOF. The required isomorphism $M_{n,m} \to (E/E(F^m - V^n))_F$ can be defined, for example, thus: $1 \to 1_E \bmod E(F^m - V^n)$. The verification of the remaining statements is quite mechanical.

The second statement follows from the fact that $M_{n,m}$ is simple.

3. LEMMA 3.6. *Let $T \subset W(k)$ be a 'multiplicative system of representatives' for the residue class field k (including zero). Any element x of $M_{n,m}$ can be uniquely expressed in the form*

$$x = \sum_{i>-\infty} \varepsilon_i \theta^i, \quad \varepsilon_i \in T. \tag{3.3}$$

An element x in this form is special if and only if the coefficients ε_i satisfy the conditions $\varepsilon_i^{\sigma^{m+n}} = \varepsilon_i$, i.e. if they are contained in the multiplicative system of representatives for the subring $W(k_{m+n})$ of $W(k)$.

PROOF. Clearly every element x can be expressed in the form $\sum_{i>-\infty} \varepsilon_{ij} p^i \sum_{j=0}^{m+n-1} \theta^j = \sum_{\substack{i>-\infty \\ 0 \leqslant j \leqslant m+n-1}} \varepsilon_{ij} \theta^{(m+n)i+j}$, so that a representation of the form (3.3) is always possible. Its uniqueness is immediate. The condition for x to be special is that $F^{-m} V^n x = x$, i.e. $\sum \varepsilon_i \theta^i = \sum \varepsilon_i^{\sigma^{-m-n}} \theta^i$, from which the last assertion of the lemma follows by the uniqueness of (3.3).

4. LEMMA 3.7. *The multiplication of the elements of $M_{n,m}$ on the right by any non-zero element of $K_{n,m}$ is an E_F-module automorphism of $M_{n,m}$. Conversely, any non-zero E_F-module endomorphism of $M_{n,m}$ is induced by right multiplication by a certain element of $K_{n,m}$ which is uniquely determined. An automorphism leaving all special elements fixed is the identity.*

PROOF. The only part of the first statement that is not completely obvious is the verification that the action of F commutes with right multiplication by any element α of $K_{n,m}$. It is enough to verify this in the case when $\alpha = \varepsilon \theta^j \neq 0$, $\varepsilon \in T \cap W(k_{m+n})$. Then we have

$$F\left[\left(\sum_i a_i \theta^i\right) \varepsilon \theta^j\right] = F\left(\sum_i a_i \varepsilon^{\sigma^{-(a+b)i}} \theta^{i+j}\right) = \sum_i a_i^{\sigma} \varepsilon^{\sigma^{-(a+b)i+1}} \theta^{i+j+n}.$$

On the other hand,

$$\left[F\left(\sum_i a_i \theta^i\right)\right] \varepsilon \theta^j = \left(\sum_i a_i^{\sigma} \theta^{i+n}\right) \varepsilon \theta^j = \sum_i a_i^{\sigma} \varepsilon^{\sigma^{-(a+b)(i+n)}} \theta^{i+j+n}.$$

But $-(a+b)n = 1 - a(m+n)$ and $\varepsilon^{\sigma^{-a(m+n)}} = 1$ and from this the assertion follows. Now let $\varphi : M_{n,m} \to M_{n,m}$ be a given E_F-endomorphism. If this leaves the unit-element fixed, $\varphi(1) = 1$, then $\varphi(F^k V^l \cdot 1) = F^k V^l \varphi(1) = \theta^{kn+lm}$, $V = pF^{-1}$, so that φ leaves all elements θ^i fixed and hence is the identity. Otherwise let $\varphi(1) = \alpha = \sum \varepsilon_i \theta^i$; considering α as element[1] of $K_{n,m}$ we see that the automorphism $\varphi \circ \alpha^{-1}$ defined by $\varphi \circ \alpha^{-1}(x) = \varphi(x) \circ \alpha^{-1}$, leaves the unit-element fixed. Hence φ reduces to right multiplication by α and so the lemma is proved.

§5. The structure of isosimple modules; proof of the first finiteness theorem

1. LEMMA 3.8. *Let m and n be two coprime positive integers. Then*

[1] This is possible because α, like 1, is a special element, so that $\varepsilon_i \in W(k_{m+n})$ by Lemma 3.6.

the integer N can be expressed in the form $am + bn$, where a, b are integers $\geqslant 0$, if and only if $mn - m - n - N$ cannot be expressed in this form.

COROLLARY 1. *All integers $N \geqslant (m-1)(n-1)$ can be expressed in the form $am + bn$, $a, b \geqslant 0$, but $(m-1)(n-1) - 1 = mn - m - n$ cannot be expressed in this form.*

COROLLARY 2. *The number of integers N, satisfying $0 \leqslant N \leqslant mn - m - n$ and representable as $am + bn$ is equal to the number of integers not representable in this form and is $\frac{1}{2}(m-1)(n-1)$.*

PROOF. Let $N \geqslant (m-1)(n-1)$, and put $N = am + bn$, where a, b are integral, but not necessarily non-negative. We express a in the form $a_0 + cn$, $0 \leqslant a_0 \leqslant n-1$, and consider the representation $N = a_0 m + b_0 n$, where $b_0 = b + mc$. We have

$$b_0 = \frac{N - a_0 m}{n} \geqslant \frac{N - (n-1)m}{n} \geqslant -\frac{n-1}{n},$$

so that $b_0 \geqslant 0$, because b_0 is an integer. Then $N = a_0 m + b_0 n$ is the required representation.

Now let $0 \leqslant N \leqslant mn - m - n$. If N is representable, then $mn - m - n - N$ is not representable. For otherwise $mn - m - n$ would be representable, but from the equation $mn - m - n = am + bn$ it follows that $a \equiv -1 \bmod n$, $b \equiv -1 \bmod m$, hence $a \geqslant n-1$, $b \geqslant m-1$, which is a contradiction.

Conversely, if N is not representable, then $mn - m - n - N$ is representable. For otherwise we should have $N = am - bn$, $0 \leqslant a \leqslant n-1$, $b > 0$, but then $mn - m - n - N = (n - 1 - a)m + (b-1)n$. This completes the proof of the lemma.

2. Let M be an isosimple[1] module. We embed M in $M_F \approx W(k) \otimes K_{n,m}$. Every element x of M can be written in the form $x = \sum_{i > -\infty} \varepsilon_i \theta^i$. Let us put $\nu(x) = \min i$, subject to the condition $\varepsilon_i \neq 0$. We choose an element $x = \sum_{i \geqslant i_0} \varepsilon_i \theta^i$ for which $i_0 = \nu(x)$ has the least possible value (for the given embedding), and consider a new embedding $M \to M_F$ for which $1 + \sum_{i>0} \eta_i \theta^i \in M$ (this is the composition $M \xrightarrow{\psi} M_F \xrightarrow{\varphi} M_F$, where φ is right multiplication by $\theta^{-i_0} \in K_{n,m}$ and ψ is the original embedding). We identify M with its image under this embedding. Then M coincides with the submodule $W(k) \otimes E_{n,m}$ and contains an element that is $\equiv 1 \bmod W(k) \otimes E_{n,m}\theta$.

Let $J = J(M)$ be the set of all integers of the form $\nu(x)$, $x \in M$. It is easy to see that $\nu(Fx) = \nu(x) + n$, $\nu(Vx) = \nu(x) + m$. Therefore the set J is invariant under translations of the form $am + bn$, $a, b > 0$, and moreover, $0 \in J$ (because $0 = \nu(1 + \sum_{i>0} \eta_i \theta^i)$). It follows from Lemma 3.8 that for $N \geqslant (m-1)(n-1)$ we have $N \in J$ and the set $\overline{J} = Z_+ \setminus J$ contains at most $\frac{1}{2}(m-1)(n-1)$ elements.

3. LEMMA 3.9. *Let M be an isosimple module of type (m, n) satisfying the above conditions. Consider the finite set of integers $\overline{J}$ defined above.*

---

[1] That is, isogenous to a simple module.

a) *The set* $\overline{J}$ *does not depend on the choice of the embedding*[1] *and is an invariant of the module* M.

b) *For the given embedding* $M \subset W(k) \otimes E_{n,m}$ *the module* M *contains a system of elements of the form*

$$z_{j_i} = \theta^{j_i} + \sum_{\substack{k \in \overline{J} \\ k > j_i}} \varepsilon_{ik}\theta^k, \qquad \varepsilon_{ik} \in T.$$

Here j_i *runs over all numbers of* J *such that* $j_i - m \in \overline{J}$, $j_i - n \in \overline{J}$. *The system* $\{z_{j_i}\}$ *is uniquely determined and coincides with a minimal generating set of the* E*-module* M. *It will be called a standard system. The module* M *is special if and only if all elements* z_{j_i} *are special.*

PROOF. a) Any embedding $M \subset W(k) \otimes E_{n,m}$, containing x such that $\nu(x) = \min_{y \in M} \nu(y) = 0$, differs from another such embedding by right multiplication by a unit in $E_{n,m}$ for which $\nu(y)$, $y \in M$, is invariant.

b) The existence of systems of the form described is evident; the elements may be constructed successively, by choosing at the j-th step, $j \in J$, any element $z' \in M$ of the form $z' = \theta^j + \sum_{i>j} \varepsilon_{ij}\theta^i$ and then putting

$$z_j = 0, \quad \text{if} \quad j \in \bigcup_{i_k < j} \{j_k + am + bn\},$$

$$z_j = z'_j - \sum_{i \in J} \eta_{ij} z'_j, \quad \text{if} \quad j \notin \bigcup_{j_k < j} \{j_k + am + bn\},$$

where the elements $\eta_{ij} \in W(k)$ are chosen so that the decomposition of z_j has the form given in the lemma.

Let us show now that the elements z_j form a minimal generating system of the E-module M. In fact, from the equality $J = \bigcup_i \{j_i + am + bn\}$ it follows that $M = \sum_i E z_{j_i}$. The minimal number of generators of M agrees with the dimension of the k-linear space $M/(FM + VM)$, by Nakayama's Lemma. But the images of z_{j_i} in this linear space are clearly linearly independent; since the z_{j_i} generate M, it follows that they form a minimal system.

The elements z_{j_i} are uniquely determined, because otherwise $\nu(z_{j_i} - z'_{j_i}) \in \overline{J}$, which is impossible, because $z_{j_i} - z'_{j_i} \in M$.

If M is special, then the elements z_{j_i} are special. For otherwise $F^{-m}V^n z_{j_i} = z'_{j_i} = z_{j_i}$, $z'_{j_i} \in M$, has the same form as z_{j_i}, which contradicts the uniqueness. Conversely, it is clear that if the z_{j_i} are special, then M is special.

This completes the proof of the lemma.

4. COROLLARY 1 (First finiteness theorem for isosimple modules). *There exist only a finite number of non-isomorphic special modules*

[1] We have in mind only embeddings for which $\min\{\nu(x) \mid x \in M\} = 0$.

isogenous to a fixed simple module.

PROOF. Indeed, every special submodule $M \subset W(k) \otimes E_{n,m}$, $0 \in J$, is defined by the finite collection of coefficients $\varepsilon_{ik} \in T \cap W(k_{m+n})$, satisfying the conditions $\varepsilon_{ik}^{\sigma^{m+n}} = \varepsilon_{ik}$, that occur as coefficients in the standard system of generators. The number of coefficients in such a collection in every case cannot exceed $\frac{1}{2}r(m-1)(n-1)$, where r is the number of elements of $\bar{J}$, and this gives for the number of non-isomorphic special modules isogenous to $E/E(F^m - V^n)$ the upper bound $p^{\frac{1}{2}r(m-1)(n-1)(m+n)}$, $r \leqslant \min(m, n)$, because $j_i \not\equiv j_k \bmod m$ and $\bmod n$. This bound is of course much too large, besides we have not taken into account the fact that different choices of coefficients may give isomorphic modules.

COROLLARY 2 (Second finiteness theorem for isosimple modules). *Let M be an isosimple module of type (m, n), and $M_0 \subset M$ its maximal special submodule. Then $F^{m-1}M \subset M_0$.*

PROOF. In fact, $F^{m-1}M \subset W(k) \otimes E_{n,m}\theta^{(m-1)n} \cap M$, but by Lemmas 3.8 and 3.9, $M \supset W(k) \otimes E_{n,m}\theta^{(m-1)n}$, because all elements $x \in M_F$ for which $\nu(x) \geqslant (m-1)(n-1)$ belong to M. But the module $W(k) \otimes E_{n,m}\theta^{(m-1)n}$ is special.

EXAMPLE 1. Let us show that any module M isogenous to a module of the form $E/E(F - V^n)$ is isomorphic to such a module. The same holds for modules isogenous to $E/E(F^m - V)$.

Indeed, if $m = 1$ or $n = 1$, then $\bar{J}$ must be empty. Therefore the standard system of generators constructed in Lemma 3.9 consists of the single element 1.

It follows that $M \approx E \cdot 1 = E/E(F - V^n)$ (respectively, $E/E(F^m - V)$).

EXAMPLE 2. Let us describe all special modules isogenous to

$$E/E(F^2 - V^{2m+1}), \quad m \geqslant 0.$$

The set of natural numbers $\bar{J}$ whose complement contains 0 and is mapped into itself by all translations of the form $2a + (2m+1)b$, $a, b \geqslant 0$, clearly must have the form $(1, 3, 5, \ldots, 2i-1)$, where $0 \leqslant i \leqslant m$ ($\bar{J}$ is empty if $i = 0$). The complement of such a set is

$$J_i = \{2a + (2m+1)b\} \cup \{2i + 1 + 2a + (2m+1)b\}, \quad a, b \geqslant 0.$$

By Lemma 3.9 the special submodule $M \subset W(k) \otimes E_{2m+1,2}$ containing 1 is generated by the elements 1, θ^{2i+1} if the set $J(M) = \{\nu(x) \mid x \in M\}$ coincides with J_i. By Lemma 3.9a), all these modules are non-isomorphic. Thus, we have obtained a complete classification of such modules.

It is clear that an entirely analogous investigation can be carried out in the case

$$M \sim E/E(F^{2m+1} - V^2).$$

We note the following general symmetry principle: the classification of modules isogenous to $\bigoplus_i E/E(F^{m_i} - V^{n_i})$ differs from the classification of modules isogenous to $\bigoplus_i E/E(F^{n_i} - V^{m_i})$ only in the replacement of σ by σ^{-1} in all the calculations.

5. A description of the special isosimple modules can also be given in classical terms.

Consider a non-principal order $E^0_{n,m} = W(k_{m+n})[\Theta^n, \Theta^m] \subset E_{n,m}$; by a (fractional) left ideal $\mathfrak{a}$ of $E^0_{n,m}$ we understand a finitely generated left $E^0_{n,m}$-module consisting of elements of $K_{n,m}$. Two ideals $\mathfrak{a}$, $\mathfrak{a}'$ are said to be equivalent if there exists an element α of $K_{n,m}$ such that $\mathfrak{a} = \mathfrak{a}'\alpha$. Equivalent ideals are combined into one class.

THEOREM 3.6. *The isomorphism classes of special modules of type (m, n) can be put into one-to-one correspondence with the classes of (fractional left) ideals of the order $E^0_{n,m}$.*

PROOF. We may establish a correspondence between the special modules $M \subset W(k) \otimes K_{n,m}$ and the sets M_s of special elements in M. Then M_s is a $W(k_{m+n})[F, V]$-submodule of M and, moreover, $F^m - V^n$ belongs to the annihilator of M_s. Hence there is a natural left $W(k_{m+n})[F, V]/W(k_{m+n})[F, V](F^m - V^n)$-module structure on M_s. Now the ring $W(k_{m+n})[F, V]/P$, where $P = (F^m - V^n)$, is isomorphic to $E^0_{n,m}$. Therefore M corresponds to an $E^0_{n,m}$-ideal: the image of M_s under the identification mapping $W(k_{m+n}) \otimes K_{n,m} \to K_{n,m}$.

Any other embedding of M in $W(k) \otimes K_{n,m}$ differs from the one chosen before only by right multiplication by an element $\alpha \in K_{n,m}$ which maps special elements to special elements.

Finally, the E-module M can clearly be uniquely reconstructed (up to isomorphism) from the $E^0_{n,m}$-module M_s.

Thus the theorem is proved.

REMARK. It would be interesting to calculate the number of classes mentioned in the theorem. The following arguments allow us to estimate this number from below and to show that in every case it increases indefinitely with $\max(m, n)$, provided $\min(m, n) \geqslant 2$. Likewise, the number of components of the module space isogenous to $E/E(F^m - V^n)$ increases indefinitely.

According to Lemma 3.9 every class may be described in an invariant manner by means of a system of non-negative integers J, containing zero and mapped into itself by all translations to the right by m and n. Such a system J in turn corresponds uniquely to a collection of integers

$$0 = j_0 < j_1 < \cdots < j_r,$$

defined by the conditions $j_i \in J$, $j_i - m \notin J$, $j_i - n \notin J$, and from which J can be uniquely reconstructed.

Let us show first that to each system J there corresponds at least one ideal class. Indeed, let $\{j_i\}$ be the corresponding collection; then the ideal

$$M_s = \sum_i E^0_{n,m}\Theta^{j_i}$$

satisfies the condition $J = \{\nu(x) \mid x \in M_s\}$. For clearly $J \subset \{\nu(x) \mid x \in M_s\}$. On the other hand, M_s represents the free $W(k_{m+n})$-module generated by elements of the form Θ^k, where $k \in J$, and the values of k are pairwise incongruent mod $(m + n)$. Hence the assertion follows.

Thus, the number of classes cannot be less than the number of different admissible sets $\{j_i\}$. We shall give an estimate for this number. We

have $0 < j_i < (m-1)(n-1)$, $j_i \neq am + bn$, $a, b \geqslant 0$. Therefore $j_i = a_i m - b_i n$, $0 \leqslant a_i \leqslant n-1$, $0 \leqslant b_i \leqslant m-1$, and such a representation is unique. Further $a_i \neq a_k$ for $i \neq k$, because otherwise $j_i - j_k = 0 \bmod n$, which is impossible (in particular $a_i \neq 0$). Besides, if $a_i > a_k$, then $b_i > b_k$, because otherwise $j_i - j_k = (a_i - a_k)m + (b_k - b_i)n$, which is impossible. Finally, $a_i m - b_i n > 0$. Hence it follows that there is a one-to-one correspondence between the admissible collections $\{j_i\}$ and the pairs of sets $\{a_1, \ldots, a_r\}$, $\{b_1, \ldots, b_r\}$, consisting of positive integers satisfying the conditions:

$$1)\quad 1 \leqslant a_1 < a_2 < \ldots < a_r \leqslant n-1,$$
$$2)\quad 1 \leqslant b_1 < b_2 < \ldots < b_r \leqslant m-1,$$
$$3)\quad a_i m - b_i n > 0, \quad i = 1, \ldots, r.$$

Now the geometric interpretation of the pair (a_i, b_i) as a point with integer coordinates lying below the diagonal of the $m \times n$ rectangle allows us to conclude that the number of such collections grows rapidly with the size of max (m, n), when min $(m, n) \geqslant 2$.

6. We pass on to the proof of the first finiteness theorem for homogeneous modules. We shall prove a weaker result which is analogous to Lemma 3.9, and from which the required result will follow.

LEMMA 3.10. *Let $M \sim kE/E(F^m - V^n)$ be a special E-module and M_s the left $E^0_{n,m}$-module of its special elements.*

a) *M_s is isomorphic to a certain $E^0_{n,m}$-submodule of a free $E_{n,m}$-module M'_s of rank k, containing a generating system $(x_1, \ldots, x_k)$ of M'_s quâ $E_{n,m}$-module.*

b) *Any $E^0_{n,m}$-submodule M_s of M'_s containing the system $(x_1, \ldots, x_k)$ possesses over $E^0_{n,m}$ a system of generators of the form*

$$z = \sum_{i=1}^{k} x_i \sum_{j=0}^{mn-m-n} \varepsilon_{ij}\theta^j, \qquad \varepsilon_{ij} \in T \cap W(k_{m+n}).$$

PROOF. a) For M'_s we may take $E_{n,m} \otimes M_s$. The rank of this module is clearly equal to k, and it is free, because $E_{n,m}$ is a principal ideal domain. The required embedding is $M_s \to E_{n,m} \otimes M_s : m \to 1 \otimes m$.

b) From Lemma 3.8 it follows that for $N \geqslant (m-1)(n-1)$ we have $x_i\theta^N \in M_s$ for all $i = 1, \ldots, k$. Hence to obtain a generating system of the form described in the conditions of the lemma we need only take any generating system, write its elements in the form

$$\sum_{i=1}^{k} x_i \sum_{j=0}^{\infty} \varepsilon_{ij}\theta^j,$$

and omit superfluous terms. Thus the lemma is proved.

COROLLARY (First finiteness theorem). *There exist only a finite number of non-isomorphic special modules isogenous to a given one.*

§6. The second finiteness theorem

1. In this section we shall prove Theorem 3.5, called above the 'second finiteness theorem', with certain supplements, which provide the best possible result in this direction. For the constant H we shall give

an effective, though not the best possible bound (the best possible bound for isosimple modules was obtained in Corollary 2 of Lemma 3.9).

We begin by considering homogeneous modules. The following result is a quantitative formulation of Theorem 3.5 for this case.

THEOREM 3.7. *Let $M \sim kE/E(F^m - V^n)$ and let M_0 be its maximal special submodule. Then $F^{m(kn-1)}M \subset M_0$.*

For the proof we make use of the following

LEMMA 3.11. *There is a special basis of M_0, quâ W-module, which is of the form $(x_1, \ldots, x_{kn}; Fy_1, \ldots, Fy_{km})$; $x_i, y_i \in M_0$.*

PROOF. For $x_i, \ldots, x_{kn}$ we take the elements of any special basis of M_0, quâ W-module, whose images form a basis of the k-linear space M_0/FM_0, and for $y_1, \ldots, y_{km}$ corresponding elements with respect to M_0/VM_0. This is possible, because long $M_0/FM_0 = kn$, long $M_0/VM_0 = km$. The images of the elements x_i, Fy_j in the space M_0/pM_0 are linearly independent. Hence the elements x_i, Fy_j form a W-basis of M_0, because long $M_0/pM_0 = kn + km$.

Proof of Theorem 3.7. Let $x \in M$. We recall that the F-height of the element x over M_0 is the least number h such that $F^h x \in M_0$. Since M_0 is a dense submodule of M, such a number always exists. Now let us assume that the theorem is false. Then there exists an element whose F-height is greater than or equal to $m(kn-1)+1$. Let

$$x = F^{-H}\Big(\sum_{i=1}^{kn} a_i x_i + \sum_{j=1}^{km} b_j F y_j\Big), \qquad a_i,\ b_j \in W, \tag{3.4}$$

be an arbitrary element of the module M, where $(x_1, \ldots, x_{kn}; Fy_1, \ldots, Fy_{km})$ is a special basis of M, constructed as in the lemma. If there is a coefficient $a_i \not\equiv 0 \bmod p$, then the height of the element x is equal to H, and conversely.

Every element x can be uniquely expressed in the form (3.4), where H is the exact height of x; we shall call (3.4) a reduced representation for x.

Let us show that if $H \geqslant m(kn-1)+1$, then M contains a special element not belonging to M_0, which will contradict the definition of M_0. We shall construct such an element by the following algorithm starting from an element x of positive height.

α) In the reduced representation (3.4) for the element x we choose an index i, $0 \leqslant i \leqslant kn$, for which $a_i \not\equiv 0 \bmod p$.

β) If the congruence $\left(\frac{a_i}{a_j}\right)^{\sigma^{m+n}} \equiv \frac{a_j}{a_i} \bmod p$ is satisfied for all j, $1 < j < kn$, then we look for an element $\bar{a}_j \equiv \frac{a_j}{a_i} \bmod p$ such that $\bar{a}_j = a_j^{\sigma^{m+n}}$, and construct the element

$$z = F^{-1}\Big(\sum_{j=1}^{kn} \bar{a}_j x_j\Big).$$

Since the height H is positive, the element z belongs to M, because $z = F^{H-1}x + y$, $y \in M_0$. Further, $z \notin M_0$, because $\bar{a}_i \equiv 1 \bmod p$. Finally, it is easily seen that z is special. In this case the algorithm is completed with the construction of z.

γ) If there exists an index j, $1 \leqslant j \leqslant kn$, for which $\left(\frac{a_j}{a_i}\right)^{\sigma^{m+n}} \not\equiv \frac{a_j}{a_i} \bmod p$, then we consider instead of x the element $x' = (F^m - V^n)\frac{x}{a_i}$, write it out in the reduced representation, and apply α) to it, in case the height of x is positive. In the contrary case the algorithm fails completely.

We now show that with the help of this algorithm we are always able to construct a special element that is not contained in M_0, provided we start with an element of height $H \geqslant m(kn - 1) + 1$.

The transition from x to x' will be called a complete step of the algorithm, and the transition from x to z (when β) applies) an incomplete step.

First of all we note that after a complete step has been carried out, the F-height of x' is exactly m less than the height of x, because

$$x' = (F^m - V^n)\frac{x}{a_i} = \\ = F^{-H+m}\left\{\sum_{l=1}^{kn}\left(\frac{a_l}{a_i} - \left(\frac{a_l}{a_i}\right)^{\sigma^{-m-n}}\right)x_l + \sum_{j=1}^{km} c_j F y_j\right\}, \quad c_j \in W, \qquad (3.5)$$

and

$$\frac{a_j}{a_i} - \left(\frac{a_j}{a_i}\right)^{\sigma^{-m-n}} \not\equiv 0 \bmod p.$$

Further, denote by $\delta(x)$ the number of indices i in the reduced representation (3.4) for which $a_i \not\equiv 0 \bmod p$. If β) is not fulfilled, then $\delta(x) \geqslant 2$ and (3.5) is a reduced representation for x', because $\frac{a_j}{a_i} = \left(\frac{a_j}{a_i}\right)^{\sigma^{-m-n}} \not\equiv 0 \bmod p$. From (3.5) it is clear that after carrying out the complete step, $\delta(x)$ decreases by at least 1:

$$\delta(x') \leqslant \delta(x) - 1.$$

For if $a_l \equiv 0 \bmod p$, then $\frac{a_l}{a_i} - \left(\frac{a_l}{a_i}\right)^{\sigma^{-m-n}} \equiv 0 \bmod p$, and besides, the i-th coefficient comes to be zero.

Thus, since $1 \leqslant \delta(x) \leqslant kn$, after $s \leqslant kn - 1$ complete steps of the algorithm we reach an element $x^{(s)} \in M$ for which $a_i^{\sigma^{m+n}} \equiv a_i \bmod p$ or $\delta(x^{(s)}) = 1$. The height of $x^{(s)}$ is precisely sm less than the height of x and is therefore positive, provided we start with $H \geqslant m(kn - 1) + 1$. It follows that β) is fulfilled for $x^{(s)}$, and so we may apply a final incomplete step, giving us a special element not in M_0.

So we have obtained a contradiction, and this completes the proof.

2. We now pass to the proof of Theorem 3.5 in the general case. Let $M \sim \bigoplus_{i=1}^{s} k_i E/E(F^{m_i} - V^{n_i})$, and $M_0 \subset M$ its maximal special submodule. We may assume that

$$\frac{m_1}{n_1} > \frac{m_2}{n_2} > \ldots > \frac{m_s}{n_s}.$$

THEOREM 3.8. *There exists an integer*

$$H = H(k_1, m_1, n_1; \ldots; k_s, m_s, n_s),$$

such that $F^H M \subset M_0$. *More precisely, we may take for* H *the integer defined inductively in the following way: If* $s = 1$, *then* $H = m_1(k_1 n_1 - 1)$. *If* $s \geqslant 2$, *then*

$$H = \left[\frac{m_1}{n_1}\left(n_1 n_2 \ldots n_s + \frac{2(s-1)H' + 1}{\frac{m_1}{n_1} - \frac{m_s}{n_s}}\right)\right] + (s-1)H',$$

where $H' = \max H(k_{i_1}, m_{i_1}, n_{i_1}; \ldots; k_{i_r}, m_{i_r}, n_{i_r})$ *(the maximum being taken over all proper subsystems* $(i_1, \ldots, i_r) \in (1, \ldots, s)$*).*

PROOF. For $s = 1$ the result follows from the previous theorem, so let $s \geqslant 2$.

We put $M_0 = \bigoplus_i (M_{0i})_F$, where $M_{0i} \sim k_i E/E(F^{m_i} - V^{n_i})$. Since $(M)_F = \bigoplus_i (M_{0i})_F$, every element $x \in M$ can be uniquely represented in the form

$$x = \sum_{i=1}^{s} F^{-H_i} x_i, \tag{3.6}$$

where $x_i \in M_{0i} \setminus FM_{0i}$ or $x_i = 0$. If $x_i = 0$, we set $H_i = -\infty$. The height of x over M_0 is clearly equal to $\max H_i$.

With every element $x \in M$ we associate a collection of integers, consisting of all the positive numbers H_i ('partial height') defined by the decomposition (3.6) taken in order of magnitude with the right multiplicities. I claim that the difference between two successive numbers from this collection does not exceed H' (if the collection consists of a single number, we take this number as the difference).

For let $H_k - H_l > H'$, and put

$$x = x_1 + x_2, \qquad x_1 = \sum_{H_i \leqslant H_l} F^{-H_i} x_i, \qquad x_2 = \sum_{H_i \geqslant H_k} F^{-H_i} x_i.$$

Clearly the element $\sum_{H_i \geqslant H_k} F^{H_l - H_i} x_i = F^{H_l} x - F^{H_l} x_1$ belongs to the submodule $N = (\bigoplus_{H_i \geqslant H_k} M_{0i})_F \cap M$ and has height $> H'$ over $\bigoplus_{H_i \geqslant H_k} M_{0i}$. But this contradicts the definition of H', because the module $\bigoplus_{H_i \geqslant H_k} M_{0i}$ is the maximal special submodule of N.

We now note that if $x \in M_{0i} \setminus FM_{0i}$, then for any natural number R we have $V^{Rn_i} x_i \in F^{Rm_i} M_{0i} \setminus F^{Rm_i + 1} M_{0i}$. In particular, if $S = (H_1, \ldots, H_s)$ is the collection of numbers from the decomposition (3.6) for x, then the analogous collection for $V^{Rn_1 \ldots n_s} x$ will be

$$S^R = \left(H_1 - \frac{m_1}{n_1} Rn_1 \ldots n \quad \ldots, H_s - \frac{m_s}{n_s} Rn_1 \ldots n_s\right).$$

Let S_+^R be the positive part of this collection. If we start from an element x of height H, then in S the largest number is $H_{\max} = H$ and the smallest number is $H_{\min} \geqslant H - (s-1)H'$ (by the estimate obtained for the

difference between successive positive numbers H_i).

Hence in S^R the largest number is $\geqslant H - (s-1)H' - \frac{m_s}{n_s} Rn_1 \dots n_s$, and the smallest is $\leqslant H - \frac{m_1}{n_1} Rn_1 \dots n_s$. For the difference we obtain as a lower bound

$$\left(\frac{m_1}{n_1} - \frac{m_s}{n_s}\right) Rn_1 \dots n_s - (s-1)H';$$

subject to the condition that $H - (s-1)H' - \frac{m_1}{n_1} Rn_1 \dots n_s > 0$, the same estimate applies to the difference between the largest and smallest numbers in the collection $S_+^R = S^R$.

Now take R to be the least integer for which

$$\left(\frac{m_1}{n_1} - \frac{m_s}{n_s}\right) Rn_1 \dots n_s - (s-1)H' \geqslant (s-1)H' + 1. \tag{3.7}$$

If with this condition we still have

$$H - (s-1)H' - \frac{m_1}{n_1} Rn_1 \dots n_s > 0, \tag{3.8}$$

then we have a contradiction, because for the element $V^{Rn_1 \dots n_s} x$ the difference between the maximal and minimal positive heights H_i is $\geqslant (s-1)H' + 1$, and hence this is a difference between consecutive partial heights greater than H', and this, as we have seen, is impossible.

To ensure that (3.7) holds it is enough to put

$$R = \left[\frac{2(s-1)H' + 1}{\left(\frac{m_1}{n_1} - \frac{m_s}{n_s}\right) n_1 \dots n_s} + 1\right];$$

then (3.8) cannot also hold, and we obtain the following bound for H:

$$H \leqslant \frac{m_1}{n_1} Rn_1 \dots n_s + (s-1)H' \leqslant \left[\frac{m_1}{n_1}(n_1 n_2 \dots n_s) + \frac{2(s-1)H' + 1}{\frac{m_1}{n_1} - \frac{m_s}{n_s}}\right] + (s-1)H'.$$

Thus the theorem is established, and with it the proof of the second finiteness theorem is complete.

The remainder of this section is devoted to the problem of clarifying to what extent a similar result remains true for modules that are not equidimensional.

3. Let us call a module M *reductive* if it is isogenous to a direct sum of equidimensional modules and a finite number of modules of the form E/EV (corresponding to additive formal groups).

Let M be a reductive module. By a generalized maximal special submodule we understand a submodule M_0 of M generated by the maximal special submodule M_0' in the usual sense and a maximal submodule M_0'' satisfying the condition $VM_0'' = 0$.

LEMMA 3.12. 1) $M_0 = M_0' \oplus M_0''$.

2) $M_0'' \approx kE/VE$.

3) M_0 *is a dense submodule of* M.

PROOF. 1) We have $M_0 = M_0' + M_0''$ by definition and $M_0' \cap M_0'' = 0$.

2) Clearly M_0'' is isogenous to kE/VE (this follows from the

classification theorem up to isogeny). There exists a chain of finite length of the form $M_0'' \supset M_1 \supset M_2 \supset \ldots \supset M_{s-1} \supset M_s$, where $M_s \approx kE/VE$, long $M_i/M_{i+1} = 1$. We shall show that in such a chain $M_{s-1} \approx M_s$. The required result follows from this. Thus, let $M_{s-1} = M_s + Ex$, $M_s = \bigoplus_{i=1}^{k} Ex_i$, $Vx_i = 0$. Then

$$Fx = \sum_{i=1}^{k} \Big(\sum_{j=0}^{\infty} e_{ij} F^j \Big) x_i, \qquad e_{ij} \in W,$$

and for at least one value of i we have $e_{i0} \not\equiv 0 \bmod p$. I claim that $M_{s-1} = Ex_1 \oplus \ldots \oplus Ex_{i-1} \oplus Ex \oplus Ex_{i+1} \oplus \ldots \oplus Ex_k$. The verification consists in establishing equality with the direct sum replaced by an ordinary sum, but this is obvious, because x_i may be expressed by x and $\{x_j\}$, $j \neq i$.

3) In any case M contains a dense submodule isomorphic to $M_0' \oplus kE/EV$. Since M_0 contains this submodule, M_0 is also dense.

THEOREM 3.9. *Let M be a reductive module and M_0 its generalized maximal special submodule. Then there exists a constant H, depending only on the isogeny classes of the equidimensional components of M, such that $F^H M \subset M_0$. In the notation of Theorem 3.8 we may set* $H = H(\ldots;\ k_i,\ m_i,\ n_i;\ \ldots) + \max m_i$.

PROOF. Let

$$x = F^{-H_1} x' + F^{-H_2} x'',$$
$$x' \in (M_0' \setminus FM_0') \cup \{0\}, \qquad x'' \in (M_0'' \setminus FM_0'') \cup \{0\}.$$

If $x' = 0$, then $H_2 \leqslant 0$ by the definition of M_0''.

If $x' \neq 0$, but $x'' = 0$, then $H_1 \leqslant H(\ldots;\ k_i,\ m_i,\ n_i;\ \ldots)$ by Theorem 3.8.

If $x' \neq 0$ and $x'' \neq 0$, then in the first place $H_2 \leqslant H_1$, because otherwise the element $F^{H_1} x - x'$ does not belong to M_0'', which contradicts the equation $V(F^{H_1} x - x') = 0$.

Further, $Vx = F^{-H_1} Vx'$, and as is easily seen, the height of Vx' over the equidimensional part is less than the height of x' by at most $\max m_i$. Hence by the preceding theorem, $H_1 - \max m_i \leqslant H(\ldots;\ k_i,\ m_i,\ n_i;\ \ldots)$.

Thus the theorem is proved.

4. The last form of the second finiteness theorem is of interest in that, combined with the first finiteness theorem, it may be used to give a much stronger result, which turns out to be characteristic for reductive modules.

We shall say that a class of isogenous modules has the H-property if there exists a constant $H > 0$ such that for any two (reductive) modules of the given class there exists an isogeny (embedding) $M_1 \subset M_2$ such that long $M_1/M_2 < H$.

THEOREM 3.10. *An isogeny class of modules possesses the H-property if and only if it consists of reductive modules.*

PROOF. We show first that every class of reductive modules has the H-property. Let M_1 be any module of the given class. Its height over its generalized maximal special submodule M_0 is bounded by a constant h

depending only on the class. We may embed all non-isomorphic generalized special modules of the given class in M_0. Since the number of these modules is finite, the height of M_0 over each of these modules does not exceed a certain constant h_1 depending only on the class. Conversely, M_2 may be embedded in a special module whose height over M_2 is bounded by h (e.g. $M_2 \subset F^{-h}M_0'$, where M_0' is the generalized maximal special submodule of M_2). We embed this special module in turn in M_1 so that the height of M_1 over it is $\leqslant h_1$. Thus we obtain the required result.

Now we show that, conversely, any class possessing the H-property consists of reductive modules.

For this purpose we shall, in any class of non-reductive modules, effectively construct pairs of modules for which the least height for the embeddings exceeds all bounds.

Any non-reductive module M is isogenous to a direct sum of the form $M \sim M_1 \oplus \bigoplus_i k_i E/EV^{r_i}$, where M_1 is equidimensional and $\max r_i \geqslant 2$. For any $i \geqslant 0$ and any M we denote by $M_{(i)}$ the submodule of M consisting of all elements $x \in M$ such that $V^i x = 0$. It is easily seen that if $M' \sim M''$, then $M'_{(i)} \sim M''_{(i)}$ for all i; if M' is a dense submodule of M'', then $M'_{(i)}$ is a dense submodule of $M''_{(i)}$. Further, the height of M'' over M' in this case is not less than the height of $M''_{(i)}$ over $M'_{(i)}$.

For any integer $h \geqslant 0$ consider the module $M(h) = Ex_0 + Ex_1$, where $V^2x_0 = 0$, $Vx_0 = F^h x_1$. It is easy to see that $M(h) \sim E/EV^2$. In every isogeny class of non-reductive modules there exist modules M', M'' such that

$$M'_{(2)} \approx kE/EV^2 + lE/EV, \qquad M''_2 \approx kM(h) + lE/EV$$

(the numbers k and l are defined by the class, while h may be chosen arbitrarily). The theorem will follow if we show that for any embedding $M'_{(2)} \subset M''_{(2)}$ the height of the bigger over the smaller module is $\geqslant h$.

For brevity let us write M' instead of $M'_{(2)}$ and M'' instead of $M''_{(2)}$.

Let $M' \subset M''$ be an arbitrary embedding. By definition the module M'' contains an element x of height h over VM'' (i.e. $F^h x \in VM''$, $F^{h-1}x \notin VM''$). let us show that the height of x over M' is not less than h. Indeed, otherwise $F^{h-1}x \in M'$ and $V(F^{h-1}x) = F^{h-1}Vx = 0$. Now if $y \in M'$ and $Vy = 0$, then $y \in VM'$, hence $F^{h-1}x \in VM'$, which is impossible, because $F^{h-1}x \notin VM''$.

This contradiction completes the proof of the theorem.

§7. Cyclic isosimple modules; the component of maximal dimension

1. In the remaining parts of this chapter we shall calculate the module space in certain special cases. In particular, in this section we shall describe the component of maximal dimension of the space of cyclic isosimple modules.

Let $M \subset W(k) \otimes E_{n,m}$ be a cyclic E-module subject to the condition $0 \in J = \{ \nu(x) \mid x \in M \}$. By Lemma 3.9 such a module is generated over E by an element of the form

$$z = 1 + \sum_{k \in \bar{J}} \varepsilon_k \theta^k, \qquad \bar{J} = Z_+ \setminus J, \qquad \varepsilon_k = \varepsilon_k(M),$$

whose coefficients $\varepsilon_k(M)$ are uniquely determined by M. Consider the mapping φ of the set of modules of the form just described into the affine space $\underline{A}^s$ over the field k that associates with M the point $(\bar{\varepsilon}_k(M))$, $k \in \bar{J}$, $\varepsilon_k = \varepsilon_k \bmod p$. By Lemma 3.8 the dimension s of this space is $\frac{1}{2}(m-1)(n-1)$.

2. THEOREM 3.11. a) *The mapping φ establishes a one-to-one correspondence between the points of a certain dense constructive subset of A^s and the cyclic modules $M \subset W(k) \otimes E_{n,m}$ belonging to the special submodule $M_0 = W(k) \otimes E_{n,m}\theta^{(m-1)(n-1)}$.*

b) *The index of any such module M over M_0 is of the form*

$$e = (e_i) = \left(\frac{b_i - a_i}{m+n}\right) \qquad (i = 1, \ldots, m+n). \tag{3.9}$$

Here (a_i) is a permutation of the numbers $(0, m, 2m, \ldots, (n-1)m;$ $n, 2n, \ldots, mn)$ and (b_i) is a permutation of the numbers $((m-1)(n-1),$ $(m-1)(n-1)+1, \ldots, mn)$. These permutations are defined by the conditions

$$a_i = b_i \mod (m+n), \qquad a_i - b_i \leqslant a_{i+1} - b_{i+1}.$$

c) *The mapping φ is an isomorphism of the algebraic structure of the constructive subset of the space $A(M_0, H)$ corresponding to the index (3.9) and the number of E-generators of the identity, on the dense subset of A^s described in* a).

PROOF. a) Let us show first that the image Y of the set of cyclic modules M belonging to M_0, under the mapping φ, is constructive in A^s. Thus, consider the mapping

$$\psi\colon E/m^h \times A^s \longrightarrow p^{-h}M_0/M_0; \qquad m = EF + EV \subset E, \qquad h \geqslant 1, \tag{3.10}$$

that associates with the pair $(\underline{a} \bmod m^h, \varepsilon)$, where $a \in E$, $\varepsilon = (\bar{\varepsilon}_{k_1}, \ldots, \bar{\varepsilon}_{k_s}) \in A^s$, $k_i \in \bar{J}$, the element $a(1 + \sum_{k \in \bar{J}} \varepsilon_k \theta^k) \bmod M_0$. For this to be a correct definition it is necessary to choose h so as to satisfy the inequality $\min(mi + nj) \geqslant (m-1)(n-1)$. In this case the class of elements $a(1 + \sum_{k \in \bar{J}} \varepsilon_k \theta^k) \bmod M_0$ depends only on the class of $a \bmod m^h$ and the image of this element automatically lies in $p^{-h}M_0$.

The mapping ψ is a morphism of the canonical quasi-algebraic structure on the sets (3.10). (E/m^h is an artinian local ring with residue class field k, and M_0 may be considered as $W(k)$-module.) For any element $z \in p^{-h}M_0$ the set Y_z of all points of the space A^s for which the corresponding module contains z coincides with the projection on A^s of the closed set $\psi^{-1}(z) \in E/m^h \times A^s$. This projection is constructive in A^s. By definition $Y = A^s \setminus \bigcup_z Y_z$, where the union is taken for all special elements $z \in p^{-h}M_0 \setminus M_0$. Hence the set Y is also constructive. (Thus, the union considered above may be regarded as consisting of only a finite number of sets, because Y_z depends only on the class of $z \bmod M_0$.)

It remains to show that the set Y is dense in A^s, i.e. that it contains an open subset. For this purpose it is enough to show that for any special element $z \in p^{-h}M_0 \setminus M_0$ the set $A^s \setminus Y_z$ contains an open subset of A^s.

Let $z \in W(k) \otimes E_{n,m}$ be a special element, $\nu(z) \in J = \{am + bn\}$. We

may confine ourselves to considering such elements, for if $\nu(z) < 0$ or $\nu(z) \in \overline{J}$, then Y_z is empty. The condition $z \notin M_0$ signifies that $\nu(z) = 1 < (m-1)(n-1)$. We may assume that $m < n$. Let us show that Y_z is contained in a certain proper closed subset of A^s.

Since $1 < (m-1)(n-1)$ and $l \in J = \{am + bn\}$, there exists an integer i, $1 \leqslant i \leqslant m-1$, such that $l + i \in \overline{J}$ (otherwise J would contain an interval of m consecutive integers starting with l, and hence all integers $\geqslant l$ would belong to J; but this is impossible by Lemma 3.8). We choose the least i with this property.

Let $\bar{\varepsilon}_k \equiv \varepsilon_k \bmod p \in k$; suppose that we have the inclusion $\varepsilon = (\bar{\varepsilon}_k)_{k \in \overline{J}} \in Y_z$. This means that for a certain element $a = \sum_{j = cm+dn < (m-1)(n-1)} \lambda_j V^c F^d \in E$, $\lambda_j \in T$, and the special element $z = \sum_{j \geqslant l} \eta_j \theta^j$ we have the equality

$$a\left(1 + \sum_{k \in \overline{J}} \varepsilon_k \theta^k\right) = \sum_{l \leqslant j = cm+dn < (m-1)(n-1)} \lambda_j \theta^j + \sum_{j \geqslant l} \sum_{k \in \overline{J}} \lambda_j \varepsilon_k^{\sigma_j} \theta^{j+k} \equiv$$

$$\equiv \sum \eta_j \theta^j \mod W \otimes E_{n,m} \theta^{l+i+1}. \qquad (3.11)$$

(Here $\sigma_j = \sigma^{md-cn}$ if $j = cm + dn$; $c, d \geqslant 0$.) Since $l, l+1, \ldots, l+i-1 \in J$, it is not hard to see that for a fixed z and ε the coefficients $\lambda_l, \lambda_{l+1}, \ldots, \lambda_{l+i-1}$ are defined by this equation uniquely as functions of $\varepsilon_1, \ldots, \varepsilon_{i-1}$ and η_j. (We obtain a diagonal system of equations for the λ_k.) In particular, $\lambda_l = \eta_l \neq 0$, since $\varepsilon_0 = 1$. Now $l + i \notin J$ and moreover, $1, 2, \ldots, i \notin J$. Therefore, by comparing the coefficients of θ^{l+i} on the right and left-hand sides of (3.11) we find that (3.12)

$$\bar{\eta}_{l+1} = \bar{\lambda}_l \bar{\varepsilon}_i^{\sigma_l} + f(\bar{\lambda}_l, \ldots, \bar{\lambda}_{l+i-1}; \bar{\varepsilon}_1, \ldots, \bar{\varepsilon}_{i-1}) = \bar{\eta}_l \bar{\varepsilon}_i^{\sigma_l} + g(\bar{\varepsilon}_1, \ldots, \bar{\varepsilon}_{i-1}). \quad (3.12)$$

The condition (3.12) for fixed z represents an imposition of non-trivial relations (because $\bar{\eta}_l \neq 0$) on the coordinates $\bar{\varepsilon}_1, \ldots, \bar{\varepsilon}_i$ of ε in the space A^s. These relations are clearly algebraic. Therefore, the set Y_z in every case is contained in a proper closed subset of A^s. This completes the proof of the first statement of the theorem.

b) Let $M \subset W(k) \otimes E_{n,m}$ be any E-module. Since it is dense, its rank over $W(k)$ is $m + n$. We shall show that any collection of elements $z_1, \ldots, z_k \in M$ for which $\nu(z_i) \neq \nu(z_j)$ when $i \neq j$ and

$$\{\nu(z_i)\}_{i=1,\ldots,k} = J \setminus (J + m + n), \qquad J = \{\nu(x) \mid x \in M\},$$

constitutes a $W(k)$-basis for M. It is clear that the set of indices of the W-module generated by $z_1, \ldots, z_k$ coincides with J and that this W-module is contained in M. Hence it follows that it coincides with M. It remains to verify that $k = m + n$. Indeed, the set $J \setminus (J + m + n)$ can be obtained as follows. We write out the elements of J in increasing order and cross out those that are congruent mod $(m + n)$ to an element written down before. Since J contains all integers beginning with a given one, the numbers that remain form a complete set of residues mod $(m + n)$, so that $k = m + n$.

In the notation of the theorem for the module M we have

$$J \setminus (J + m + n) = (a_i).$$

Hence we may take as a $W(k)$-basis of M any collection of elements $z_i \in M$

such that $\nu(z_i) = a_i$. Then

$$\nu(p^e i z_i) = (m+n)\, e_i + a_i = b_i.$$

In addition, $p^e i z_i \in M_0$, because $b_i \geqslant (m-1)(n-1)$. Since (b_i) coincides with $J_0 \setminus (J_0 + m - n)$, where $J_0 = \{\nu(x) \mid x \in M_0\}$, the elements $p^e i z_i \in M_0$ constitute a W-basis for M_0. This proves the second statement.

c) The functions ε_k are single-valued onto the corresponding subset of $A(\underline{M}_0, H)$; also M is uniquely determined at the point $(\varepsilon_k)_{k \in \overline{J}}$. The fact that ε_k is algebraic is trivial to verify. Hence this statement is also established.

The proof of the theorem is now complete.

Its value lies in the fact that it enables us to construct explicitly an algebraic system of isosimple modules of type (m, n), with the property that any one of the modules in the system is contained in only a finite number of isomorphic modules (the number being bounded by a constant depending on p, m and n). The dimension of this system is $\frac{1}{2}(m-1)(n-1)$, and this is the best possible value for the cyclic isosimple module of type (m, n). It seems plausible that the last assertion remains true for any modules, not necessarily cyclic, of a given type.

§8. Classification of two-dimensional modules

1. In this section we shall show that by specializing the general theory developed above we shall obtain a complete classification of two-dimensional modules (up to automorphisms of the maximal special submodule in the equidimensional case).

We begin with modules isogenous to $E/E(F^{2m+1} - V^2)$. In Example 2 of §5, 4. we described all special modules of a given class. They were enumerated by sets J_i for which there are $m+1$ possibilities

$$J_i = \{2a + (2m+1)\, l\} \cup \{2i + 1 + 2a + (2m+1)\, b\}.$$

Any submodule $M \subset W(k) \otimes E_{2,\,2m+1}$ satisfying the conditions of §5, 2. and corresponding to the set j_i has by Lemma 3.9 two standard generators:

$$z_1 = 1 + \sum_{k=1}^{i} \varepsilon_{2k-1} \theta^{2i-1}, \qquad z_2 = \theta^{2i+1}. \tag{3.13}$$

Let us define a number j, $0 \leqslant j \leqslant i$, by the conditions

$$\left.\begin{aligned} &\varepsilon_{2k-1} \in W(k_{m+n}), \quad k \leqslant i-j, \\ &\varepsilon_{2(i-j)+1} \notin W(k_{m+n}). \end{aligned}\right\} \tag{3.14}$$

Then we have the following assertion.

THEOREM 3.12. a) *The numbers i and j coincide for isomorphic E-modules.*

b) *For fixed i and j the module M belongs to the special submodule*

$$EF^j z_1 + Ez_2 \approx E \cdot 1 + E\theta^{2(i-j)+1} = M_{0,\,m-i+j}$$

and its index over this submodule is

$$e_j = (0, \ldots, 0, \underbrace{1, \ldots, 1}).$$

c) *The space of submodules M^j belonging to a fixed special submodule $M_{0,m-1+j}$ and of index e_j over it has dimension j and is isomorphic to the complement of the union of p^{2m+3} parallel hyperplanes*

$$\bar{\varepsilon}_1 = a, \quad a \in k_{2m+3},$$

in the space $A^s = (\bar{\varepsilon}_k)$, after factoring out the finite group of automorphisms obtained by identifying isomorphic modules. In particular, this group acts on an affine variety, and therefore the factor-space exists and is an affine variety.

PROOF. a) The number i is defined invariantly, because it gives the type of the maximal special submodule. The invariance of j follows from the fact, which will be shown below, that it defines the index e_j of the module over its maximal special submodule.

b) Let i and j be fixed. Consider the module M generated by the standard basis z_1, z_2 (cf. (3.13)). Since $F^j z_1$ is congruent to the special element z_1' mod $W \otimes E_{2,2m+1}\theta^{2i+1}$ and $W \otimes E_{2,2m+1}\theta^{2i+1} \subset M$, it follows that the submodule

$$EF^j z_1 + Ez_2 \subset M$$

is special. To prove that it is maximal it is enough to verify that M contains no special element z of index $\nu(z) = 21 < 2j$. Indeed, such a special element would be congruent mod Ez_2 to an element of the form $(\sum_{k=l}^{i} \lambda_k F^k) z_1$, and an argument similar to that which was used in the proof of (3.8) shows that in this case the coefficient $\bar{\varepsilon}_{2(i-j)+1}$ may be expressed in terms of the $\bar{\varepsilon}_k$, $k < 2(i-j)+1$, and the coefficients of a special element z by means of certain universal formulae over the prime field. This however is impossible, because

$$\bar{\varepsilon}_{2(i-j)+1} \notin k_{2m+3}.$$

The module $EF^j z_1 + Ez_2$ coincides with $Ez_1' + Ez_2$, where z_1' is a certain standard element, $\nu(z_1') = 2j$. Hence it is isomorphic to $E\theta^{2j} + E\theta^{2i+1}$: the required isomorphism is now obtained by multiplying the last module on the right by a unit that maps θ^{2j} to z_1' (in the algebra $E_{2,2m+1}$).

Since $pM \subset M_0$ (because $\nu(p) = 2m+3$), the index of M over M_0 consists of zeros and ones. The number of ones is exactly equal to j, because the linear space over kM/M_0 is generated by the linearly independent images of elements with the exponents $0, 2, \ldots, 2j-2$.

c) The last assertion has in fact already been established. Consider the module space parametrized by the residues mod p of the coefficients

$$(\varepsilon_{2(i-j)+1}, \varepsilon_{2(i-j)+3}, \ldots, \varepsilon_{2i-1}), \quad \varepsilon_k \in W(k), \quad \varepsilon_{2(i-j)+1} \notin W(k_{2m+3})$$

of the standard element z_1. For Γ we may take the finite group

$$E_{2,2m+1}^*/(1 + \theta^{2m} E_{2,2m+1})^*$$

It only remains to note that by multiplying the standard generator on the right by a suitable unit, we can always arrange it so that the coefficients

ε_{2k-1}, $1 \leqslant k \leqslant i-j$, become zero. Therefore different choices of these coefficients do not give rise to further invariants of the system.

EXAMPLE. We shall carry out the calculations completely in the case $m = 1$. We have two special modules: $E.1$ and $E.1 + E.\theta$. To the first of these there belongs no module other than itself; to the second there belongs the algebraic system of modules $E(1 + \varepsilon\theta)$, $\varepsilon \in T$, $\varepsilon \notin W(k_5)$. Put $x_\varepsilon = 1 + \varepsilon\theta$. The modules Ex_ε and Ex_η are isomorphic if and only if for some element $\alpha \in E_{2,3}$ we have $Ex_\varepsilon\alpha = Ex_\eta$. Let

$$\alpha \equiv \alpha_0 + \alpha_1\theta \bmod \theta^2; \qquad \alpha_0, \alpha_1 \in W(k_5) \cap T, \qquad \alpha_0 \neq 0.$$

Then we have

$$x_\varepsilon\alpha \equiv (1 + \varepsilon\theta)(\alpha_0 + \alpha_1\theta) \equiv \alpha_0 + (\varepsilon\alpha_0^{\sigma 3} + \alpha_1)\theta \mod \theta^2$$

and hence

$$Ex_\varepsilon\alpha = E(1 + (\varepsilon\alpha_0^{\sigma 3-1} + \alpha_1\alpha_0^{-\sigma 3})\theta).$$

Thus $Ex_\varepsilon \approx Ex_\eta$ if and only if, for some β_0, $\beta_1 \in k_5$, we have

$$\bar{\eta} = \beta_0^{p^3-1}\bar{\varepsilon} + \beta_1, \qquad \beta_0 \neq 0. \tag{3.15}$$

The factor-space with respect to this group of automorphisms of a line over k, with the points whose coordinates belong to k_5 deleted, can be described explicitly: the mapping

$$\bar{\varepsilon} \longrightarrow (\bar{\varepsilon}^{p^5} - \bar{\varepsilon})^{\frac{p^5-1}{\delta}}, \qquad \delta = (p^5 - 1,\ p^3 - 1)$$

defines an isomorphism of this factor-space with the multiplicative group of k. I do not know whether the existence of a group structure on the module space is accidental or whether it has an invariant significance.

This example was analyzed by Dieudonné [30] by means of somewhat cumbersome calculations. Dieudonné only showed the necessity of the conditions (3.15) for a module isomorphism, and besides, in the paper [30] it is not mentioned that the systems considered exhaust all modules isogenous to $E/E(F^3 - V^2)$.

2. THEOREM 3.13. *Any module isogenous to E/EV^2 is isomorphic to one of the modules $M(h)$ constructed in the proof of Theorem* 3.10:

$$M(h) = Ex_0 + Ex_1, \quad V^2x_0 = 0, \quad Vx_0 = F^h x_1 \qquad (h = 0,\ 1,\ 2,\ \ldots).$$

For distinct values of h the modules $M(h)$ are non-isomorphic.

PROOF. Let $M \sim E/EV^2$ *and take h to be the least integer for which* $F^h M_{(1)} \subset VM$, where $M_{(1)} = \{x \in M \mid Vx = 0\}$. Such a number always exists, because $M_F \approx E_F z_0 + E_F V z_0$, where $V^2 z_0 = 0$, so that $(M_{(1)})_F = (VM)_F$.

Since $VM \approx E/EV$, the module VM is cyclic. Let $F^h x_1$ (where $x_1 \in M_{(1)}$) be its generator and let $x_0 \in M$ be an element such that $Vx_0 = F^h x_1$. Then $M = Ex_0 + Ex_1$, because

$$M_{(1)} = (Ex_0 + Ex_1)_{(1)} \quad \text{and} \quad M/M_{(1)} = (Ex_0 + Ex_1)/M_{(1)}.$$

Indeed, the first equation is clear. If the second equation did not hold, then there would be an element $x \in M$, $x \equiv F^{-k}x_0 \bmod M_{(1)}$, $k \geqslant 1$, but then

$$Vx = F^{-k}Vx_0 \in VM \text{ and } F^{h-k}x_1 = F^{-k}Vx_0 \in VM,$$

which contradicts the minimality of h.

Thus the theorem is established.

3. Let us summarize our results on the classification of indecomposable two-dimensional modules.

a) Class $E/E(F^{2m+1} - V^2)$, $m < \infty$. There are $m + 1$ non-isomorphic special modules

$$M_h^{(m)} = E \cdot 1 + E \cdot \theta^{2(m-h)+1}, \qquad 0 \leqslant h \leqslant m.$$

The modules belonging to $M_h^{(m)}$ are distributed over $h + 1$ components, corresponding to the index e_k, $0 \leqslant k \leqslant h$. The dimension of the component with index e_k is k.

b) The class E/EV^2, $m = \infty$. The modules in this class fall into a countable set of zero-dimensional components $M(h)$.

The module E/EV^2 is in a certain sense a limit of the modules $E/E(V^2 - F^{2m+1})$ for $m \to \infty$. The space of modules isogenous to E/EV^2 also turns out to be the 'limit' (!) of the sequence of module spaces isogenous to $E/E(V^2 - F^{2m+1})$, leaving only the 'special' modules, and the continuous components are annihilated by a large group of automorphisms.

4. We now turn to modules that are decomposable up to isogeny. Let us begin with modules isogenous to $E/E(F^{m_1} - V) \oplus E/E(F^{m_2} - V)$, where $m_1 \neq m_2$. We may assume that $m_1 < m_2$. Suppose first that $m_1, m_2 \neq \infty$ (and $m_1, m_2 \neq 0$, because a module with $m_1 m_2 = 0$ is decomposable and therefore uniquely defined by its class).

For every pair (m_1, m_2) with these properties there exists a unique special module in the given class (cf. §5, Example 1):

$$M_0 = E/E(F^{m_1} - V) \oplus E/E(F^{m_2} - V).$$

We shall use the representation

$$M_0 = W(k) \otimes E_{1, m_1} \oplus W(k) \otimes E_{1, m_2} = M_{01} \oplus M_{02}$$

and we shall consider modules M containing M_0 and contained in

$$M_{0F} = W(k) \otimes K_{1, m_1} \oplus W(k) \otimes K_{1, m_2}.$$

Any module isogenous to M_0 is isomorphic to one of these modules. We shall keep the notation introduced in §4; the element θ in E_{1, m_1} will be denoted by θ_1 and in the algebra E_{2, m_2} by θ_2. By height we shall always mean F-height.

LEMMA 3.13. a) *Let M be an E-module such that $M_{0F} \supset M \supset M_0$. If M belongs to M_0, then the height of M over M_0 does not exceed* $m_1 = \min(m_1, m_2)$.

b) *Let M belong to M_0, and let the height of M over M_0 be h. The factor module M/M_0 is cyclic; as a generator we can take the image of an element of the form*

$$z = 0_1^{-h} + \sum_{i=1}^{h} \varepsilon_i 0_2^{-i}, \quad \varepsilon_i \in T, \qquad \varepsilon_h \neq 0, \tag{3.16}$$

and this element is uniquely determined by M.

c) *For any h, $1 \leqslant h \leqslant m_1$, and any set $(\varepsilon_1, \ldots, \varepsilon_h)$ of elements $\varepsilon_i \in T$ such that $\varepsilon_h \neq 0$, the module $Ez + M_0$, where z is defined by* (3.16), *belongs to the special submodule M_0 and its index over M_0 is* $(0, \ldots, 0, \underbrace{1, \ldots, 1}_{h})$.

PROOF. a) Let

$$x = F^{-h_1}x_1 + F^{-h_2}x_2 \in M;\ x_1 \in M_{01} \setminus FM_{01} \cup \{0\};\quad x_2 \in M_{02} \setminus FM_{02} \cup \{0\}.$$

We may assume that $M = M_0$, $x \neq 0$ and $h_1 > 0$, $h_2 > 0$. Then $x_2 \neq 0$, for otherwise $EF^{-h_1}x_1$ would be a special submodule of M not contained in M_0, which is impossible, because M_0 is maximal. Similarly $x_1 \neq 0$. Further, $h_1 = h_2 = h$; for if $h_1 > h_2$, then the element

$$F^{h_2}x - x_2 = F^{-h_1+h_2}x_1 \in M$$

generates a special submodule not contained in M_0. Similarly we obtain a contradiction in the case where $h_1 < h_2$. Finally, $h \leqslant m_1$. For if $h > m_1$, then there exists an integer $g \geqslant 0$ for which $m_2 \geqslant h - g > m_1$, and then the element

$$VF^g x = x' + x'', \qquad x' \in (M_{01})_F, \qquad x'' \in (M_{02})_F,$$

is such that $x'' \in M_{02}$, but $x' \in M_{01}$. Therefore $x' \in M$ generates a special submodule, which is impossible because $x' \in M_0$.

b) Consider an element of maximal height in M. By the result of a) this may be taken in the form

$$z = F^{-h}(x_1 + x_2) = \sum_{i=1}^{h} \varepsilon_i \theta_1^{-i} + \sum_{i=1}^{h} \eta_i \theta_2^{-i} + x_0, \qquad \varepsilon_i,\ \eta_i \in T,\ \varepsilon_h \eta_h \neq 0, \qquad x_0 \in M_0. \tag{3.17}$$

We may assume that $\varepsilon_h = 1$. Let $k = k(z) \leqslant h - 1$ be the least integer for which in the representation (3.17), $\varepsilon_{k-1} = \ldots = \varepsilon_k = 0$, $\varepsilon_{k-1} \neq 0$. Consider the element $z' = z - \varepsilon_{k-1}F^{h-k+1}z$ and write it in the form (3.17). For this element it is clear that $k(z') \leqslant k(z) - 1$. Continuing in this way, we obtain after at most $h - 1$ steps an element of the form (3.16).

Now suppose that there is already an element of the form (3.16) in the module, say

$$z' = \theta_1^{-h} + \sum_{i=1}^{h} \varepsilon_i' \theta_2^{-i}.$$

If $z' \neq z$, then there exists an integer k such that $h \geqslant k \geqslant 1$ and $\varepsilon_i = \varepsilon_i'$ for $i > k$, $\varepsilon_k \neq \varepsilon_k'$. Then

$$(\varepsilon_k - \varepsilon_k')^{-1} F^{h-1}(z - z') = \theta_2^{-1} + z_0, \qquad z_0 \in M_0,$$

and θ_2^{-1} is a special element of M not contained in M_0. This contradiction shows that $z = z'$.

Let $x \in M$ be any element; we shall show that $x \in Ez + M_0$. This is true for elements of height $\leqslant 0$. Assume that it has already been established for elements of height $k - 1$, $1 \leqslant k \leqslant h$; we shall then prove it for elements of height k. We have

$$x = \varepsilon\theta_1^{-k} + \eta\theta_2^{-k} + x', \qquad F^{k-1}x' \in M_0.$$

I claim that the element $x - \varepsilon F^{h-k}z$ has height $\leqslant k - 1$. Indeed,

$$x - \varepsilon F^{h-k}z = (\eta - \varepsilon\eta_h^{\sigma^{h-k}})\,\theta_2^{-k} + x'', \quad F^{k-1}x'' \in M_0,$$

but then $\eta - \varepsilon\eta_h^{\sigma^{h-k}} = 0$, for otherwise the element $x - \varepsilon F^{h-k}z$ would be of the form $F^{-h_1}x_1 + F^{-h_2}x_2$ with $h_1 = h_2$, which is impossible. The result

follows by induction.

c) We have to show that $M = Ez + M_0$ contains no special elements of height $\geqslant 1$, when z is defined by (3.16). Clearly, since $Vz \in M_0$, $F^h z \in M_0$, any element of M is congruent mod M_0 to an element of the form $x = (\sum_{i=0}^{h-1} \lambda_i F^i) z$, $\lambda_i \in T$. Let $\lambda_0 = \ldots = \lambda_{k-1} = 0$, $\lambda_k \neq 0$. Then

$$x \equiv \lambda_k \theta_1^{-h+k} + \lambda_k \varepsilon_h^{\sigma^k} \theta_2^{-h+k} \mod F^{-h+k+1} M_0,$$

and the element x can be special only in the case when $\lambda_k = 0$ or $\varepsilon_h = 0$, neither of which is true.

Thus, we see that $M = Ez + M_0$ belongs to M_0; since $pM \subset M_0$, the index of M over M_0 consists of zeros and ones only; the number of ones is equal to the dimension h of the space M/M_0 generated by the linearly independent images of z, Fz, ..., $F^{h-1}z$. This completes the proof of the lemma.

THEOREM 3.14. *The equidimensional Dieudonné modules isogenous to a module of the form* $E/E(F^{m_1} - V) \oplus E/E(F^{m_2} - V)$ *split into* $m_1 + 1$ *components* A_h, $0 \leqslant h \leqslant m_1$. *The component* A_h *consists of modules having a maximal special submodule of index* $(0, \ldots, 0, \underbrace{1, \ldots, 1}_{h})$ *and is isomorphic to the space of orbits of a certain finite group* Γ_h *acting on an* h*-dimensional affine space with certain hyperplanes deleted.*

PROOF. Essentially everything has already been proved; the space on which Γ_h acts is parametrized by the residues of $(\varepsilon_1, \ldots, \varepsilon_h)$ mod p of the coefficients of (3.16) subject to the condition $\varepsilon_h \neq 0$. For Γ_h we can take the group

$$E^*_{1, m_1}/(1 + \theta_1^h E_{1, m_1})^* \times E^*_{1, m_2}/(1 + \theta_2^h E_{1, m_2})^*.$$

5. Consider now the class of equidimensional modules isogenous to $M_0 = 2E/E(F^m - V)$, $m \geqslant 1$. We shall continue with the notation introduced in the previous point before the statement of Lemma 3.13, for the case $m_1 = m_2 = m$; a result analogous to Lemma 3.13 applies here, but with certain changes.

Let us call a submodule M, where $M_{0F} \supset M \supset M_0$, *primitive* if it does not contain θ_1^{-1} and θ_2^{-1}. Any module isogenous to M_0 is isomorphic to a primitive submodule of M_{0F}: for clearly, $E\theta_1^{-1} + M_{01} \approx M_{01}$ and $E\theta_2^{-1} + M_{02} \approx M_{02}$. Hence it is enough to consider primitive submodules.

LEMMA 3.14. a) *Any primitive submodule is isomorphic to a primitive submodule whose height does not exceed* m.

b) *A primitive submodule* M *of height* $h \leqslant m$ *has the following properties: the factor-module* M/M_0 *is cyclic, a generator being given by the image of an element of the form*

$$z = \theta_1^{-h} + \sum_{i=1}^{h} \varepsilon_i \theta_2^{-i}, \qquad \varepsilon_i \in T, \qquad \varepsilon_h \neq 0, \tag{3.18}$$

and such an element is uniquely determined by M.

PROOF. a) Just as in the proof of Lemma 3.13 a), it can be shown that any element of a primitive module M not contained in M_0 is of the form

$$x = \sum_{i=1}^{h} \varepsilon_i \theta_1^{-i} + \sum_{i=1}^{h} \eta_i \theta_2^{-i} + x_0, \qquad \eta_i,\ \varepsilon_i \in T, \qquad \varepsilon_h \eta_h = 0, \qquad x_0 \in M_0. \quad (3.19)$$

Now assume that among all the modules $M' \supset M_0$ isomorphic to M, M itself has the following property: the length of M/M_0 is minimal. In this case we shall call M a *minimal* module. Let us show that then $h \leqslant m$. Thus, assume that $h > m$; we may also assume that $\varepsilon_h = 1$. If $\eta_1 \notin W(k_{m+1})$, then the element $(V - F^m)x \in M$, represented in the form (3.19):

$$(V - F^m)x = \sum_{i=1}^{h-m} \varepsilon_i' \theta_1^{-i} + \sum_{i=1}^{h-m} \eta_i' \theta_2^{-i} + x_0', \qquad x_0' \in M_0,$$

has the property that $\varepsilon_{h-m}' = 0$, $\eta_{h-m}' \neq 0$, which contradicts the primitivity of M. If $\eta_h \in W(k_{m+1})$, then M contains the special element $\theta_1^{-1} + \eta_h^{\sigma^{h-1}} \theta_2^{-1}$ and the module

$$M_0' = E(\theta_1^{-1} + \eta_h^{\sigma^{h-1}} \theta_2^{-1}) + M_{02} \subset M$$

is isomorphic to M_0; at the same time long $M/M_0' <$ long M/M_0, which contradicts the minimality of M.

b) The same argument that led to the proof of Lemma 3.13, b) gives the required result.

COROLLARY. *Any special module isogenous to M_0 is isomorphic to M_0.*

PROOF. Indeed, let $M \supset M_0$ be a primitive special module and assume that the length of M/M_0 is minimal. If $M \neq M_0$, then M_0 contains an element of the form (3.18). I claim that $\varepsilon_h \in W(k_{m+1})$, for otherwise, as in the proof of a), we obtain

$$M \supset M_0' = E(\theta_1^{-1} + E_h \theta_2^{-1}) + M_0 \approx M_0,$$

which contradicts the minimality of M/M_0.

Now M, being a special module, contains with z also the element $F^{-m}Vz$, which has the form (3.18) but is not equal to z, provided $\varepsilon_h \in W(k_{m+1})$. This contradicts the uniqueness of z; thus $M = M_0$.

THEOREM 3.15. *The equidimensional Dieudonné modules isogenous to a module of the form $2E/E(F^m - V)$, $m \geqslant 1$, split into $m + 1$ components A_h', $0 \leqslant h \leqslant m$. The component A_h' consists of modules having a maximal special submodule $2E/E(F^m - V)$ of index $(0, \ldots, 0, \underbrace{1, \ldots, 1}_{h})$ and is isomorphic to the space of orbits of a certain finite group Γ_h' acting on an h-dimensional affine space with the p^{m+1} hyperplanes*

$$\bar{\varepsilon}_h = a, \qquad a \in k_{m+1},$$

deleted.

PROOF. As was remarked above, any module isogenous to M_0 is isomorphic to a certain minimal (and therefore primitive) module. Every minimal module $M = M_0$ belongs to itself as special submodule, because by the Corollary to Lemma 3.14, any special module is isomorphic to M_0. The minimal modules of a given height h are parametrized by the points $(\bar{\varepsilon}_1, \ldots, \bar{\varepsilon}_h)$, where ε_i, the coefficients of z in (3.18), are in M. From the minimality it follows that $\bar{\varepsilon}_h \notin k_{m+1}$ (cf. proof of the Corollary).

Conversely, if $\overline{\varepsilon}_h \in k_{m+1}$, then $Ez + M_0 = M$ is minimal over M_0, because it contains no special elements of height $\geqslant 1$. For otherwise in the notation of Lemma 3.13, a) we would obtain a special element

$$x \equiv \lambda_k \theta_1^{-h+k} + \lambda_k \varepsilon_h^{\sigma^k} \theta_2^{-h+k} \bmod F^{-h+k+1}M;$$

but the condition for $F^m V^{-1} x = x$ to be special gives

$$\lambda_k^{\sigma^{m+1}} = \lambda_k, \qquad (\lambda_k \varepsilon_h^{\sigma^k})^{\sigma^{m+1}} = \lambda_k \varepsilon_h^{\sigma^k},$$

whence $\varepsilon_h \in W(k_{m+1})$, which is not the case by hypothesis. The statement about the index is verified in the same way as in Theorem 3.14. Thus the theorem is proved.

6. It remains to classify the reductive modules.

THEOREM 3.16. *Any module isogenous to*

$$M_0 = Ex_0 \oplus Ex_1, \quad Vx_0 = 0, \qquad (F^m - V)x_1 = 0,$$

is isomorphic to one of the modules of the form

$$M_h = Ex_0 + Ex_1 + EF^{-h}(x_0 + x_1), \qquad 0 \leqslant h \leqslant m.$$

The modules M_h for distinct h are pairwise non-isomorphic.

PROOF. Let $M_0 = Ex_0 \oplus Ex_1 (Vx_0 = 0, \ (F^m - V)x_1 = 0)$ be a generalized maximal special submodule of M (cf. §7, 3.). First of all we show that the height of M over M_0 cannot exceed m. For otherwise M would contain an element of the form

$$x = F^{-h_1}x' + F^{-h_2}x'', \quad x' \in (Ex_0 \setminus FEx_0) \cup \{0\}, \qquad x'' \in (Ex_1 \setminus FEx_1) \cup \{0\},$$

$h_1 > 0$, $h_2 > 0$. If $x \neq 0$, then x' and x'' are not zero; this follows from the maximality of M_0. Further, for the same reason, $h_1 = h_2 = h$. If $h > m$, then $Vx = F^{m-h}x'' \in M_0$, but $EVx \neq Ex_1$, which contradicts the maximality of M_0, because $Ex_0 + EVx$ is a generalized special submodule containing M_0, but not equal to it.

As in Theorems 3.14 and 3.15, we obtain further that $M = Ex + M_0$ if x is an element of maximal height. In the same way we find that x can be chosen in the form

$$x = F^{-h}x_0' + F^{-h}x_1,$$

where $x_0' \in Ex_0 \setminus FEx_0$. But because $Ex_0' = Ex_0$, we may replace the generator x_0 by x_0'. Thus, M is isomorphic to M_h.

The height of M_h over its generalized maximal special submodule is exactly h. For no element of height $k \geqslant 1$ over M_0 can be contained in a generalized special submodule, because as we have shown, such an element is of the form

$$x = F^{-k}x' + F^{-k}x'', \qquad x', \ x'' \in M_0 \setminus FM_0,$$

and clearly $Vx \neq 0$ or $Vx'' \neq 0$ and besides, $(F^m - V)x \neq 0$, because $(F^m - V)x = F^{m-k}x' + (F^m - V)F^{-k}x''$ and $x' \neq 0$. It follows that the number h is invariantly defined and hence the modules M_h are pairwise non-isomorphic.

Thus, the theorem is established.

§9. Comments

The basic results of this chapter were formulated in the papers [4] and [5] of the author. The idea of classifying the modules M in a given class to within isogeny by considering submodules of M_F was stated in Dieudonné [30]; there he writes that he 'knows of no regular method of forming and classifying these submodules'. Theorem 3.13 gives the local analogue of the corresponding result for algebraic groups isogenous to the two-dimensional Witt group (cf. Serre [56]).

Chapter IV

ALGEBROID FORMAL GROUPS AND ABELIAN VARIETIES

The aim of this chapter is the study of algebroid commutative formal groups. The method we adopt consists in the following: we start from the theorem on the structure of commutative algebraic groups, obtained by global means in algebraic geometry, and then study the completions of algebraic groups, obtaining the properties of these groups 'globally'. We shall at first assume the base field to be algebraically closed, except when the contrary is stated.

In the first section it is shown that it is sufficient to study completions of algebraic varieties. The basic tool for their study is here Theorem 2.2 whose application rests on the p-adic representation of the endomorphism ring of the abelian variety construted in §§2 and 3. The possibility of using a variant of such a representation is mentioned in a remark by Cartier, but in explicit form it does not seem to occur in the literature. After this, in §4 the main result of this chapter is established, according to which every commutative formal group is weakly algebroid (see the definition at the beginning of §4). The fifth section deals with two problems. First we formulate two conjectures whose proof would lead to a complete classification of algebroid groups, and we give a number of examples on the use of these conjectures. Secondly we study a generalization of the notion of the 'supersingular invariant of an elliptic curve' of Deuring [23] for the case of curves of genus 2.

§1. General results

1. Firstly we remark that a formal group is algebroid if and only if every group isogenous to it is algebroid. This follows from Proposition 1.6, which shows that under any isogeny an algebroid group remains algebroid (in an obvious interpretation). Therefore we may confine ourselves to the description of algebroid formal groups up to isogeny, and in particular, to consider only reduced groups, algebraic as well as formal.

2. The completion of an algebraic group coincides with the completion of its connected component of the identity. Further, the completion of a non-commutative connected group is a non-commutative formal group. Thus,

for our purpose we may confine ourselves to considering connected commutative algebraic groups. The structure of such groups is described in the following known result.

PROPOSITION 4.1. *Let G be a connected commutative algebraic group over an algebraically closed field k of arbitrary characteristic. G contains a connected affine subgroup G_a whose factor-group $X = G/G_a$ is an abelian variety.*

Every connected affine group G_a over a field k is isogenous to a direct sum of a toroidal group and a unipotent group. A toroidal group is isomorphic to a direct sum of a finite number of multiplicative groups.

Every unipotent group is isogenous to a direct sum of Witt groups if the characteristic of the base field is finite, and to a direct sum of additive groups if the characteristic is zero.

COROLLARY. *An algebroid formal commutative group is isogenous to a direct sum of a complete abelian variety, a toroidal group and a unipotent group.*

Clearly all toroidal and unipotent formal groups are algebroid and are even isomorphic to completions of affine groups. It remains to examine the question whether equidimensional Dieudonné groups, which can only occur in completions of abelian varieties, are algebroid. The fact that completions of abelian varieties are equidimensional follows from Weil's theorem, that multiplication by an integer is an isogeny.

§2. The formal structure of abelian varieties; preliminary reduction

1. Let I be the injective hull of the simple artinian group $S = \operatorname{Spec} k[x]/(x^p)$, $c(x) = 1 \oplus x + x \oplus 1$; T the multiplicative formal group over k (cf. § 3 of Ch. I).

For any formal group G the group of 'formal characters' $\operatorname{Hom}(G, T)$ possesses a natural $W(k_1)$-module structure. (Clearly, this group is complete in the topology generated by the powers of p.) If the formal group G is reduced, then this module is free and its rank agrees with the dimension of the toroidal part of G.

We now recall the definition of the 'Tate group'. For any commutative (abstract) group Γ and any prime number p we consider the projective system formed by the groups ${}_{p^k}\Gamma$ consisting of the elements of Γ annihilated by multiplication by p^k, and homomorphisms $p^{k-1}: {}_{p^k}\Gamma \to {}_{p^l}\Gamma$, $k > 1$ (multiplication). The projective limit of this system is a $W(k_1)$-module and will be denoted by $\mathcal{T}_p(\Gamma)$. The mapping $\Gamma \Rightarrow \mathcal{T}_p(\Gamma)$ clearly is a covariant functor. In the case when X is an algebraic group, defined over a fixed algebraically closed field k, we shall for brevity instead of $\mathcal{T}_p(\operatorname{Hom}(\operatorname{Spec} k, X))$ simply write $\mathcal{T}_p(X)$.

PROPOSITION 4.2. *Let X be an abelian variety over the field k, and X^t the dual variety. Let M be a contravariant functor from the category of abelian varieties to the category of $W(k)$-modules, defined as follows:*

$$\left.\begin{aligned} M(X) &= M_1 \oplus M_2 \oplus M_3, \\ M_1 &= \mathrm{Hom}(\hat{X}, I), \\ M_2 &= W(k) \underset{W(k_1)}{\otimes} \mathrm{Hom}(\hat{X}, T), \\ M_3 &= W(k) \underset{W(k_1)}{\otimes} \mathscr{T}_p(X^t). \end{aligned}\right\} \tag{4.1}$$

This functor is additive and has the following properties:

a) *Let* $\varphi: X \to Y$ *be an isogeny of abelian varieties. Then the module homomorphism* $M(\varphi): M(Y) \to M(X)$ *is injective and the length* k *of the cokernel of* $M(\varphi)$ *is the largest integer such that* p^k *divides* deg φ.

b) *The rank of* $M(X)$ *is* 2dim X.

c) *If the morphism* $\varphi: X \to Y$ *is not an isogeny, then* long coker $M(\varphi) = \infty$.

PROOF. Every isogeny $\varphi: X \to Y$ is a product of 'elementary' isogenies, i.e. isogenies whose kernel is one of the following artinian groups:

1) G_n = Spec $k[Z/nZ]$, $(n, p) = 1$,
2) G_p = Spec $k[Z/pZ]$,
3) G_p^* (the linear groups dual to G_p),
4) s = Spec $k[x]/(x^p)$, $c(x) = x \otimes 1 + 1 \otimes x$.

An exact sequence of the form

$$0 \to G \to X \xrightarrow{\varphi} Y \to 0 \tag{4.2}$$

by the functorial correspondence $X \rightrightarrows X^t$ induces a dual sequence

$$0 \to G^t \to Y^t \xrightarrow{\varphi^t} X^t \to 0, \qquad G^t = \ker \varphi^t. \tag{4.3}$$

Results of Serre [55], combined with the 'duality theorem' of Cartier [21], show that if G is an artinian group of one of the types 1)-4), then the dual sequence (4.3) is exact and, moreover, the kernel G^t of the isogeny φ^t is isomorphic to the artinian group G^*, the linear dual of G. (It appears probable that the isomorphism between G^t and G^* holds for any artinian group G that occurrs as kernel of an isogeny of abelian varieties, but this variant of the duality of A. Weil apparently does not follow from results in the existing literature.)

The truth of Proposition 4.2 a) for the product $\varphi \circ \psi$ of two isogenies clearly follows from the statements for φ and ψ separately. It is therefore sufficient to verify these statements for elementary isogenies.

The exact sequences (4.2) and (4.3) induce exact sequences

$$0 \to \mathrm{Hom}(\hat{Y}, I) \to \mathrm{Hom}(\hat{X}, I) \to \mathrm{Hom}(G, I) \to 0, \tag{4.4}$$

$$0 \to W(k) \otimes \mathrm{Hom}(\hat{Y}, T) \to W(k) \otimes \mathrm{Hom}(\hat{X}, T) \to W(k) \otimes \mathrm{Hom}(G, T) \to 0, \tag{4.5}$$

$$0 \to W(k) \otimes \mathscr{T}_p(\hat{Y}^t) \to W(k) \otimes \mathscr{T}_p(\hat{X}^t) \to W(k) \otimes \mathscr{T}_p(G^*) \to 0. \tag{4.6}$$

(The first two of these follow because the objects I and T are injective if $G = G_p$ or $G = S$, and from the fact that $\hat{\varphi}: \hat{X} \to \hat{Y}$ is an isomorphism if $G = G_n$ or $G = G_p^*$; the exactness of the third follows from the work of

Serre [55].)

It follows immediately that $M(\varphi)$ is injective.

Let $G = G_n$, $(n, p) = 1$. Then $G^t = G^* = G_n$. In this case deg $\varphi = n$ is not divisible by p, and the third term of the exact sequences (4.4), (4.5) and (4.6) is zero.

Let $G = G_p$. In this case $G^t = G_p^*$, deg $\varphi = p$, the third term of the sequences (4.4) and (4.6) is zero and the third term of (4.5) is isomorphic to $W(k)/pW(k)$, i.e. of length 1. A similar result holds if $G = G_p^*$, with this difference that here the third terms of (4.4) and (4.5) become zero.

Finally, for $G = S$ only the third term in (4.4) is zero and Hom (G, I) = Hom $(S, I) = W(k)/pW(k)$, while deg $\varphi = p$.

From what was said above the truth of a) follows. The statement b) follows from the fact that the isogeny $p.1_X$ representing multiplication by p has degree p^{2n}, where $n = \dim X$, and the cokernel of $M(p1_X)$ has length $r = \operatorname{rg} M(X)$.

Let $Z = \operatorname{Im} \varphi \subset Y$. If $\dim Z < \dim X$, then $\operatorname{rg} M(Z) < 2 \dim X$, whence c) follows.

Thus the proposition is proved.

2. From this result we can already obtain a number of consequences on the structure of algebroid formal groups. The following fact was obtained in a different way in the author's doctoral dissertation.

Let X be an abelian variety of dimension n, and put

$$\hat{X} \sim fG_{1,0} + \sum_i G_{n_i, m_i}, \qquad n_i m_i > 0.$$

Then

$$\sum n_i = \sum m_i = n - f. \tag{4.7}$$

Indeed, since the varieties X and X^t are isogenous, the dimension of the toroidal components of $\hat{X}$ and of $\hat{X}^t$ has the same value f. Let us put $M(X) = M_1 \oplus M_2 \oplus M_3$ corresponding to the decomposition (4.1); then the length of the cokernel of the restriction of $M(p1_X)$ to $M_2 \oplus M_3$ is equal to $2f$, and the length of the cokernel of the restriction of this homomorphism to M_1 is $\sum_i (n_i + m_i)$. Therefore $2f + \Sigma(n_i + m_i) = 2n$. On the other hand, $f + \Sigma n_i = n$. Hence (4.7) follows. From it we immediately obtain the following result:

COROLLARY. *All homogeneous formal groups of the form $kG_{n,m}$, where $mn > 1$, are non-algebroid.*

(For otherwise we should have $kG_{n,m} \sim \hat{X}$, where X is an abelian variety, but then by (4.7) it follows that $m = n$, which is impossible, because $mn > 1$ and $(m, n) = 1$.)

Only the series of equidimensional homogeneous groups like $G_{1,1}$ do not satisfy the conditions of this corollary, and in fact they form an exception: all such groups are algebroid. Indeed, $G_{1,1} \approx \hat{X}$, where X is an elliptic curve (one-dimensional abelian variety) with vanishing Hasse invariant. (If the Hasse invariant is different from zero, then $\hat{X} \approx G_{1,0}$, so that toroidal groups can be realized as completions of an abelian variety.) This result follows trivially from the proof of Theorem 4.1 below.

Thus, the majority of commutative formal groups of a given dimension are non-algebroid. Condition (4.7), representing a strict 'selection rule' for algebroid formal groups, however, does not exclude the possibility of any equidimensional formal group being contained in the completion of an abelian variety together with other formal groups. Our main objective in the next two sections consists in proving that such a possibility really occurs.

§3. The formal structure of abelian varieties; the fundamental theorem

1. Following Serre [55], we shall deduce from Proposition 4.2 the possibility of a p-adic representation for the endomorphism ring of a variety X over the module $M(X)$.

PROPOSITION. *Let $\varphi: X \to X$ be an endomorphism of an abelian variety, and let $M(\varphi)$ be the corresponding endomorphism of $M(X)$. Then the characteristic polynomial of $M(\varphi)$ coincides with the characteristic polynomial of φ in the sense of A. Weil.*

PROOF. We shall make use of the following lemma of A. Weil:

LEMMA 4.1. *Let $P(\lambda)$, $Q(\lambda)$ be polynomials of the same degree with coefficients in the ring $W(k_1)$ of p-adic numbers and highest coefficient unity. Let $\varepsilon_1, \ldots, \varepsilon_r$; $\eta_1, \ldots, \eta_r$ be the roots of P and Q respectively. Suppose that for any polynomial $F(T)$ with integer coefficients we have $\nu_p(\prod_{i=1}^{r} F(\varepsilon_i)) = \nu_p(\prod_{i=1}^{r} F(\eta_i))$. Then $P(\lambda) = Q(\lambda)$.*

Since the characteristic polynomial $P(\lambda)$ of φ is defined by the property $P(\lambda) = \det(\varphi - \lambda 1_X)$ for any integral λ, and the characteristic polynomial $Q(\lambda)$ of $M(\varphi)$ satisfies the corresponding condition $Q(\lambda) = \det(M(\varphi) - \lambda E)$ for all integral λ, we need only verify that for any endomorphism $\varphi: X \to X$ the highest powers of p by which $\det \varphi$ and $d(\varphi) = \det M(\varphi)$ are divisible, coincide. By Weil's Lemma this result suffices if the coefficients of $P(\lambda)$ and $Q(\lambda)$ belong to the ring of p-adic integers $W(k_1)$.

We begin by verifying the last statement. It is clearly satisfied for $P(\lambda)$. For $Q(\lambda)$ it is enough to verify that $d(\varphi)$ is always contained in the ring of p-adic integers. We have $d(\varphi) = d_1(\varphi)d_2(\varphi)d_3(\varphi)$, where $d_i(\varphi)$ is the determinant of the restriction of $M(\varphi)$ to the component M_i ($i = 1, 2, 3$) of $M(X)$. It is clear that $d_2(\varphi)$ and $d_3(\varphi)$ belong to $W(k_1)$. M_1 is an E-module, the restriction of φ to M_1 is an E-module endomorphism and in particular commutes with F. The determinant $d_1(\varphi)$ on M coincides with the determinant of the restriction of φ to FM_1, which in turn equals $d_1^{\sigma}(\varphi)$. Since $d_1(\varphi) = d_1^{\sigma}(\varphi)$, we have $p^k d_1(\varphi) \in W(k_1)$, where k is an integer. But it is also clear that $\nu_p(d_1(\varphi)) \geqslant 0$.

It remains to verify the equality of the p-adic exponent of $\deg \varphi$ and of $d(\varphi)$. But this follows immediately from Proposition 4.2, because $\nu_p(d(\varphi))$ coincides with the length of the cokernel of the homomorphism $M(\varphi)$.

Thus the proposition is established.

2. THEOREM 4.1. *Let X be an abelian variety defined over a*

finite field k_a of p^a elements, F_a the Frobenius endomorphism of this variety (induced by raising to the p^a-th power), $n = \dim X$ and $P(\lambda) = \lambda^{2n} + \ldots + p^{an}$ the characteristic polynomial of F_a. Put

$$P(\lambda) = \prod_{i=1}^{2n} (\lambda - \tau_i), \qquad \nu_p(\tau_i) = ac_i, \qquad 0 \leqslant c_i \leqslant 1,$$

where the elements τ_i belong to a ring of the form $W(k_b)[p^{1/e}]$, $b \equiv 0(a)$, $e \geqslant 1$. Denote by r_c the number of roots τ_i of $P(\lambda)$ satisfying $\nu_p(\tau) = ac$ and let $n_c = cr_c$, $m_c = r_c - n_c$. Then

$$\hat{X} \sim r_0 G_{1,0} + \sum_{0<c<\frac{1}{2}} (G_{nc,\,mc} + G_{mc,\,nc}) + \frac{1}{2} r_{\frac{1}{2}} G_{1,1}. \tag{4.8}$$

PROOF. Let us put $P(\lambda) = P_1(\lambda)P_2(\lambda)P_3(\lambda)$, where $P_i(\lambda)$ is the characteristic polynomial of the restriction of F_a to M_i. It is clear that the degree of $P_2(\lambda)$ is f, where f is the rank of the toroidal component of X. Let us show that

$$P_2(\lambda) = \prod_{\nu(\tau_i)=a} (\lambda - \tau_i), \qquad P_3(\lambda) = \prod_{\nu(\tau_i)=0} (\lambda - \tau_i). \tag{4.9}$$

Indeed, the kernel of F_a on the toroidal component of $\hat{X}$ has a composition series, whose factors are all isomorphic to G_p. It follows that $M(F_a)$ induces an automorphism of M_3 (cf. proof of Prop. 4.2), and hence the p-adic exponents of the characteristic roots of $M(F_a)$ on M_3 are all zero. Similarly the endomorphism $p^a F_a^{-1}$ induces an automorphism on M_2 whose characteristic roots are all p-adic units. Therefore in any case the equations (4.9) hold if we do not insist that the products are extended over *all* roots with the corresponding exponent. But on M_1 the endomorphism $M(F_a)$ is topologically nilpotent (i.e. for any $k > 0$ there exists an e such that $M(F_a)^e M_1 \subset p^k M_1$). It follows that none of the characteristic roots of $M(F_a)$ on M_1 can be a p-adic unit. Hence every root τ with $\nu_p(\tau) = 0$ is a root of $P_3(\lambda)$. Now by the functional equation of the zeta-function on an abelian variety, the polynomial $P(\lambda)$ has together with any root τ_i also a root $p^a \tau_i^{-1}$, so that the number of roots with $\nu_p(\tau_i) = a$ is the same as the number with $\nu_p(\tau_i) = 0$. For the same reason $P_2(\lambda)$ contains all factors $\lambda - \tau_i$ with $\nu_p(\tau_i) = a$ and only these. In particular, $f = r_0$ and the equations (4.9) are proved. They imply the following relation which is of great importance to us:

$$P_1(\lambda) = \prod_{0<\nu(\tau_i)<a} (\lambda - \tau_i) = \prod_{\substack{\nu(\tau_i)=ac \\ 0<c<\frac{1}{2}}} (\lambda - \tau_i)(\lambda - p^a \tau_i^{-1}) \prod_{\nu(\tau_j)=\frac{a}{2}} (\lambda - \tau_j). \tag{4.10}$$

$P_1(\lambda)$ represents the characteristic polynomial of $M(F_a)$ on M_1 and we are now in a position to apply Theorem 2.2. Thus, M_1 is the Dieudonné module of the corresponding component of $\hat{X}$. This component is defined over k_a, and the corresponding module over the algebraic closure $k \supset k_a$ is isomorphic to $W(k) \underset{W(k_a)}{\otimes} M_1$. Further, $M(F_a)$ induces on M_1 an endomorphism which coincides with Λ in the notation of Ch. 2, §3. The required result

on the structure of the E-module $W(k) \otimes M_1$ is now obtained immediately from (4.10) by Theorem 2.2. This result is clearly equivalent to the decomposition (4.8).

The theorem is now proved.

REMARK 1. The decomposition (4.8) shows that every simple group $G_{n,m}$ other than the multiplicative group is contained in the completion of an abelian variety with the same multiplicity as $G_{m,n}$ ('symmetry condition'). We have proved this result only for varieties over a finite field, and only up to isogeny. Clearly it can also be obtained as a consequence of the more general result, that the completions $\hat{X}$ and $\hat{X}^t$ of an abelian variety and its Picard variety are connected by a certain duality of formal groups[1] (see the remarks below on Weil duality).

REMARK 2. As J. Tate has remarked, the decomposition (4.8) may be written in a more symmetric form:

$$X \sim \sum_{0 \leqslant c < \frac{1}{2}} (G_{nc,\, mc} + G_{mc,\, nc}) + \frac{1}{2} r_{\frac{1}{2}}\, G_{1,1},$$

if we interpret the group $G_{0,m}$ for any m as the zero-dimensional group Spec k.

§4. Weakly algebroid groups

1. DEFINITION. A formal group is said to be weakly algebroid if it is isogenous to a subgroup of an algebroid formal group.

We shall now prove the fundamental result of this chapter.

THEOREM 4.2. *Every commutative formal group is weakly algebroid.*

2. *PROOF.* We shall effectively construct the totality of all abelian varieties whose completions contain (up to isogeny) all possible groups $G_{n,m}$. For this purpose it is sufficient to consider the Jacobian variety J_a of the Davenport-Hasse curves:

$$y^p - y = x^{p^a - 1} \qquad (a = 1,\ 2,\ 3,\ \ldots).$$

The dimension of J_a is $\frac{1}{2}(p-1)(p^a-2)$. In the paper of Davenport and Hasse [22] it is proved that the roots of the characteristic polynomial $P_a(\lambda)$ of the endomorphism F_a of J_a are trigonometric sums of the following form:

$$\tau(\psi, \chi) = \sum_{t \in k_a^*} \psi(t)\, \chi(t).$$

Here ψ ranges over a certain set of additive characters of the field k_a and χ ranges over a set of multiplicative characters, summed over all products in the group of non-zero elements of the field. The arithmetic of such sums was already studied by Stickelberger. Since we are interested in the p-adic behaviour of such sums, the following interpretation (cf. Dwork [1]) is particularly suitable for us. We set

---

[1] This is stated more precisely in the report by Barsotti [14]; no proof is given in this paper.

$$\psi_1(t)=\theta_a(\tilde{t}), \qquad \psi_i(t)=\psi_1(it), \qquad 1\leqslant i\leqslant p-1,$$
$$\chi_1(t)=\tilde{t}^{-1}, \qquad \chi_j(t)=\tilde{t}^{-j}, \qquad 1\leqslant j\leqslant p^a-2.$$

Here $\tilde{t}$ is a multiplicative representative of the element $t \in k_a$ in the ring $W(k_a)$, and the character θ_a is defined as follows:

$$\theta_a(t)=\zeta^{\tilde{t}+\tilde{t}^p+\ldots+\tilde{t}^{p^a-1}}, \qquad \zeta^p=1,\ \zeta\neq 1. \tag{4.11}$$

It is well known that $\zeta \in W(k_1)[p^{1/e}]$, $e = p - 1$. According to Davenport and Hasse, the decomposition of $P_a(\lambda)$ into factors has the following form:

$$P_a(\lambda)=\prod_{i,j}(\lambda-\tau(\psi_i,\chi_j)), \quad 1\leqslant i\leqslant p-1,\ 1\leqslant j\leqslant p^a-2.$$

Clearly, $\tau(\psi_i, \chi_j) \in W(k_a)[p^{1/(p-1)}]$, so that the conditions of Theorem 4.1 hold.

We shall now compute the p-adic exponents of the roots $\tau(\psi_i, \chi_j)$.

In the first place

$$\tau(\psi_i,\chi_j)=\sum_{l\in k_a^*}\psi(it)\chi_j(t)=\varepsilon_i^{-j}\sum_{l\in k_a^*}\psi(it)\chi_j(it)=\varepsilon_i^{-j}\tau(\psi_1,\chi_j),$$

where ε_i is a multiplicative representative of the element i mod p in the ring $W(k_a)$. Next, we consider $j=\sum_{i=0}^{a-1} j_i p^i$, $0 \leqslant j_i \leqslant p-1$, the p-adic decomposition of j, and write

$$\sigma(j)=\sum_{i=0}^{a-1} j_i, \qquad \gamma(j)=\prod_{i=0}^{a-1} j_i.$$

By a relation due to Stickelberger (cf. Dwork [1]),

$$\tau(\psi_1,\chi_j)=-\gamma(j)^{-1}\lambda^{\sigma(j)} \mod \lambda^{\sigma(j)+1}, \quad \lambda=1-\zeta.$$

Since $\nu_p(\lambda) = 1/(p-1)$, we have

$$\nu_p(\tau(\psi_1,\chi_j))=\nu_p(\tau(\psi_i,\chi_j))=\frac{\sigma(j)}{p-1} \qquad (i=1,\ldots,p-1).$$

It is clear that $\sigma(j)$ assumes all values between 1 and $a(p-1)-1$, as j runs from 1 to $p^a - 2$. Therefore the set of numbers $\frac{\nu(\tau(\psi_i,\chi_j))}{a}$ includes all rational numbers between zero and one whose denominator divides $a(p-1)$. By Theorem 4.1 this means that the decomposition of the formal group $\hat{J}_a$ includes homogeneous groups of all types (m, n) for which the sum $m + n$ divides $a(p-1)$ (indeed, by Theorem 4.1, the inclusion in $\hat{J}_a$ of a group of type (m, n) is equivalent to the existence of a characteristic root τ with exponent $\nu_p(\tau) = \frac{an}{n+m}$).

Hence, for any pair of coprime integers m, n the algebroid formal group $\hat{J}_{m+n}$ contains a component isogenous to $rG_{n,m}$, $r \geqslant 1$.

This completes the proof of the theorem.

§5. Remarks and examples

1. The sequence of groups $\hat{J}_a$, while showing that all commutative formal groups are weakly algebroid, unfortunately does not provide us with the means of describing all algebroid formal groups. The groups $G_{n,m} + G_{m,n}$ are the smallest formal groups that satisfy the selection rule (4.7) and the symmetry condition of Theorem 4.1 (from which the relation (4.7) follows automatically). I should be inclined to state the following conjectures:

CONJECTURE 1. *The groups $G_{n,m} + G_{m,n}$ are algebroid.*

The proof of this conjecture and a slight sharpening of Theorem 4.1 (proof of the symmetry condition for groups that are completions of abelian varieties over not necessarily finite fields) could be deduced from the following complete classification of algebroid commutative groups.

CONJECTURE 2. *A group G is algebroid if and only if it is isogenous to a group of the form*

$$G \sim \sum_i G_{r_i,\infty} + sG_{1,0} + \sum_j (G_{n_j,m_j} + G_{m_j,n_j}), \qquad m_j n_j \neq 0.$$

For the proof of Conjecture 1 it is necessary to know how to construct an abelian variety in which the Frobenius endomorphism satisfies strict arithmetical conditions. For we have the following variant of Theorem 4.1, which deserves a separate formulation, because it does not require the calculation of the roots of $P(\lambda)$ and the verification that they are 'not too badly ramified'.

THEOREM 4.1'. *Let X be an abelian variety defined over a finite field k_a of p^a elements, $\dim X = g$, and let F_a and $P(\lambda)$ have the same meaning as in Theorem 4.1. Then the formal group X is isogenous to $G_{n,m} + G_{m,n}$ $(n < m,\ n + m = g,\ (n, m) = 1)$ if and only if the characteristic polynomial $P(\lambda) = \sum_{i=0}^{2g} a_i \lambda^i$ satisfies the following conditions:*

$$\min \frac{v_p(a_j)}{a(2g-j)} = \frac{v_p(a_g)}{ag} = \frac{n}{m+n}.$$

PROOF. If $P(\lambda)$ satisfies the conditions of the theorem, then by the remark to Lemma 2.2 and the functional equation

$$P(p^a \lambda^{-1})\, \lambda^{2g} = p^{ag} P(\lambda)$$

a non-commutative decomposition of this polynomial over the ring $W(k)[p^{1/g}]$ (where $k \supset k_a$ is the algebraic closure and $g = n + m$) has the form

$$P(\lambda) = \prod_{i=1}^{g} (\lambda - p^{\frac{an}{g}} x_i) \prod_{i=1}^{g} (\lambda - p^{\frac{am}{g}} y_i),$$

where $x_i,\ y_i \in W(k)[p^{1/g}]$ are invertible. If $a = 1$, it follows immediately that $\hat{X} \sim G_{n,m} + G_{m,n}$; if $a > 1$, then the result follows by the same reasoning as in the proof of Theorem 2.2.

Now if $P(\lambda)$ does not satisfy the condition of the theorem, then either

$$\min \frac{\nu_p(a_j)}{a(2g-j)} = \frac{r}{s} \neq \frac{n}{n+m},$$

or $\min \dfrac{\nu_p(a_j)}{a(2g-j)} = \dfrac{n}{n+m}$, but the least value of j for which this minimum is attained is greater than g. In the first case the completion $\hat{X}$ contains a group $G_{r,s-r}$ and the second case is impossible, because then $X \sim G_{n,m} + G_{m,n} + G$, where G is a group of dimension $\geqslant 1$, which contradicts the equation $\dim \hat{X} = g = n + m$.

This proves the theorem.

I do not know how to construct abelian varieties with such properties in the general case; the difficulty is increased by the fact that it is clearly hopeless to try and obtain such varieties by reducing mod p an abelian variety over a field of characteristic zero with the required properties.

Therefore I shall confine myself to two examples that verify the conjectures for very small values of p, m, n, namely: $p = 3$, $n = 1$, and $m = 2, 3$.

In both cases the example is furnished by the Jacobian variety of a hyperelliptic curve of genus 3 or 4, respectively, over a field of three elements.

The determination of curves whose Jacobian variety possesses a given formal structure can only proceed by trial and error: with the help of the Hasse-Witt matrix it is possible to select curves for which the completion of the Jacobian variety contains no toroidal components, and then we can immediately calculate the number of points on these curves in fields of 3, 3^2, 3^3 elements for genus 3 and even in fields of 3^4 elements for genus 4. The characteristic polynomial can then be constructed, by making use of the well known formulae:

$$N_a = 1 + q^a - \sum_{i=1}^{g} (\tau_i^a + q^a \tau_i^{-a}) \qquad (a = 1, \ldots, g).$$

(This formula is valid for any complete non-singular curve of genus g over a field of q elements; N denotes the number of points on this curve over a field of q^a elements, and $P(\lambda) = \prod_{i=1}^{g} (\lambda - \tau_i)(\lambda - q\tau_i^{-1})$ is the characteristic polynomial of the Frobenius endomorphism $(x) \to (x^q)$ on the Jacobian variety of the curve.)

After these general remarks we come to our examples.[1] Any details which are omitted may easily be checked.

EXAMPLE 1. X is the Jacobian variety of the curve of genus 3

$$y^2 = x^7 - x + 1$$

over a field of $q = 3$ elements.

Here

$$N_1 = 7, \qquad N_2 = 13, \qquad N_3 = 37,$$

[1] The hyperelliptic curve considered below has a singular point at infinity, but this is a cusp which corresponds to a unique point on the non-singular model.

whence

$$P(\lambda) = \lambda^6 + 3\lambda^5 + 6\lambda^4 + 12\lambda^3 + 18\lambda^2 + 27\lambda + 27.$$

The Newton polygon gives

$$\min \frac{\nu_3(a_i)}{6-1} = \frac{\nu_3(a_3)}{3} = \frac{1}{3}.$$

Thus, X satisfies the condition of Theorem 4.1′. It follows that

$$\hat{X} \sim G_{1,2} + G_{2,1}.$$

EXAMPLE 2. X is the Jacobian variety of the curve of genus 4

$$y^2 = x^9 + x^7 + x + 1$$

over a field of $q = 3$ elements.

In this case

$$N_1 = 7, \quad N_2 = 13, \quad N_3 = 37, \quad N_4 = 85,$$

whence

$$P(\lambda) = \lambda^8 + 3\lambda^7 + 6\lambda^6 + 12\lambda^5 + 21\lambda^4 + 36\lambda^3 + 54\lambda^2 + 81\lambda + 81.$$

The Newton polygon gives

$$\min \frac{\nu_3(a_i)}{8-i} = \frac{\nu_3(a_4)}{4} = \frac{1}{4}.$$

Therefore by Theorem 4.1′,

$$\hat{X} \sim G_{1,3} + G_{3,1}.$$

2. Another circle of questions on the structure of the completion of algebraic groups is connected with the following circumstance. Consider a given algebraic system of curves of genus 2 over a field of finite characteristic. It can be shown that the points of the parameter space for which the completion of the Jacobian variety corresponding to the curve has a given isogeny type are constructible sets. What is the structure of these sets and in particular their dimension? This problem is the widest natural generalization of the problem of describing the 'supersingular' invariants of an elliptic curve, solved by Deuring [23].

A complete answer to this question presupposes fairly precise information on the module space of curves of a given genus.

For $g = 1$ the curve is defined by its absolute invariant j. Its completion is isomorphic either to $G_{1,0}$ or to $G_{1,1}$. The first case is typical, the second is realized for the values

$$\left[\frac{p}{12}\right] + r_p, \qquad r_p = 0, \ 1 \text{ or } 2,$$

of j that are roots of $A_p(j)$, the Hasse invariant, which can be described explicitly. In this text see the papers by Deuring [23] and Igusa [49].

For $g = 2$ the question has apparently not been investigated. Here the possible structure of the completion $\hat{J}$ is $G_{1,0} + G_{1,0}$, $G_{1,0} + G_{1,1}$ and $G_{1,1} + G_{1,1}$. They are all realized and correspond to the values 2, 1, 0 of the rank of the matrix AA^{σ}, where A is the Hasse-Witt matrix of the curve. This computation likewise makes use of the condition $p > 2$. From the general formulae proved by the author [8] it follows that for the curve

$$y^2 = \sum_{i=0}^{5} a_i x^i \equiv F(x)$$

of genus 2 over a field of characteristic p the Hasse-Witt matrix has the form

$$A = \begin{pmatrix} b_{p-1} & b_{p-2} \\ b_{2p-1} & b_{2p-2} \end{pmatrix},$$

where the b_i are defined by the identity

$$F(x)^{\frac{p-1}{2}} = \sum_{i-0}^{5\frac{p-1}{2}} b_i x^i.$$

Therefore the choice of the structure on the completion $\hat{J}$ is equivalent to the imposition of the following relations for the coefficients of the polynomial $F(x)$:

$$\hat{J} \sim 2G_{1,0} \Leftrightarrow\Rightarrow b_{p-1} b_{2p-2} - b_{p-2} b_{2p-1} = |A| = 0;$$

$$\hat{J} \sim G_{1,0} + G_{1,1} \Leftrightarrow\Rightarrow |A| = 0, \qquad AA^{\sigma} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix};$$

$$\hat{J} \sim 2G_{1,1} \Leftrightarrow\Rightarrow \begin{cases} b_{p-1}^{p+1} + b_{p-2}\ b_{2p-1}^{p} = 0, \\ b_{p-1}^{p} + b_{2p-2}\ b_{2p-1}^{p} = 0. \end{cases}$$

These relations constitute an analogue to Deuring's formulae [23] for supersingular elliptic curves. They enable us to show that the dimension of the locally closed subsets of the module space corresponding to the three possible variants of the structure of $\hat{J}$ is equal to 3 ('general case'), 2, and 1, respectively. For $g = 1$, all elliptic curves whose completion is isomorphic to $G_{1,1}$, are isogenous among themselves 'globally'. Is this also true for $g = 2$ and the case $\hat{J} \sim 2G_{1,1}$?

For $p = 2$ the result can be obtained particularly simply. According to Igusa [50], in this case every hyperelliptic curve of genus 2 can be reduced to a normal form of one of three types. It turns out that this decomposition corresponds exactly to the decomposition of the Jacobian varieties of these curves into three types according to the structure of their completions.

The precise results are as follows.

a) Normal form

$$y^2 - y = x^3 + \alpha x + \beta x^{-1} + \gamma (x-1)^{-1}, \qquad \alpha\beta\gamma \neq 0.$$

In this case a basis for the space of differentials of the first kind of the curve consists of the differentials $\frac{dx}{x}$ and $\frac{dx}{x+1}$. Since they are 'logarithmic', we have according to Cartier and Barsotti

$$\hat{J} \sim G_{1,0} + G_{1,0}.$$

b) Normal form

$$y^2 - y = x^3 + \alpha x + \beta x^{-1}, \qquad \beta \neq 0.$$

Here the basis for the space of differentials of the first kind can be taken to be of the form $(dx, \frac{dx}{x})$. Only one of these differentials is logarithmic, while the other is complete. Therefore

$$\hat{J} \sim G_{1,0} + G_{1,1}.$$

c) Normal form

$$y^2 - y = x^5 + \alpha x^3.$$

Here the differentials of the first kind are dx and xdx. No linear combination of them can be a logarithmic differential, so that $\hat{J}$ has no toroidal components. Therefore

$$\hat{J} \sim G_{1,1} + G_{1,1}.$$

§6. Comments

The first general result on the structure of completions of abelian varieties is contained in the paper [8] of the author, which arose from an attempt to answer two questions raised by Barsotti [11], [12]. Already in this paper there appears in embryonic form the connection between the formal structure and the characteristic polynomial of the Frobenius endomorphism. The complete result (here Theorems 4.1 and 4.2) were formulated in the author's note [6]. It would be interesting to try to apply the techniques of Barsotti [13] to a proof of the general 'symmetry condition'

In the case of non-commutative groups the study of the representation of formal groups in algebroid groups is a basic tool in the classification (cf. Dieudonné [29]). In contrast to the commutative case, here all simple groups (and further all groups without a centre) turn out to be algebroid. The fundamental investigation of extensions of formal groups was begun in the paper of Dieudonné [31]. Only partial results were obtained; in this problem one can see particularly clearly the necessity of including the theory of non-commutative groups in the general categorical frame-work, similarly to that outlined in the first chapter of our paper, for the application of standard homological techniques.

In the same paper [31] Dieudonné constructs an interesting example which shows that a non-commutative extension of an additive formal group by another additive group may be a non-algebroid group. It seems likely that this example is connected with the general 'pathological' properties of the Witt group (in particular, the additive group). Perhaps formal extensions of algebroid groups are algebroid if we confine ourselves to the consideration of groups without unipotent components.

Received by the editors 1st January 1963.

References

[1] B. Dwork, On the rationality of the zeta-function of an algebraic variety, Amer. J. Math. 82 (1960) 631-648 (Russian transl. Matematika 5: 6 (1961) 55-71).

[2] N. Jacobson, Theory of rings (New York 1943) (Teoriya kolets, Moscow 1947).

[3] E.B. Dynkin, Normed Lie algebras and analytic groups, Uspekhi Mat. Nauk 5, 1 (1950) 135-186 (AMS transl. 1st series, No. 97 1953).

[4] Yu.I. Manin, Two-dimensional formal abelian groups, Doklady Ak. Nauk 143 (1962) 35-37 (Soviet Math. Doklady 3, 2, 335-337).

[5] Yu.I. Manin, On the classification of formal abelian groups, Doklady Ak. Nauk 144 (1962) 490-492 (Soviet Math. Doklady 3, 3, 757-759).

[6] Yu.I. Manin, Commutative formal groups and abelian varieties, Doklady Ak. Nauk 145 (1962) 280-283 (Soviet Math. Doklady 3, 4, 992-994).

[7] Yu.I. Manin, A remark on restricted Lie algebras, Sibirsk. Mat. Zh. 3 (1962) 479-480.

[8] Yu.I. Manin, On the theory of abelian varieties over a field of finite characteristic, Izvestiya Ak. Nauk, Ser. Mat. 26 (1962) 281-292.

[9] L.S. Pontryagin, *Nepreryvnye gruppy* (Moscow 1954), Topologische Gruppen I, II (Leipzig 1957 , 1958).

[10] C. Chevalley, Théorie des groupes de Lie II (Paris 1951) (Teoriya grupp Li 2, Moscow 1958).

[11] I. Barsotti, Abelian varieties over fields of positive characteristic, Rend. Circ. Mat. Palermo, ser. II, 5 (1956) 145-169.

[12] I. Barsotti, Gli endomorfismi delle varietà abeliane su corpi di caratteristica positiva, Ann. Scuola Norm. Sup. Pisa, ser. III, 10 (1956) 1-24.

[13] I. Barsotti, Moduli canonici i gruppi analitici commutativi, Ann. Scuola Norm. Sup. Pisa, Ser. III, 13 (1959) 303-372.

[14] I. Barsotti, Analytical methods for abelian varieties in positive characteristics, Colloque sur la théorie des groupes algébriques, Bruxelles 1962.

[15] A. Borel, Groupes linéaires algébriques, Ann. of Math. 64 (1956) 20-82.

[16] P. Cartier, Isogénies des variétés des groupes, Bull. Soc. Math. France 87 (1959) 191-220.

[17] P. Cartier, Calcul différentiel sur les varietés algébriques en caractéristique non nulle, C.R. Acad. Sci (Paris) 235 (1957) 1109-1111.

[18] P. Cartier, Théorie différentielle des groupes algébriques, C.R. Acad. Sci (Paris) 244 (1957) 540-542.

[19] P. Cartier, Hyperalgébres et groupes de Lie formels, Séminaire Sophus Lie (1955-1956) 1-5.

[20] P. Cartier, Groupes algébriques et groupes formels, Dualité. Colloque sur la théorie des groupes algébriques, Bruxelles 1962.

[21] P. Cartier, Dualité des varietés abéliennes, Séminaire Bourbaki, Mai 1958.

[22] H. Davenport, H. Hasse, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, Journ. reine angew. Math. 172 (1934) 151-182.

[23] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abhandl. Math. Sem. Hamburg Univ. 14 (1941) 197-272.

[24] J. Dieudonné, Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$, Comm. Math. Helv. 28 (1954) 87-118.

[25] J. Dieudonné, Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$ (II), Amer. J. Math. 77 (1955) 218-244.

[26] J. Dieudonné, Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$ (III) Math. Z. 63 (1955) 53-75.

[27] J. Dieudonné, Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$ (IV), Amer. J. Math. 77 (1955) 429-452.

[28] J. Dieudonné, Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$ (V), Bull. Soc. Math. France 84 (1956) 207-239.

[29] J. Dieudonné, Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$ (VI), Amer. J. Math. 79 (1957) 331-388.
[30] J. Dieudonné, Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$ (VII), Math. Ann. 134 (1957) 114-133.
[31] J. Dieudonné, Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$ (VIII), Amer. J. Math. 80 (1958), 740-772.
[32] J. Dieudonné, Sur les groupes formels abéliens unipotents, Rend. Circ. mat. Palermo, II ser. 5 (1956) 170-180.
[33] J. Dieudonné, Le calcul différentiel dans les corps de caractéristique $p > 0$. Proc. Internat. Congress Amsterdam 1954, vol. 1 (1957) 240-252 (transl. Mezhdunarodnye matematicheskii kongress v Amsterdame (1954), Moscow Fizmatgiz 1961, 134-150).
[34] J. Dieudonné, Sur quelques groupes de Lie abéliens sur un corps de caractéristique $p > 0$, Arch. Math. 5 (1954) 274-281; corrections Arch. Math. 6 (1955) 88.
[35] P. Gabriel, Objets injectifs dans les catégories abéliennes, Séminaire Dubreil-Pisot (1958-1959).
[36] P. Gabriel, La localisation dans les anneaux non commutatifs, Séminaire Dubreil-Pisot (1959-1960).
[37] P. Gabriel, Sur les catégories localement noethériennes et leurs applications aux algèbres étudiées par Dieudonné (Groupes formels), Séminaire J.-P. Serre (1960).
[38] M. Greenberg, Schemata over local rings, Ann. of Math. 73 (1961) 624-648.
[39] A. Grothendieck, Éléments de géométrie algébrique (en collaboration avec J. Dieudonné). Ch. I. Le language des schémas, Ch. III. Étude cohomologique des faisceaux cohérents, Institut des Hautes Études Scientifiques, Paris, Publ. Math. No. 8 (1960), No. 11 (1961).
[40] A. Grothendieck, Technique de descente et théorèmes d'existence en géométrie algébrique. I. Généralités, Descente par morphismes fidèlement plats, Séminaire Bourbaki 190 (1959-1960).
[41] A. Grothendieck, Technique de descente et théorèmes d'existence en géométrie algébrique II. Le théorème d'existence en théorie formelle des modules, Séminaire Bourbaki 195 (1959-1960).
[42] A. Grothendieck, Techniques de construction et théorèmes d'existence en géométrie algébrique I. Description axiomatique de l'espace de Teichmüller et de ses variantes, Séminaire H. Cartan 7-8 (1960-1961).
[43] A. Grothendieck, Techniques de construction et théorèmes d'existence en géométrie algébrique III. Préschémas quotients, Séminaire Bourbaki 212 (1960-1961).
[44] A. Grothendieck, Sur quelques points d'algèbre homologique, Tohoku Math. J. 9 (1957) 119-221 (O nekotorykh voprosakh gomologicheskoi algebry, Moscow 1961).
[45] A. Grothendieck, Séminaire de géométrie algébrique 1961 exp. XI: Exemples et compléments.
[46] A. Grothendieck, Sur quelques propriétés fondamentales en théorie des intersections, Séminaire Chevalley 4 (1958).
[47] J.I. Igusa, On some problems in abstract algebraic geometry, Proc. Nat. Acad. Sci. 41 (1955) 964-967.
[48] J.I. Igusa, Analytical groups over complete fields, Proc. Nat. Acad. Sci. 42 (1956) 540-541.
[49] J.I. Igusa, Class number of a definite quaternion field with prime discriminant, Proc. Nat. Acad. Sci. 44 (1958) 312-314.
[50] J.I. Igusa, Arithmetic variety of moduli for genus two, Ann. of Math. 72 (1960) 612-649.
[51] M. Lazard, La non-existence des groupes de Lie formels non abéliens à un paramètre, C.R. Acad. Sci. (Paris) 239 (1954) 942-945.
[52] M. Lazard, Sur les groupes de Lie formels à un paramètre, Bull. Soc. Math. France 83 (1955) 251-274.

[53] M. Lazard, Lois de groupes et analyseurs, Ann. Sci. École Norm. Sup. (3) 72 (1955) 299-400.
[54] J.-P. Serre, Sur la topologie des variétés algébriques en caractéristique p, Symposium International de Topologia Algebrica, Mexico (1958) 24-53.
[55] J.-P. Serre, Quelques propriétés des variétés abéliennes en caractéristique p, Amer. J. Math. 80 (1958) 715-740.
[56] J.-P. Serre, Groupes algébriques et corps de classes (Paris 1959).
[57] J.-P. Serre, Groupes proalgébriques, Institut des Hautes Études Scientifiques, Publ. Math. No. 7 (1960).
[58] J.-P. Serre, Sur les corps locaux à corps résiduel algébriquement clos, Bull. Soc. Math. France 80 (1961) 105-154.
[59] S. Togo, Note on formal Lie groups, Ann. of Math. 81 (1959) 632-638.
[60] S. Togo, Note on formal Lie groups II. J. Sci. Hiroshima Univ. ser. A-1, 25 (1961) 353-356.

Translated by P.M. Cohn