p-Divisible Groups [1]

J. T. TATE

Introduction

After a brief review of facts about finite locally free commutative group schemes in § 1, we define p-divisible groups in § 2, and discuss their relation to formal Lie groups. The § 3 contains some theorems about the action of $\mathrm{Gal}(\bar{K}/K)$ on the completion C of the algebraic closure $\bar{K}$ of a local field K of characteristic 0. In § 4 these theorems are applied to obtain information about the Galois module of points of finite order on a p-divisible group G defined over the ring of integers R in such a field K, and to prove that G is determined by that Galois module, or, what is the same, by its generic fiber $G\times_R K$.

The notion of p-divisible group and the basic theorems of § 2 are the result of joint work with SERRE, and § 3 and § 4 owe much to discussions with him. Although p-divisible groups are interesting enough in their own right, our main motivation for studying them has been their applications to abelian varieties. For some of these, and for further results on p-divisible groups, as well as additional bibliography, see SERRE, [10] and [11].

This text owes much – probably its very existence – to the efforts of T. SPRINGER, who wrote a first draft shortly after the conference. In several places, and particularly in § 3, he has made improvements on the original oral exposition. I thank him heartily for his help.

§ 1. Finite group schemes

(1.1). Let R be a commutative ring (or a prescheme). By a *finite group of order m over R* we shall mean a group scheme G which is locally free of rank m over R. Such a G is defined by a locally free (sheaf of) algebra(s) A of rank m over R. The group structure is described by homomorphisms

[1] The research described here has been partially supported by NSF.

$\mu: A\to A\otimes A$, $\varepsilon: A\to R$, and an automorphism $i: A\to A$, describing multiplication, neutral element, and inverse, respectively. These are subject to a number of rather obvious conditions (see for example [4] or [6]).

Examples. (a) Let Γ be a finite abstract group of order m. Let A be the ring of R-valued functions on Γ, let $(\mu f)(s,t)=f(st)$, let $(if)(s)=f(s^{-1})$, and let $\varepsilon f=f(1)$. Then $\Gamma=\mathrm{Spec}(A)$ is a finite group of order m over R.

(b) Let $A=R[X]/(X^m-1)$, with $\mu(x)=x\otimes x$, where x is the image of X in A. Then $\mathrm{Spec}(A)$ is a finite group of order m over R which is denoted by $\boldsymbol{\mu}_m$; it is the kernel of the homomorphism m: $\mathbf{G}_m\to\mathbf{G}_m$, where $\mathbf{G}_m$ denotes the "multiplicative group", viewed over R.

(c) Let $a, b\in R$ with $ab=2$. Put $A=R+Rx$, with $x^2+ax=0$, and put $\mu x=x\otimes 1+1\otimes x+bx\otimes x$. Then $G_{a,b}=\mathrm{Spec}(A)$ is the most general group of order 2 over R whose affine algebra A is free over R. Moreover, $G_{a,b}$ and $G_{a',b'}$ are isomorphic if and only if there is a unit u in R such that $a'=ua$, $b'=u^{-1}b$.

(1.2). Duality

From now on we assume all groups to be commutative. Then there is a duality theory, due to CARTIER (see [3], p. 106). Let $G=\mathrm{Spec}A$ be a finite group over R and $m: A\otimes A\to A$ define the multiplication in A and $\mu: A\to A\otimes A$ the group law. Put $A'=\mathrm{Hom}_{R\text{-modules}}(A,R)$. We then get dual homomorphisms

$$\mu': A'\otimes A'\to A', \quad m': A'\to A'\otimes A'.$$

μ' defines an algebra structure on A' and it is easy to check that m' defines a product on $G'=\mathrm{Spec}(A')$, which makes it into a group scheme. The order of G' is equal to that of G. G' is called the *Cartier dual* of G. There is a canonical isomorphism $G\tilde{\to}(G')'$.

If T is a prescheme over R, then the group $G'(T)$ is canonically isomorphic to $\mathrm{Hom}_T(G,\mathbf{G}_m)$ (homomorphisms of group schemes over T of $G\times_R T$ into $\mathbf{G}_m\times T$, $\mathbf{G}_m$ denoting the multiplicative group).

Examples. (a) Let $G=\mathbf{Z}/m\mathbf{Z}$ be the cyclic group of order n (as in Example (a) of (1.1)). Then $G'=\boldsymbol{\mu}_m$.

(b) If $G=G_{a,b}$ (Example (c) of (1.1)), then $G'=G_{b,a}$.

(1.3). Short exact sequences

A sequence

$$0\to G'\xrightarrow{i} G\xrightarrow{j} G''\to 0 \tag{1}$$

of finite R-groups is called *exact* if i is a closed immersion which identifies G' with the kernel of j (in the sense of categories), whereas j is faithfully flat. If j is given, it is easy to get G' (it is the inverse image of the unit section of G''). Given i, one can construct G''. This is more delicate (see [4], Exposé V and VI_B or [7]).

If (1) is exact, then we have for the orders m, m', m'' of G, G', G'' the relation $m=m'm''$. This follows from the fact (proved loc. cit.) that the graph of the equivalence relation in $G\times_R G$ defined by G' is isomorphic to $G\times_{G''} G$.

Finally, the dual of an exact sequence (1) is also exact.

(1.4). Connected and étale groups

In this section we suppose R is a *complete noetherian local* ring. If G is a group of finite order over R, there is a canonical exact sequence

$$0\to G^0 \xrightarrow{i} G \xrightarrow{j} G^{et}\to 0,$$

where G^0 is *connected* and G^{et} is *étale* over R. If the corresponding affine rings are A^0, A, and A^{et}, then A is a product of local R-algebras, and A^0 is the local quotient of A through which the map $\varepsilon: A\to R$ factors, while A^{et} is the maximal étale subalgebra of A. The map i is an open and closed immersion, and G^0 is the maximal connected subgroup of G. For varying G, the functors $G\mapsto G^0$, and $G\mapsto G^{et}$ are *exact*.

G is *connected* if $G^0=G$. In that case, the order of G is a power of the characteristic exponent of the residue field k of R, i.e., is 1 if $\operatorname{char}(k)=0$, and is a power of p if $\operatorname{char} k=p>0$. This follows from the theory of finite group schemes over k (or even over $\bar{k}$).

G is *étale* if $G=G^{et}$. The functor $G\mapsto G(\bar{k})$ is an equivalence of the category of étale R-groups of finite order and finite π-modules on which π operates continuously, where $\pi=\operatorname{Gal}(\bar{k}/k)$ is the *fundamental group* of R. Given such a π-module Γ, the étale finite R-group Γ corresponding to it is given by $\Gamma=\operatorname{Spec} A$, where A is the ring of all functions $\Gamma\to R_{et}$ which commute with π, and where R_{et} is a "maximal local étale integral extension" of R (i.e., a maximal unramified extension of R in the old terminology, if R is a complete discrete valuation ring), and where π operates on R_{et} in the unique way compatible with its operation on the residue field extension k_{et}/k (the residue field k_{et} of R_{et} being a separable algebraic closure of k). For general (not necessarily étale) G, we have $G^{et}=G(\bar{k})$.

§ 2. p-divisible groups

(2.1). Definition

Let p be a prime number, and h an integer $\geqslant 0$. A *p-divisible group G over R of height h* is an inductive system

$$G=(G_\nu, i_\nu),\qquad \nu\geqslant 0,$$

where

(i) G_ν is a finite group scheme over R of order $p^{\nu h}$;

(ii) for each $\nu\geqslant 0$,

$$0\to G_\nu \xrightarrow{i_\nu} G_{\nu+1} \xrightarrow{p^\nu} G_{\nu+1}$$

is exact (i.e., G_ν can be identified via i_ν with the kernel of multiplication by p^ν in $G_{\nu+1}$).

These axioms for ordinary abelian groups would imply

$$G_\nu\cong(\mathbf{Z}/p^\nu\mathbf{Z})^h \quad\text{and}\quad G=\varinjlim G_\nu=(\mathbf{Q}_p/\mathbf{Z}_p)^h.$$

A *homomorphism* $f: G\to H$ of p-divisible groups is defined in the obvious way: if $G=(G_\nu, i_\nu)$, $H=(H_\nu, i_\nu)$ then f is a system of homomorphisms $f_\nu: G_\nu\to H_\nu$ of R-groups, which is such that $i_\nu\cdot f_\nu=f_{\nu+1}\cdot i_\nu$ for all $\nu\geqslant 1$.

By iteration, one gets from the i_ν closed immersions

$$i_{\nu,\mu}: G_\nu\to G_{\mu+\nu}$$

for all μ, $\nu\geqslant 0$, which identify G_ν with the kernel of multiplication by p^ν in all $G_{\mu+\nu}$. It follows that the homomorphism

$$p^\mu: G_{\mu+\nu}\to G_{\mu+\nu}$$

can be factored through G_ν and then a consideration of orders shows that we have an exact sequence

$$0\to G_\mu \xrightarrow{i_{\mu,\nu}} G_{\mu+\nu} \xrightarrow{j_{\mu,\nu}} G_\nu\to 0, \tag{2}$$

where $j_{\mu,\nu}$ is the unique homomorphism such that $i_{\nu,\mu}\cdot j_{\mu,\nu}=p^\mu$.

Examples. (a) Let X be an abelian scheme over R of dimension d. Let X_n be the kernel of multiplication by n. Then (X_{p^ν}, i_ν) (i_ν denoting the obvious inclusion) is a p-divisible group $X(p)$, with height $h=2d$.

(b) The same construction can be performed for other groups over R. If one takes $X=\mathbf{G}_m$, the resulting p-divisible group is $\mathbf{G}_m(p)=(\boldsymbol{\mu}_{p^\nu}, i_\nu)$. Its height is 1.

Question: Are there any p-divisible groups over $\mathbf{Z}$ other than products of powers of $\mathbf{G}_m(p)$ and of $\mathbf{Q}_p/\mathbf{Z}_p$?

(2.2). Relations with formal Lie groups

In this section we assume R complete, noetherian, local, with residue field k of characteristic $p>0$. For our present purposes, an *n-dimensional formal Lie group Γ over R* can be defined as a suitable homomorphism of the ring $\mathscr{A}=R[[X_1,\cdots,X_n]]$ of formal power series over R in n variables X_i into $\mathscr{A}\hat{\otimes}_R\mathscr{A}$, the ring of formal power series in $2n$ variables Y_i, Z_j. Such a homomorphism can be described by a family $f(Y,Z)=(f_i(Y,Z))$, of n power series in $2n$ variables, f_i being the image of X_i.

The following axioms are imposed

(i) $X=f(X,o)=f(o,X)$,

(ii) $f(X,f(Y,Z))=f(f(X,Y),Z)$,

(iii) $f(X,Y)=f(Y,X)$, (since we consider only commutative groups).

We write $X*Y=f(X,Y)$. It follows from the axioms that $X*Y=X+Y+$ terms in higher powers of the variables.

Put $\psi(X)=X*\cdots*X$ (p times). This determines a homomorphism $\psi:\mathscr{A}\to\mathscr{A}$, which corresponds to multiplication by p in Γ. Γ is said to be *divisible* if $p:\Gamma\to\Gamma$ is an isogeny. This means that ψ makes $\mathscr{A}$ into a *free* module of finite rank over itself.

We can then repeat the construction of Example (a) in (2.1), obtaining a p-divisible group $\Gamma(p)=(\Gamma_{p^\nu},i_\nu)$ of height h over R, where p^h is the degree of the isogeny $p:\Gamma\to\Gamma$. (This degree is a power of p because it is equal to the order of the finite R-group $\Gamma_p=\mathrm{Ker}\,p$, which is connected (see 1.4).) More generally, for arbitrary ν, we have $(\Gamma(p))_\nu=\Gamma_{p^\nu}=\mathrm{Spec}\,A_\nu$, where $A_\nu=\mathscr{A}/J_\nu$, and where $J_\nu=\psi^\nu(I)\,\mathscr{A}$ is the ideal in $\mathscr{A}$ generated by the elements $\psi^\nu(X_i)$, $1\leqslant i\leqslant n$. (Here $I=J_0$ denotes the ideal generated by the variables X_i). Clearly, each A_ν is a local ring; hence $\Gamma(p)$ is a *connected* p-divisible group (i.e., each $\Gamma(p)_\nu$ is connected).

Proposition 1. *Let R be a complete noetherian local ring whose residue field k is of characteristic $p>0$. Then $\Gamma\mapsto\Gamma(p)$ is an equivalence between the category of divisible commutative formal Lie groups over R and the category of connected p-divisible groups over R.*

Remark. We can only sketch the proof here, omitting many technical details. The techniques involved are amply covered in Gabriel's exposés VII_A and VII_B of [4].

Let Γ be a divisible formal group over R. Let $\mathfrak{m}$ be the maximal ideal of R so that, with the previous notations, $\mathfrak{m}\mathscr{A}+I=M$, say, is the maximal ideal of $\mathscr{A}$.

Lemma 0. *The ideals $\mathfrak{m}^\nu\mathscr{A}+J_\nu$ constitute a fundamental system of neighborhoods of 0 in the M-adic topology of $\mathscr{A}$.*

Indeed, $\mathscr{A}/(\mathfrak{m}^\nu A+J_\nu)=A_\nu/\mathfrak{m}^\nu A_\nu$ is an Artin ring, so the ideals in question are M-adically open. On the other hand, they are arbitrarily small, because we have

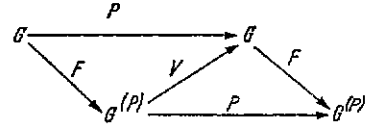
$$\psi(X_i)=pX_i+(\text{terms of degree}\geqslant 2),$$

hence $\psi(I)\subset pI+I^2\subset(\mathfrak{m}\mathscr{A}+I)\,I=MI$, and consequently, by induction on ν, we have $J_\nu=\psi^\nu(I)\,\mathscr{A}\subset M^\nu I$.

From Lemma 0 it follows that the map $\mathscr{A}\to\varprojlim(\mathscr{A}/J_\nu)=\varprojlim(A_\nu)$ is bijective, because $\mathscr{A}$ is M-adically complete. From this bijectivity it is easy to see that the functor $\Gamma\to\Gamma(p)$ is fully faithful.

To complete the proof of Prop. 1 we must show that any given connected p-divisible group G over R is isomorphic to some $\Gamma(p)$. Let $G=(G_\nu,i_\nu)$ and $G_\nu=\mathrm{Spec}\,(A_\nu)$. The inclusions $i_\nu:G_\nu\to G_{\nu+1}$ make (A_ν) into a projective system. Put $A=\varprojlim A_\nu$. The group law on G defines a homomorphism $A\to A\hat{\otimes}_R A$, which will have the required properties for a formal Lie group, once we know that A is isomorphic to $R[[X_1,\cdots,X_n]]$ for some n. Then it also follows easily that the formal Lie group Γ is divisible and that G is isomorphic to $\Gamma(p)$.

To prove that A is an algebra of formal power series over R, one first observes that A is flat over R. (Indeed the R-module A is isomorphic to a countable direct product of copies of R, because the A_ν are free of finite type over R, and the maps $A_{\nu+1}\to A_\nu$ surjective.) This being so, one is reduced by standard procedures to the case in which $R=k$ is a field of characteristic $p>0$. In that case, the injective limits of finite commutative group schemes of p-power order over k form an abelian category, and a p-divisible group over k is just an object in that category on which p is surjective with finite kernel. There is an exact functor $G\mapsto G^{(p)}$ from that category to itself which preserves the order of the finite objects, and there are homomorphisms of functors F (Frobenius) and V (Verschiebung) such that the following diagram is commutative for any G in the category:



(3)

(See [3], p. 98, or [4], exposé VII, or [6], p. 18, 19.) If G is p-divisible of height h, then so is $G^{(p)}$, and the diagram shows then that F and V are surjective, with finite kernels of order $\leqslant p^h$.

Suppose now that G is the connected p-divisible group over k we were considering before this general discussion. For each v, let H_v be the kernel of $F^v: G \to G^{(p^v)}$. Then we have $H_v \subset G_v$, and also $G_v \subset H_N$ for sufficiently large N (depending on v), because G_v is finite and connected. Thus, we have $A = \varprojlim A_v = \varprojlim B_v$, where $H_v = \operatorname{Spec} B_v$. Let I_v be the augmentation (i.e., the maximal) ideal of B_v, let $I = \varprojlim I_v$ be the augmentation ideal of A, and let $x_1, \cdots, x_n$ be elements of I whose images form a k-base for I_1/I_1^2. Then the images of the x_i in B_v generate I_v for each v, because $I_v/I_v^2 \to I_1/I_1^2$ is bijective. (Since H_1 is the kernel of F in H_v, the kernel of $I_v \to I_1$ is generated by the p-th powers of the elements of I_v, so that kernel is in I_v^2.) Now consider the homomorphisms $u_v: k[X_1, \cdots, X_n] \to B_v$ which send X_i to the image of x_i in B_v. These are surjective, by the above; on the other hand, $\operatorname{Ker} u_v$ contains the elements $X_i^{p^v}$ because F^v kills H_v. But $\operatorname{rank}(B_v) = (\operatorname{rank}(B_1))^v$, since F is *surjective*, and $\operatorname{rank}(B_1) = p^n$, by the structure theory of finite groups killed by F. Since the ideal $(X_1^{p^v}, \cdots, X_n^{p^v})$ is of codimension p^{nv} in $k[X]$, it follows that that ideal is the kernel of u_v, and hence that the u_v induce an isomorphism $u: k[[X_1, \cdots, X_n]] \xrightarrow{\sim} A$. This completes our sketch of the proof of Proposition 1.

If $G = (G_v, i_v)$ is now any p-divisible group over our complete noetherian local R, the connected components G_v^0 determine a *connected* p-divisible group G^0. From the exact sequences

$$0 \to G_v^0 \to G_v \to G_v^{et} \to 0$$

one gets an exact sequence

$$0 \to G^0 \to G \to G^{et} \to 0, \tag{4}$$

where G^{et} is an *étale* p-divisible group. The dimension, n, of the formal Lie group corresponding to G^0 is, by definition, the *dimension* of G.

Proposition 2. *The discriminant ideal of A_v over R is generated by $p^{nvp^{hv}}$, where $h = ht(G)$ and $n = \dim(G)$.*

In general, for a finite group $H = \operatorname{Spec} B$ over R, let $\operatorname{disc}(H)$ denote the discriminant ideal of B over R. If $0 \to H' \to H \to H'' \to 0$ is an exact sequence of finite groups over R (cf. 1.3) of orders m', m, and m'', then by the transitivity of discriminants one proves easily that $\operatorname{disc}(H) = (\operatorname{disc} H')^{m''} (\operatorname{disc} H'')^{m'}$. This fact, together with the fact that $\operatorname{disc}(H) = 1$ if H is étale, allows us, via (4), to reduce the case of an arbitrary G to that of a connected $G \simeq \Gamma(p)$. As in the proof of Prop. 1 above we have then $A_v = \mathscr{A}/J_v$. Consider $\mathscr{A}$ as a free module of rank p^{vh} over itself by means of $\varphi = \psi^v$. We change the notation, and consider $\mathscr{A}$ as an algebra (via φ) over another copy $\mathscr{A}'$ of $\mathscr{A}$. Denoting by I' the augmentation ideal in $\mathscr{A}'$ (generated by the X_i'), we have $A_v \simeq \mathscr{A}/I'\mathscr{A}$, so it suffices to prove that the discriminant ideal of $\mathscr{A}$ over $\mathscr{A}'$ is generated by the desired power of p.

To do this, consider the modules of formal differentials Ω and Ω' of $\mathscr{A}$, resp. $\mathscr{A}'$. They are free modules over $\mathscr{A}$ (resp. $\mathscr{A}'$) generated by the differentials of the variables dX_i, resp. dX_i', $1 \leqslant i \leqslant n$. The homomorphism $\varphi: \mathscr{A}' \to \mathscr{A}$ induces an $\mathscr{A}'$-linear map $d\varphi: \Omega' \to \Omega$. Choosing bases in Ω, resp. Ω', we get a basis element θ, resp. θ', of $\Lambda^n\Omega$, resp. $\Lambda^n\Omega'$. Let $d\varphi(\theta') = a\theta$, with $a \in \mathscr{A}$. Then one has

Lemma 1. *The discriminant ideal of $\mathscr{A}$ over $\mathscr{A}'$ is generated by $N_{\mathscr{A}/\mathscr{A}'}(a)$.*

Granting this lemma, the proof of Prop. 2 is finished as follows. Choose a basis (ω_i) of Ω consisting of translation-invariant differentials, i.e., differentials such that if $\mu: \mathscr{A} \to \mathscr{A} \hat{\otimes}_R \mathscr{A}$ defines the formal group structure $d\mu: \Omega \to \Omega \oplus \Omega$ satisfies $d\mu(\omega_i) = \omega_i \oplus \omega_i$. Using the corresponding basis (ω_i') in the copy Ω' of Ω we have, by the definition of φ as arising from the homomorphism $p^v: \Gamma \to \Gamma$, that $d\varphi(\omega_i') = p^v \omega_i$, whence $a = p^{vn}$. Proposition 2 then follows by Lemma 1.

As to a proof of that lemma, it can be based on the existence of a trace map $\operatorname{Tr}: \Lambda^n\Omega \to \Lambda^n\Omega'$ with the following properties:

(i) Tr is $\mathscr{A}'$-linear.

(ii) The map $a \mapsto (\theta \mapsto \operatorname{Tr}(a\theta))$ establishes an isomorphism of $\mathscr{A}'$-modules

$$\mathscr{A} \xrightarrow{\sim} \operatorname{Hom}_{\mathscr{A}'}(\Lambda^n\Omega, \Lambda^n\Omega').$$

(iii) If $\theta \in \Omega'$ and $a \in \mathscr{A}$, then

$$\operatorname{Tr}(a \cdot d\varphi(\theta)) = (\operatorname{Tr}_{\mathscr{A}/\mathscr{A}'}(a))\,\theta.$$

Such a trace map exists whenever $\mathscr{A} \simeq \mathscr{A}' \simeq R[[X_1, \ldots, X_n]]$ and $\varphi: \mathscr{A}' \to \mathscr{A}$ is an R-algebra homomorphism making $\mathscr{A}$ a free $\mathscr{A}'$-module of finite rank; see for example Hartshorne's notes on *Residues and Duality*, Springer lecture notes 20, 1966, at least for the corresponding "non-formal" situation.

(2.3). Duality for p-divisible groups

Let $G=(G_\nu, i_\nu)$ be a p-divisible group over R. For each ν, let G'_ν be the Cartier dual of G (cf. 1.2). The exact sequences (2) in (2.1) with $\mu=1$ shows that we have injective homomorphisms

$$i'_\nu : G'_\nu \to G'_{\nu+1},$$

where i_ν is the dual of the map $G_{\nu+1}\to G_\nu$ induced by multiplication by p. It is easy to check that the system $G'=(G'_\nu, i'_\nu)$ satisfies the axioms of (2.1), and is therefore a p-divisible group, called the *dual of* G. Clearly, G' and G have the same height. Of course, this notion of dual makes sense over any base ring (or prescheme) R. In case R is complete local noetherian with residue characteristic p, as in 2.2, so that the dimension of G is defined (cf. the lines before Prop. 2), we have the following all-important

Proposition 3. *Let n and n' be the dimension of G and its dual G'. Then $n+n'=h$, the height of G and G'.*

The dimension and height of G do not change if we reduce G mod the maximal ideal of R. Hence we are reduced at once to the case in which $R=k$, a field of characteristic p. From diagram (3) we get an exact sequence

$$0 \to \operatorname{Ker} F \to \operatorname{Ker} p \to \operatorname{Ker} V \to 0.$$

Now $\operatorname{Ker} p = G_1$ has order p^h, and $\operatorname{Ker} F$ has order p^n. (F is injective on G^{et}, so the kernel of F in G is the same as that of F in the connected component G^0. Viewing G^0 as a formal Lie group on n parameters, we see that the order of $\operatorname{Ker} F$ is p^n, as remarked in the proof of Prop. 1.) Since F and V are dual with respect to Cartier duality one checks that $\operatorname{Ker} V$ is the Cartier dual of the Cokernel of the map $F: G'_\nu \to G'^{(p)}_1 = (G_1^{(p)})'$, and consequently $\operatorname{Ker} V$ has order $p^{n'}$. Now the assertion follows from the multiplicativity of orders in an exact sequence.

Examples. a) The p-divisible group $\mathbf{G}_m(p)$ has $h=n=1$, and is dual to the étale p-divisible group $\mathbf{Q}_p/\mathbf{Z}_p$ which has $h=1$, $n=0$.

b) Let X be an abelian scheme of dimension n over R. If the dual abelian scheme X' exists, then we have $(X(p))' \simeq X'(p)$. Both $X(p)$ and $X'(p)$ have height $2n$ and dimension n. The connected component $X(p)^0$ of $X(p)$ is the formal completion of X along the zero section, and can have any height between n and $2n$. For example, if X is an elliptic curve ($n=1$), then the height of $X(p)^0$ is 1 or 2 according as the "Hasse invariant" of $X(p)$ is non-zero or zero.

(2.4). Points; the Galois modules $\Phi(G)$ and $T(G)$

Let R be a complete discrete valuation ring, with residue field $k=R/\mathfrak{m}$ of characteristic $p>0$, and let K be the field of fractions of R (very soon we shall assume k perfect and K of characteristic 0). Let L be the completion of a (possibly infinite) algebraic extension of K and let S be the ring of integers in L. Thus S is a complete rank 1 valuation ring, but the valuation on S may not be discrete.

Let G be a p-divisible group over R. We define the *group $G(S)$ of points of G with values in S* by

$$G(S) = \varprojlim_i G(S/\mathfrak{m}^i S),$$

where $\mathfrak{m}$ is the maximal ideal of R, and where

$$G(S/\mathfrak{m}^i S) = \varinjlim_\nu G_\nu(S/\mathfrak{m}^i S).$$

Clearly, $G(S)$ is a $\mathbf{Z}_p$-module. From the definition of p-divisible groups, $G_\nu(S/\mathfrak{m}^i S)$ is the kernel of multiplication by p^ν in $G(S/\mathfrak{m}^i S)$. Thus the kernel of multiplication by p^ν in $G(S)$ is $\varprojlim_i G_\nu(S/\mathfrak{m}^i S) \simeq G_\nu(S)$, and the torsion subgroup of $G(S)$ is given by

$$G(S)_{\text{tors}} \simeq \varinjlim_\nu G_\nu(S).$$

If G is étale over R, then the maps $G_\nu(S/\mathfrak{m}^{i+1}S) \to G_\nu(S/\mathfrak{m}^i S)$ are bijective for all i, and consequently *$G(S)$ is a torsion group if G is étale.*

In general, if $G_\nu = \operatorname{Spec} A_\nu$ and $A = \varprojlim_\nu A_\nu$, and $A_\nu \simeq A/J_\nu$ as in § 2, then a point $x \in G(S)$ can be identified with a homomorphism $A \to S$ which is continuous with respect to the valuation topology in S and the topology defined by the ideals $\mathfrak{m}^i A + J_\nu$ in A. In particular, if G is connected, corresponding to a formal Lie group Γ, so that $A \simeq R[[X_1, \ldots, X_n]]$, then it follows from the above remark and Lemma 0 that $G(S)$ is the group of points $x=(x_1, \ldots, x_n)$ of Γ with coordinates x_i lying in the maximal ideal of S. Thus, *if G is connected, then $G(S)$ is an analytic group over L.*

Now consider the exact sequence (4), and let A^{et} and A^0 denote the algebras of G^{et} and G^0.

Proposition 4. *If the residue field k of R is perfect, then the map $G \to G^{et}$ has a formal section, and consequently the sequence*

$$0 \to G^0(S) \to G(S) \to G^{et}(S) \to 0$$

is exact.

Proof. If $R=k$, then the exact sequence (4) splits canonically, and we have $A \simeq A^0 \hat{\otimes}_R A^{et} \simeq A^{et}[[X_1, \ldots, X_n]]$ in that case. By flatness we conclude $A \simeq A^{et}[[X]]$ in the general case.

Corollary 1. *If $x \in G(S)$, then there exists a finite extension field L' of L and an element $Y \in G(S')$, where S' is the ring of integers in L', such that $py=x$.*

Indeed, by Prop. 4, it suffices to prove this for G^{et} and G^0 separately. For G^0 it follows from the fact that the map $p: G^0 \to G^0$ makes A^0 a free A^0-module of finite rank (cf. § 2). For G^{et} we are reduced to a statement over the residue field, and the result follows because the maps $G_{\nu+1} \to G_\nu$ induced by multiplication by p are surjective.

Corollary 2. *If L is algebraically closed, then $G(S)$ is divisible.*

From now on we suppose that k is perfect and the *characteristic of K is* 0. This characteristic 0 assumption will be absolutely crucial in all that follows, because (1) there is then a logarithm map which will show that $G(S)$ is locally isomorphic to L^n, where $n=\dim G$, and (2) the $G_\nu \times_R K$ are then automatically étale, so we will know that $G_\nu(S)$ (which is isomorphic to $G_\nu(L)$ since G_ν is finite and flat over R) is isomorphic to $(\mathbf{Z}/p^\nu\mathbf{Z})^h$ for sufficiently large L (depending on ν).

The logarithm. The tangent space t_G of G at the origin is, by definition, the tangent space of the formal Lie group Γ corresponding to G^0 at the origin. We write $t_G(L)$ to denote its points with coordinates in L. Such a point is an R-linear map $\tau: A^0 \to L$ such that $\tau(fg)=f(o)\,\tau(g)+g(o)\,\tau(f)$ for all $f, g \in A^0 \simeq R[[X_1, \ldots, X_n]]$, or, equivalently, is simply an R-linear map of $I^0/(I^0)^2$ into L, where $I^0=(X_1, \ldots, X_n)$ is the augmentation ideal in A^0 (namely the map induced by the restriction of τ to I^0). Thus, $t_G(L)$ is a vector space of dimension $n=\dim G$ over L. The logarithm map: $\log: G(S) \to t_G(L)$ is defined as follows:

$$(\log x)(f) = \lim_{i \to \infty} \left(\frac{f(p^i x) - f(o)}{p^i} \right),$$

for $x \in G(S)$ and $f \in A^0$; note that for large i we will have $p^i x \in G^0(S)$, because $G^{et}(S)$ is a torsion group. Alternatively, we can identify $I^0/(I^0)^2$ with the space of invariant differential forms ω on Γ, and define, for $x \in G^0(S)$ which is all that really matters,

$$(\log x)(\omega) = \Omega(x),$$

where $\Omega(X) \in K[[X_1, \ldots, X_n]]$ is such that $\Omega(0)=0$ and $d\Omega=\omega$, see SERRE [12]. Using either of these definitions of log, one proves easily that it is a $\mathbf{Z}_p$-homomorphism, and a local isomorphism. More precisely, that if $c^{p-1}<|p|$, the logarithm gives an isomorphism between the group of points $x=(x_i)$ in $G^0(S)$ such that $|x_i| \leqslant c$ for all i and the group of points $\tau \in t_G(L)$ such that $|\tau(X_i)| \leqslant c$ for all i. From these facts it follows that the kernel of log is the torsion subgroup of $G(S)$, and that its cokernel is a torsion group. Thus, the log induces an *isomorphism*

$$G(S) \underset{\mathbf{Z}_p}{\otimes} \mathbf{Q}_p \xrightarrow{\sim} t_G(L).$$

It also follows that $\log G(S)$ is contained in a finitely generated S-submodule of $t_G(L)$ if the valuation on S is discrete, whereas $\log G(S)=t_G(L)$ if L is algebraically closed.

Examples. 1.) If $G=\mathbf{G}_m(p)$, then $G(S)$ is the group of units congruent to 1 in S, $t_G(L)$ is L, and the logarithm is the ordinary p-adic logarithm.

2.) If X is an abelian scheme over R, and $G=X(p)$, then we can identify $G(S)$ with the subgroup of $X(S)$ consisting of the points x whose reduction mod the maximal ideal of S is of finite p-power order, $G^0(S)$ being identified with the kernel of the reduction map. The logarithm is then the map which has been studied by LUTZ (for elliptic curves) and by MATTUCK in general.

The Galois modules Φ and T. Let $\bar{K}$ be the algebraic closure of K, and $\mathcal{G}=\mathrm{Gal}(\bar{K}/K)$. Put

$$\Phi(G) = \varinjlim_{\nu} G_\nu(\bar{K}), \quad \text{with respect to the maps} \quad i_\nu: G_\nu \subsetneq G_{\nu+1}.$$

$$T(G) = \varprojlim_{\nu} G_\nu(\bar{K}), \quad \text{with respect to the maps} \quad j_\nu: G_{\nu+1} \to G_\nu.$$

Since $\mathrm{char}(K)=0$, the $G_\nu \otimes_R K$ are étale, and it follows from the definition of p-divisible groups that $\Phi(G)$ and $T(G)$ are $\mathbf{Z}_p$-modules isomorphic respectively, to $(\mathbf{Q}_p/\mathbf{Z}_p)^h$ and to $\mathbf{Z}_p^h$, where $h=\mathrm{height}(G)$, on which $\mathcal{G}$ acts continuously. We have canonical isomorphisms:

$$\Phi(G) \simeq T(G) \underset{\mathbf{Z}_p}{\otimes} (\mathbf{Q}_p/\mathbf{Z}_p) \quad \text{and} \quad T(G) \simeq \mathrm{Hom}_{\mathbf{Z}_p}(\mathbf{Q}_p/\mathbf{Z}_p, \Phi(G)),$$

so knowledge of $\Phi(G)$ is equivalent to that of $T(G)$, and knowledge of either is equivalent to knowledge of the *general fiber* $G\otimes_R K$ of the p-divisible group G.

In the notation of the preceding paragraphs, the map $G_v(S)\to G_v(L)$ is bijective, so that, $\Phi(G)$ is the torsion subgroup of $G(S)$ if L is the completion of $\bar{K}$.

Examples. 1.) If $G=\mathbf{G}_m(p)$, then $\Phi(G)$ is the group of roots of unity of p[illegible] power order in $\bar{K}$.

2.) If X is an abelian scheme of dimension n over R, and $G=X(p)$, then $T(G)=T_p(X)$, the p-adic representation space of rank $h=2n$ introduced by WEIL.

§ 3. The completion of the algebraic closure of K

R denotes a discrete valuation ring, which is complete, of characteristic 0. Its residue field k is assumed to be perfect of characteristic $p>0$. Let K denote the quotient field of R, $\bar{K}$ its algebraic closure and C the completion of $\bar{K}$. C is known to be algebraically closed (see [1], p. 42). The absolute value on K is canonically extended to C. Let π be a uniformizing element of K. For $x\in C$ we define its order $v(x)$ by

$$|x| = |\pi|^{v(x)},$$

we put $v(p)=e$.

If I is an ideal in some finite extension of K, $v(I)$ is defined in the obvious way. The relative different of a finite extension M/L is denoted by $\mathfrak{d}_{M/L}$.

In the results of this section several constants will appear. We often will denote them indiscriminately by the same letter.

(3.1). Study of certain totally ramified extensions.

Let K_∞ be an infinite Galois extension of K which is totally ramified with group $\mathscr{G}\simeq\mathbf{Z}_p$. Let K_n be the subfield of K_∞ which corresponds to the closed subgroup $\mathscr{G}(n)=p^n\mathbf{Z}_p$. Then K_n/K is cyclic of degree p^n.

Proposition 5. *There is a constant c such that*

$$v(\mathfrak{d}_{K_n/K}) = en + c + p^{-n}a_n,$$

where a_n is bounded.

This follows from standard facts about higher ramification, together with local class field theory.

We use the higher ramification groups $\mathscr{G}^v$, with the "upper numbering", which is compatible with passage to quotients ([8], p. 119, or [2], p. 81). Suppose that $\mathscr{G}^v=\mathscr{G}(i)$ for $v_i<v\leqslant v_{i+1}$. We then have $v_{n+1}=v_n+e$ for large n (recall that $e=v(p)$). This follows from local class field theory, more precisely from the description of the images of the $\mathscr{G}^v$ under the reciprocity mapping. (See [8], p. 235, Cor. 3, for the case of a finite k; see [9] for the case of an algebraically closed k, to which the case of arbitrary perfect k can be reduced by passage to the completion of the maximal unramified extension of K; see also the Berkeley Ph. D. thesis of B. F. WYMAN (June 1966).) Put $\mathfrak{d}_n=\mathfrak{d}_{K_n/K}$. A well-known formula ([8], p. 109) then gives ($o(\mathscr{G})$ denoting the order of a group $\mathscr{G}$)

$$v(\mathfrak{d}_n) = \int_{-1}^{\infty} \left(1 - o\left(\mathrm{Gal}\,(K_n/K)^v\right)^{-1}\right) dv.$$

Now $\mathrm{Gal}\,(K_n/K)^v=\mathscr{G}^v\mathscr{G}(n)$, whence

$$o\left(\mathrm{Gal}\,(K_n/K)^v\right) = p^{n-i} \quad \text{if} \quad v_i < v \leqslant v_{i+1}, \quad \text{with} \quad i \leqslant n,$$
$$= 1 \quad \text{otherwise}.$$

The assertion then follows easily.

Corollary 1. *$v(\mathfrak{d}_{K_{n+1}/K_n})=e+p^{-n}b_n$, where b_n is bounded.*

Corollary 2. *There is a constant a (independent of n) such that for $x\in K_{n+1}$ we have*

$$|\mathrm{Tr}_{K_{n+1}/K_n}(x)| \leqslant |p|^{1-ap^{-n}}|x|.$$

Let R_n be the ring of integers of K_n and $\mathfrak{m}_n$ its maximal ideal. Let $\mathfrak{d}_{K_{n+1}/K_n}=\mathfrak{m}_{n+1}^d$. Then

$$\mathrm{Tr}_{K_{n+1}/K_n}(\mathfrak{m}_{n+1}^i) = \mathfrak{m}_n^j,$$

where $j=\left[\dfrac{i+d}{p}\right]$ (see [8], p. 91, Lemma 4). This implies the asserted inequality.

Corollary 3. *There is a constant c (independent of n) such that for $x\in K_n$ we have*

$$|\mathrm{Tr}_{K_n/K}(x)| \leqslant |p|^{n-c}|x|.$$

Let σ denote a generator of the group $\mathscr{G}$.

Lemma 2. *There exists a constant $c>0$ (independent of n) such that for $x\in K_{n+1}$ we have*

$$|x - p^{-1}\,\mathrm{Tr}_{K_{n+1}/K_n}(x)| \leqslant c\,|\sigma^{p^n}x - x|.$$

Proof. Let $\tau=\sigma^{p^n}$. Then

$$px-\mathrm{Tr}_{K_{n+1}/K_n}(x)=px-\sum_{i=0}^{p-1}\tau^i x=$$
$$\sum_{i=0}^{p-1}(1-\tau^i)\,x=\sum_{i=1}^{p-1}(1+\tau+\cdots+\tau^{i-1})(1-\tau)\,x.$$

Hence

$$|px-\mathrm{Tr}_{K_{n+1}/K_n}(x)|\leqslant|(1-\tau)\,x|,$$

and we may take $c=|p|^{-1}$.

Now define a K-linear function t on K_∞ with values in K as follows: For $x\in K_n$, put

$$t(x)=p^{-n}\,\mathrm{Tr}_{K_n/K}(x).$$

This is independent of the choice of n.

Proposition 6. *There exists a constant $d>0$ such that we have for all $x\in K_\infty$,*

$$|x-t(x)|\leqslant d\,|\sigma x-x|.$$

We prove by induction on n an inequality

$$|x-t(x)|\leqslant c_n|\sigma x-x|\quad\text{if}\quad x\in K_n,\tag{*}$$

with

$$c_{n+1}=|p|^{-ap^{-n}}c_n,$$

where a is a constant >0. This will imply the assertion. We may take c_1 equal to the c of Lemma 2. Then we have for $x\in K_{n+1}$, assuming (*) to be true,

$$|\mathrm{Tr}_{K_{n+1}/K_n}(x)-pt(x)|\leqslant c_n|\sigma\,\mathrm{Tr}_{K_{n+1}/K_n}(x)-\mathrm{Tr}_{K_{n+1}/K_n}(x)|$$
$$=c_n|\mathrm{Tr}_{K_{n+1}/K_n}(\sigma x-x)|\leqslant c_n|p|^{1-ap^{-n}}|\sigma x-x|,$$

by Cor. 2 to Proposition 5. By Lemma 2 we have then

$$|x-t(x)|\leqslant\mathrm{Max}\,(|x-p^{-1}\,\mathrm{Tr}_{K_{n+1}/K_n}(x)|,\ \ |p|^{-ap^{-n}}c_n|\sigma x-x|)$$
$$\leqslant\mathrm{Max}\,(c_1,|p|^{-ap^{-n}}c_n)\,|\sigma x-x|=|p|^{-ap^{-n}}c_n|\sigma x-x|,$$

which establishes (*) for $(n+1)$.

Remark. From the proof we see that if we take K_n as a groundfield instead of K we have a corresponding inequality with *the same constant d.*

Next let X be the completion of K_∞. This is a Banach space over K, on which $\mathscr{G}$ acts continuously. The preceding results will enable us to get some information about the $\mathscr{G}$-space X.

By Prop. 6 (or by Cor. 3 of Prop. 5) the linear operator t is continuous on K_∞ and therefore extends to X by continuity. We have $t(X)=K$ because K is complete; let X_0 be the kernel of t on X, a closed subspace of X.

Proposition 7. a) *X is the direct sum of K and X_0.*

b) *The operator $\sigma-1$ annihilates K, and is bijective, with a continuous inverse, on X_0.*

c) *Let λ be a unit in K which is $\equiv 1\ (\mathrm{mod}\,\pi)$ and which is not a root of unity. Then $\sigma-\lambda$ is bijective, with a continuous inverse, on X.*

Proof. (a) Since t is *idempotent*, X is the direct sum of its range and its kernel.

(b) For each n, let $K_{n,0}=K_n\cap X_0$ be the subspace of K_n consisting of the elements whose trace to K is 0, and let $K_{\infty,0}=\bigcup_{n=0}^{\infty}K_{n,0}$. We have $K_n=K\oplus K_{n,0}$, direct sum, for $0\leqslant n\leqslant\infty$, and X_0 is the closure of $K_{\infty,0}$ in X. The operator $\sigma-1$ is injective, hence bijective, on each of the finite dimensional spaces $K_{n,0}$, for $n<\infty$, and is therefore bijective on their union $K_{\infty,0}$; let ϱ be its inverse. By Prop. 6 we have $|\varrho y|\leqslant d|y|$ for each $y=(\sigma-1)\,x$ in $K_{\infty,0}$. Hence ϱ extends by continuity to X_0, and this extension is a continuous inverse for $\sigma-1$ on X_0.

(c) Since $\sigma-\lambda$ is obviously bijective on K for $\lambda\neq 1$, we can, by (a), restrict our attention to its action on X_0. As operators on X_0 we have

$$\varrho(\sigma-\lambda)=\varrho((\sigma-1)-(\lambda-1))=1-(\lambda-1)\,\varrho.\tag{*}$$

If $|\lambda-1|\,d<1$ with d as in (b), we have $|(\lambda-1)\,\varrho(y)|<|y|$ for all $y\in X_0$ and consequently $1-(\lambda-1)\,\varrho$ is an automorphism of X_0, its inverse being given by a geometric series, and consequently, by (*), $\sigma-\lambda$ has a continuous inverse on X_0. If $|\lambda-1|\,d\geqslant 1$, we replace σ by σ^{p^n}, and λ by λ^{p^n}, where n is so large that $|\lambda^{p^n}-1|\,d<1$. We then replace K by K_n. Taking into account the remark following Prop. 6, we find from what precedes that $\sigma^{p^n}-\lambda^{p^n}$ has a bounded inverse on X, whence also $\sigma-\lambda$.

We can define, in the obvious way, cohomology groups $H^i(\mathscr{G},X)$ based on continuous cochains for the canonical topologies on $\mathscr{G}$ and X. If χ is a continuous character of $\mathscr{G}$ into the group of units of K, then we denote by $X(\chi)$ the space X with the "twisted" action

$${}^s x=\chi(s)\,(sx),$$

for $s\in\mathscr{G}$, $x\in X$.

We then have

Proposition 8. (a) *$H^0(\mathscr{C}, X)=K$, and $H^1(\mathscr{C}, X)$ is a one-dimensional vector space over K.*

(b) *If $\chi(\mathscr{C})$ is infinite, then $H^0(\mathscr{C}, X(\chi))$ and $H^1(\mathscr{C}, X(\chi))$ are 0.*

Proof. If Y is a closed subspace of X stable under $\mathscr{C}$, then $H^0(\mathscr{C}, Y(\chi))$ is the kernel of $\sigma-\lambda$ on Y, and, since a 1-cocycle on $\mathscr{C}$ is determined by its value at σ, $H^1(\mathscr{C}, Y(\chi))$ is a subgroup of the cokernel of $\sigma-\lambda$ on Y. In particular, both cohomology groups vanish if $\sigma-\lambda$ is bijective on Y. Hence by part (b) of Prop. 7 we see that $H^0(\mathscr{C}, X_0)$ and $H^1(\mathscr{C}, X_0)$ both vanish, and consequently (a) follows from part (a) of Prop. 7. Similarly, (b) follows from part (c) of Prop. 7, because if $\chi(\mathscr{C})$ is infinite, then $\lambda=\chi(\sigma)$ is not a root of unity.

(3.2). Finite extensions of K_∞

We keep the notations of (3.1). Let L denote a finite extension of K_∞. Denote by R_L its ring of integers and by $\mathfrak{m}_L$ its maximal ideal. R_∞ and $\mathfrak{m}_\infty$ have the same meaning for K_∞. Let $\mathscr{H}=\mathrm{Gal}(\bar{K}/K_\infty)$.

Proposition 9. *We have $\mathrm{Tr}_{L/K_\infty}(R_L)\supset\mathfrak{m}_\infty$.*

Replacing K by one of the K_n we may assume that there is a finite extension L_0 of K, linearly disjoint from K_∞ over K, such that $L=L_0K$ (see [8], p. 97, Lemma 6).

We may also suppose that L_0/K is a Galois extension. Put $L_n=L_0K_n$. Then

$$v(\mathfrak{d}_{L_n/K_n})=\int_{-1}^{\infty}\left(o(\mathrm{Gal}(K_n/K)^v)^{-1}-o(\mathrm{Gal}(L_n/K)^v)^{-1}\right)dv.$$

Let $\mathrm{Gal}(L/K)^v\subset\mathscr{C}$, i.e., $\mathrm{Gal}(L_0/K)^v=(1)$, for $v\leqslant h$. It follows that

$$v(\mathfrak{d}_{L_n/K_n})\leqslant\int_{-1}^{h}o(\mathrm{Gal}(K_n/K)^v)^{-1}\,dv.$$

The argument used in the proof of Prop. 5 now shows that this tends to zero with n (the order of magnitude is p^{-n}). The assertion then follows from familiar results ([8], p. 91, Lemma 4).

Corollary 1. *Let L/K_∞ be finite Galois with group G. Let f be an r-cochain of G with coefficients in L, with $r\geqslant 0$, and let $c>1$. Then there exists an $(r-1)$-cochain g of G in L such that*

$$|f-\delta g|\leqslant c|\delta f|,\quad\text{and}\quad|g|\leqslant c|f|.$$

Here $|f|$ denotes the maximum of the absolute values of the coefficients of f, and by a (-1)-cochain we mean an element $y\in L$. The coboundary δy of such a y is the 0-cochain Tr_{L/K_∞}.

Proof. By Prop. 9 there exists a (-1)-cochain $y\in L$ such that $|y|\leqslant 1$ and $|\delta y|>c^{-1}$. Define an $(r-1)$-cochain $y\cup f$ by the formulas

$$y\cup f=yf,\quad\text{if}\quad r=0$$

$$(y\cup f)(s_1,\ldots,s_{r-1})=(-1)^r\sum_{s_r\in G}s_1s_2\cdots s_r y\cdot f(s_1,s_2,\ldots,s_r),\quad\text{if}\quad r>0.$$

The identity

$$(\delta y)f-\delta(y\cup f)=y\cup(\delta f)$$

is easily checked; on dividing by the element $x=\delta y=\mathrm{Tr}_{L/K_\infty}y\in K$ we find

$$f-\delta g=x^{-1}(y\cup\delta f),\quad\text{with}\quad g=x^{-1}(y\cup f).$$

Since $|x^{-1}|<c$, and $|y|\leqslant 1$, the corollary follows.

Corollary 2. *The corollary 1 still holds true if we replace L by $\bar{K}$, G by $\mathscr{H}$, and consider cochains which are continuous from the Krull topology in G to the discrete topology in $\bar{K}$, provided that, for $r=0$, the conclusion is replaced by: there exists an element $x\in K_\infty$ such that $|f-x|\leqslant c|\delta f|$.*

This follows from Cor. 1, because a continuous cochain in $\mathscr{H}$ with values in $\bar{K}$ comes by inflation from some finite Galois L/K_∞ (cf. SERRE, Cohomologie Galoisienne, Prop. 8.)

Recall that we denote by C the completion of $\bar{K}$. By $H^r(\mathscr{H}, C)$ we mean the cohomology groups constructed with standard cochains which are continuous from the Krull topology in $\mathscr{H}$ to the *valuation topology* in C.

Proposition 10. *We have $H^0(\mathscr{H}, C)=X$, and $H^r(\mathscr{H}, C)=0$, for $r>0$.*

Proof. This will follow immediately from Corollary 2, once we show that, for every continuous cochain f on $\mathscr{H}$ with values in C, there is a sequence of cochains f_ν on $\mathscr{H}$ with values in $\bar{K}$ as in Cor. 2, such that $|f-f_\nu|\to 0$. To construct such f_ν, let D be the ring of integers in C. Then $C=\bar{K}+\pi^\nu D$ for each ν, and there exist maps $\varphi_\nu: C/\pi^\nu D\to\bar{K}$ such that $\psi_\nu\varphi_\nu=\mathrm{id.}$, where $\psi_\nu: C\to C/\pi^\nu D$ is the canonical projection. The φ_ν are automatically continuous because $C/\pi^\nu D$ is discrete. Put $f_\nu=\varphi_\nu\psi_\nu f$. Then $\psi_\nu f_\nu=f_\nu$ implies $|f_\nu-f|\leqslant|\pi|^\nu$.

(3.3). The action of $\mathscr{G}$ on C

Let $\mathscr{G}$ denote the Galois group of $\bar{K}/K$. Then $\mathscr{G}$ operates on C by continuity and we can consider the continuous cochain cohomology groups $H^r(\mathscr{G}, C)$.

Theorem 1. *We have $H^0(\mathscr{G}, C)=K$, and $H^1(\mathscr{G}, C)$ is a one-dimensional vector space over K.*

Proof. Let K_∞/K be as in 3.1; for example, we can take for K_∞ a suitable subfield of the field generated over K by all p^n-th roots of 1, all n. Then we have an isomorphism

$$H^0(\mathscr{G}, C) \simeq H^0(\mathscr{G}/\mathscr{H}, H^0(\mathscr{H}, C))$$

and an exact inflation-restriction sequence

$$0 \to H^1(\mathscr{G}/\mathscr{H}, H^0(\mathscr{H}, C)) \to H^1(\mathscr{G}, C) \to H^1(\mathscr{H}, C),$$

from which our theorem follows, using Prop. 10 and Prop. 8(a).

Remarks. 1. The one-dimensionality of $H^1(\mathscr{G}, C)$ was not known to me for arbitrary K at the time of the conference. It was proved by T. SPRINGER when he wrote up the first draft of these notes.

2. Let $\bar{R}$ denote the integral closure of R in $\bar{K}$, with the *discrete* topology. The methods we have used here yield very easily the fact that $H^1(\mathscr{G}, R)$ is killed by some power of p (the power depending perhaps on K), and this fact in turn implies easily the first part of Theorem 1, i.e., $C^{\mathscr{G}}=K$. Meanwhile, Shankar SEN has shown that $H^1(\mathscr{G}, R)$ is killed by p for p odd, and by 4 if $p=2$. From this result of SEN it follows easily that for every closed subgroup $\mathscr{G}_1$ of $\mathscr{G}$ we have $C^{\mathscr{G}_1}=\hat{K}_1$ where $K_1=\bar{K}^{\mathscr{G}_1}$, and where "hat" denotes completion.

3. Recently, James AX has given a short proof of this last result, by a direct method which avoids the use of higher ramification theory and of the intermediate field K_∞.

Now let $\chi: \mathscr{G} \to K^*$ be a continuous homomorphism (note that the values of χ are units in K^* because $\mathscr{G}$ is compact), and let $C(\chi)$ denote C with the twisted action ${}^s x=\chi(s)\,sx$. Let K_∞ denote the extension of K determined by $\operatorname{Ker}\chi$.

Theorem 2. *Suppose that there is a finite extension K_0 of K contained in K_∞ such that K_∞/K_0* is totally ramified and $\operatorname{Gal}(K_\infty/K_0)\simeq \mathbf{Z}_p$. *Then $H^0(\mathscr{G}, C(\chi))=0$ and $H^1(\mathscr{G}, C(\chi))=0$.*

Proof. It is easy to reduce the statement to the case $K=K_0$, and in that case the result follows if we apply Prop. 10 and Prop. 8(b) as in the proof of Theorem 1.

§ 4. Theorems on p-divisible groups

We continue now the discussion of (2.4). Let G be a p-divisible group over our complete discrete valuation ring R of mixed characteristic and

let K, C, and D be as in § 3. Let G' be the dual of G. By Cartier duality we have for each ν

$$G'_\nu(D) \xrightarrow{\sim} \operatorname{Hom}_D(G_\nu \underset{R}{\otimes} D, \mathbf{G}_m).$$

Passing to the projective limit as $\nu \to \infty$ we obtain an isomorphism

$$T(G') \xrightarrow{\sim} \operatorname{Hom}_D(G \underset{R}{\hat{\otimes}} D, \mathbf{G}_m(p))$$

where $\mathbf{G}_m(\mathrm{p})$ is the p-divisible group attached to $\mathbf{G}_m$, viewed over D. This isomorphism gives us pairings

$$T(G') \times G(D) \to (\mathbf{G}_m(p))(D) \simeq U$$

and

$$T(G') \times t_G(C) \to t_{\mathbf{G}_m(p)}(C) \simeq C,$$

where U denotes the group of units congruent to 1 in D. These pairings are compatible with the logarithm map $L: G(D) \to t_G(C)$ and the ordinary p-adic logarithm $U \to C$. The kernel of these logs is the torsion subgroup of their domain, and they are surjective because, C being algebraically closed, $G(D)$ and U are divisible. Thus we get an exact commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \Phi(G) & \longrightarrow & G(D) & \xrightarrow{L} & t_G(C) \longrightarrow 0 \\ & & \downarrow{\scriptstyle \alpha_0} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle d\alpha} \\ 0 & \to & \operatorname{Hom}(T', U_{\mathrm{tors}}) & \to & \operatorname{Hom}(T', U) & \to & \operatorname{Hom}(T', C) \to 0, \end{array} \qquad (*)$$

where $T'=T(G')$ is free of rank h over $\mathbf{Z}_p$, the Homs in the bottom row are $\mathbf{Z}_p$-homs, and where $U_{\mathrm{tors}} \simeq \Phi(\mathbf{G}_m(p))$ is the group of roots of unity in U. The vertical arrows are $\mathscr{G}$-homomorphisms, $\mathscr{G}$ acting on a homomorphism f by the rule $(sf)(x)=s(f(s^{-1}x))$.

Proposition 11. *α_0 is bijective and α and $d\alpha$ are injective.*

The proof is in a series of steps.

Step 1. *α_0 is bijective.* Indeed, since K is of characteristic 0, Cartier duality gives a perfect duality of finite $\mathscr{G}$-modules

$$G_\nu(C) \times G'_\nu(C) \to U_{\mathrm{tors}}$$

for each ν. The result follows on passage to the limit as $\nu \to \infty$, inductively with the G_ν and projectively with the G'.

Incidentally, if we pass to the limit projectively with both, we find a $\mathcal{G}$-isomorphism

$$T(G) \simeq \mathrm{Hom}(T(G'), H),$$

where $H = T(\mathbf{G}_m(p)) = \varprojlim_\nu$ (group of p^ν-th roots of unity).

Step 2. $\mathrm{Ker}\,\alpha$ *and* $\mathrm{Coker}\,\alpha$ *are vector spaces over* $\mathbf{Q}_p$. Applying the snake-lemma to diagram (*) and using Step 1, we find that α and $d\alpha$ have isomorphic kernels and cokernels. Since $d\alpha$ is C-linear, the result follows.

Step 3. *We have* $G(R) = G(D)^{\mathcal{G}}$ *and* $t_G(K) = t_G(C)^{\mathcal{G}}$. This follows from Theorem 1, i.e., from the fact that $K = C^{\mathcal{G}}$, which of course implies that $R = D^{\mathcal{G}}$.

Step 4. α *is injective on* $G(R)$. Indeed, the kernel of the restriction of α to $G(R)$ is $(\mathrm{Ker}\,\alpha)^{\mathcal{G}}$ by step 3, and is therefore uniquely divisible by p, by step 2. If G is connected it follows that $\mathrm{Ker}\,\alpha \cap G(R) = 0$, because in that case, viewing G as a formal Lie group we see that $\bigcap p^\nu G(R) = 0$, because the valuation on R is *discrete* (if x is a point of $G(R)$, all of whose coordinates are $\equiv 0 \pmod{\pi^i}$ then the coordinates of px are $\equiv 0 \pmod{\pi^{i+1}}$). In the general case we see then that $(\mathrm{Ker}\,\alpha) \cap G^0(R) = 0$, where G^0 is the connected component of G (use the functorality of (*) with respect to $G^0 \to G$, and the fact that $T(G') \to T((G^0)')$ is surjective). Since $\mathrm{Ker}\,\alpha$ is torsion-free and $G(R)/G^0(R)$ is a torsion group, it follows that $\mathrm{Ker}\,\alpha \cap G(R) = 0$ as claimed.

Step 5. *The map* $d\alpha$ *is injective on* $t_G(K)$. From steps 1 and 4 we conclude that $d\alpha$ is injective on $L(G(R))$; but that group spans $t_G(K)$ over $\mathbf{Q}_p$.

Step 6. *The map* $d\alpha$ *is injective.* The arrow $d\alpha$ can be factored as follows

$$t_G(C) \simeq t_G(K) \underset{K}{\otimes} C \to \mathrm{Hom}_{\mathcal{G}}(T', C) \underset{K}{\otimes} C \to \mathrm{Hom}(T', C).$$

The left-hand arrow is injective by step 5. The right-hand one is injective by

Step 7. *Let* W *be a vector space over* C *on which* $\mathcal{G}$ *operates semilinearly* (i.e., $s(cw) = s(c)\,s(w)$, for $s \in \mathcal{G}$, $c \in C$, $w \in W$). *Then the C-linear map*

$$W^{\mathcal{G}} \underset{K}{\otimes} C \to W$$

is injective. In down-to-earth terms, this statement means that if a family of elements $w_i \in W^{\mathcal{G}}$ is independent over K, then the family is independent over C. It can be proved by looking at a "shortest" hypothetical dependence relation $\sum c_i w_i = 0$, with $c_i = 1$ for some i, applying elements $s \in \mathcal{G}$ to

it and using Theorem 1, i.e., the fact that K is the fixed field of the group of automorphisms $\mathcal{G}$ of the field C. See SERRE [*10*], Prop. 4, for a more general statement.

Proposition 11 now follows from Steps 1 and 7 and the snake-lemma.

Theorem 3. *The maps*

$$G(R) \xrightarrow{\alpha_R} \mathrm{Hom}_{\mathcal{G}}(T(G'), U)$$

and

$$t_G(K) \xrightarrow{d\alpha_R} \mathrm{Hom}_{\mathcal{G}}(T(G'), C)$$

induced by α *and* $d\alpha$ *are bijective.*

Proposition 11 implies the injectivity of these maps, and also, via step 3 above, that we have injections

$$\mathrm{Coker}\,\alpha_R \subsetneq (\mathrm{Coker}\,\alpha)^{\mathcal{G}} \quad \mathrm{Coker}\,(d\alpha_R) \subsetneq (\mathrm{Coker}\,d\alpha)^{\mathcal{G}}.$$

Since $\mathrm{Coker}\,\alpha \to \mathrm{Coker}\,d\alpha$ is bijective, it follows that the map $\mathrm{Coker}\,\alpha_R \to \mathrm{Coker}\,d\alpha_R$ is injective, so we are reduced to proving that $d\alpha_R$ is surjective. Since $d\alpha_R$ is K-linear and injective, this is a question of dimensions. Let

$$W' = \mathrm{Hom}(T(G'), C) \quad \text{and} \quad W = \mathrm{Hom}(T(G), C),$$

spaces of dimension $h = \mathrm{ht}(G)$ over C on which $\mathcal{G}$ operates semilinearly. Put

$$d' = \dim_K (W')^{\mathcal{G}} \quad d = \dim_K W^{\mathcal{G}}$$
$$n = \dim G = \dim_K t_G(K) \quad n' = \dim G' = \dim_K t_{G'}(K).$$

By the injectivity of $d\alpha_R$ we already know $n \leqslant d'$ and $n' \leqslant d$, and we wish to show that equality holds. Since $n + n' = h$, it will suffice to show that $d + d' \leqslant h$. This we do as follows.

Since $T(G) \simeq \mathrm{Hom}(T(G'), H)$ (see step 1 of proof of Prop. 11), we have $W' = T(G) \otimes \mathrm{Hom}(H, C)$, so that there is a canonical non-degenerate $\mathcal{G}$-pairing

$$W \times W' \to Y,$$

where $Y = \mathrm{Hom}(H, C)$. This space Y is isomorphic to $C(\chi^{-1})$, where $\chi: \mathcal{G} \to \mathbf{Z}_p^*$ is the character such that $sz = z^{\chi(s)}$ for all roots of unity z of p-power order. Therefore, by Theorem 2, $Y^{\mathcal{G}} = H^0(\mathcal{G}, Y) = 0$, and also $H^1(\mathcal{G}, Y) = 0$. Since the spaces $W^{\mathcal{G}}$ and $(W')^{\mathcal{G}}$ are paired into $Y^{\mathcal{G}}$, it follows that $W^{\mathcal{G}} C$ and $(W')^{\mathcal{G}} C$ are orthogonal C-subspaces of W and W'. Their dimensions are d and d' (step 7 of the proof of Prop. 11). Hence $d + d' \leqslant h = \dim_C W$, as required.

Corollary 1. *The $\mathcal{G}$-module $T(G)$ determines the dimension n of $\mathcal{G}$.*

Indeed, $T(G)$ determines $T(G')$ by duality, and $n=\dim_K(t_G(K))=$ $=\dim_K(\mathrm{Hom}_{\mathcal{G}}(T(G'), C))$ by Theorem 3.

Corollary 2. *There is a canonical isomorphism of $\mathcal{G}$-modules*

$$\mathrm{Hom}(T(G), C) \simeq t_{G'}(C) \oplus t_G^*(C) \underset{C}{\otimes} \mathrm{Hom}(H, C),$$

where t_G^* is the cotangent space of G at the origin.

The proof of Theorem 3 above shows that $d\alpha'$ and $d\alpha$ map $t_{G'}(C)$ and $t_G(C)$ injectively onto subspaces of W and W' which are orthogonal complements with respect to the pairing to Y. Thus we have an exact sequence

$$0 \to t_{G'}(C) \xrightarrow{d\alpha'} W \to \mathrm{Hom}_C(t_G(C), Y) = t_G^*(C) \underset{C}{\otimes} Y \to 0,$$

and to prove the corollary, we must show that this sequence has a unique splitting compatible with the action of $\mathcal{G}$. The sequence has the form

$$0 \to C^{n'} \to W \to C(\chi^{-1})^n \to 0,$$

where χ is the character in the proof of Theorem 3. The existence of a splitting follows from $H^1(\mathcal{G}, C(\chi))=0$; and its unicity from $H^0(\mathcal{G}, C(\chi))$ $=0$ (cf. Theorem 2).

Remark: In case $G=A(p)$, where A is an abelian scheme over R, Corollary 2 can be rewritten as

$$H^1(A_C, \mathbf{Q}_p) \otimes C \simeq H^1(A_C, \Omega^0_{A_C}) \oplus H^0(A_C, \Omega^1_{A_C}) \otimes \mathrm{Hom}(H, C),$$

where $A_C=A\otimes_R C$, and where on the left we have the étale cohomology of A_C with coefficients in $\mathbf{Q}_p$. One can ask whether a similar Hodge-like decomposition exists for the étale cohomology with values in C in all dimensions, for a scheme X_C coming from a scheme X projective and smooth over R, or perhaps even over K, or for suitable "rigid analytic" spaces.

(4.2.). We can now prove the main result

Theorem 4. *Let R be an integrally closed, noetherian, integral domain, whose field of fractions K is of characteristic 0. Let G and H be p-divisible groups over R. A homomorphism $f: G\otimes_R K \to H\otimes_R K$ of the general fibers extends uniquely to a homomorphism $G\to H$.*

Corollary 1. *The map* $\mathrm{Hom}(G, H)\to\mathrm{Hom}_{\mathcal{G}}(T(G), T(H))$ *is bijective, where* $\mathcal{G}=\mathrm{Gal}(\bar{K}/K)$.

Corollary 2. *If $g: G\to H$ is a homomorphism such that its restriction $G\otimes_R K\to H\otimes_R K$ is an isomorphism, then g is an isomorphism.*

Since $R=\cap_P R_P$, where P runs over the minimal non-zero primes of R, and since each R_P is a discrete valuation ring, we are immediately reduced to the case R is a discrete valuation ring. There exists an extension R' of R which is a complete discrete valuation ring with algebraically closed residue field and such that $R=R'\cap K$; hence we may assume R is complete with algebraically closed residue field, k. If $\mathrm{char}\, k\neq p$, then G is étale and the theorem is obvious. Thus we are reduced to the case of an R of the type considered in the preceding paragraphs, which we assume from now on.

We first prove Corollary 2. Let $G=(G_\nu)$ and $H=(H_\nu)$, and let A_ν (resp. B_ν) denote the affine algebra of G_ν (resp. H_ν). We are given a coherent system of homomorphisms $u_\nu: B_\nu\to A_\nu$, of which we know that their extensions $u_\nu\otimes 1: B_\nu\otimes_R K\to A_\nu\otimes_R K$ are isomorphisms. Since B_ν is free over R, it follows that u_ν is injective for all ν. To prove surjectivity, we look at the discriminants of the R-algebras A_ν and B_ν. By Prop. 2, these discriminants are non-zero, and are determined by the heights of G and H and their dimensions. But the height and dimension of a p-divisible group over R are determined by its general fiber, the height trivially, and the dimension by Cor. 1 of Theorem 3, since the general fiber of G determines the $\mathcal{G}$-module $T(G)$. Hence the discriminants of A_ν and B_ν are equal and non-zero, and it follows that u_ν is bijective. This proves Corollary 2.

To derive the theorem from the corollary, we will use

Proposition 12. *Suppose F is a p-divisible group over R, and M a $\mathcal{G}$-submodule of $T(F)$ such that M is a $\mathbf{Z}_p$-direct summand. Then there exists a p-divisible group Γ over R and a homomorphism $\varphi: \Gamma\to F$ such that φ induces an isomorphism $T(\Gamma)\xrightarrow{\sim} M$.*

Granting this Proposition we prove the theorem, letting $F=G\times H$, and letting M be the graph of the homomorphism $T(G)\to T(H)$ which corresponds to the given homomorphism $f: G\otimes_R K\to H\otimes_R K$. By Prop. 12 we get a p-divisible group Γ over R and a homomorphism $\varphi: \Gamma\to G\times H$ such that the composition $\mathrm{pr}_1\cdot\varphi: \Gamma\to G$ induces an isomorphism $T(\Gamma)\to T(G)$, hence an isomorphism on the general fibers. By Cor. 2, it follows that $\mathrm{pr}_1\cdot\varphi$ is an isomorphism. Thus $\mathrm{pr}_2\cdot\varphi\cdot(\mathrm{pr}_1\cdot\varphi)^{-1}: G\to H$ is a homomorphism extending f. The unicity of such an extension is obvious, and this concludes the proof of Theorem 4.

Proof of Prop. 12. The submodule $M\subset T(F)$ corresponds to a closed

p-divisible subgroup $E_* \subset F \otimes_R K$. Let E be the "closure of E_* in F". By this we mean the following: Let B_ν be the affine R-algebra of F_ν, let $A_{*\nu}$ be the affine K-algebra of $E_{*\nu}$, and let $u_\nu : B_\nu \otimes_R K \to A_{*\nu}$ correspond to the inclusion $E_{*\nu} \subset F_\nu \times_R K$. Put $A_\nu = u_\nu(B_\nu)$, and put $E_\nu = \operatorname{Spec} A_\nu$. Then E_ν is a closed subgroup of F_ν for each ν, and the inclusions $F_\nu \to F_{\nu+1}$ induce inclusions $E_\nu \to E_{\nu+1}$; we put $E = \varinjlim(E_\nu)$. Although E itself may not be p-divisible (see example below), nevertheless $E \times_R K = E_*$ is p-divisible, and it follows that E_{i+1}/E_i is killed by p, hence that p induces homomorphisms

$$E_{i+\nu+1}/E_{i+1} \to E_{i+\nu}/E_i$$

which are isomorphisms on the general fiber. Let D_i be the affine algebra of E_{i+1}/E_i. Then all $D_i \otimes_R K$ can be identified, and the D_i constitute an increasing sequence of orders in a finite separable K-algebra. Hence there is an i_0 such that $D_i = D_{i+1}$ for $i \geqslant i_0$. Put $\Gamma_\nu = E_{i_0+\nu}/E_{i_0}$. Then p^{i_0} induces a coherent collection of homomorphisms $\Gamma_\nu \to E_\nu/E_0 = E_\nu$, which are isomorphisms at the general fiber, and we will therefore be done if we show that $\Gamma = \bigcup \Gamma_\nu$ is p-divisible. For this, we factor the homomorphism p^ν in $\Gamma_{\nu+1}$ as follows

$$\begin{array}{ccccc} \Gamma_{\nu+1} = E_{i_0+\nu+1}/E_{i_0} & & \xrightarrow{p^\nu} & & E_{i_0+\nu+1}/E_{i_0} = \Gamma_{\nu+1} \\ \downarrow{\scriptstyle \alpha} & & & & \uparrow{\scriptstyle \gamma} \\ E_{i_0+\nu+1}/E_{i_0+\nu} & & \xrightarrow{\beta} & & E_{i_0+1}/E_{i_0}, \end{array}$$

where α is the canonical projection, γ the canonical inclusion, and where β is induced by p^ν, and is therefore an isomorphism by our choice of i_0. It follows that the kernel of p^ν in $\Gamma_{\nu+1}$ is the same as $\operatorname{Ker}\alpha = \Gamma_\nu$, so Γ is p-divisible as claimed.

The following example, due to SERRE, shows that the map φ in Prop. 12 need not be a closed immersion. Let X be an elliptic curve over R whose reduction $\tilde{X}$ has Hasse invariant $\neq 0$, and suppose the points of order p on X are rational. Then there exist two such points, say x and y, which are independent, but such that $\tilde{x} = \tilde{y}$ is of order p, and the sequence

$$0 \to X \xrightarrow{\varphi} (X/\mathbf{F}_p x) \times (X/\mathbf{F}_p y) \to \operatorname{Coker} \varphi \to 0$$

is then exact over K, but φ is not injective over R, because $\varphi\tilde{x} = 0$. Passing to the associated p-divisible groups, one gets the desired example.

References

[1] ARTIN, E.: Algebraic numbers and algebraic functions. Lecture notes. New York 1950/51.

[2] ARTIN, E. and J. Tate: Class Field Theory. Harvard 1961.
[3] CARTIER, P.: Colloque sur la theorie des groupes algébriques. Brussels 1962.
[4] DEMAZURE, M. and A. Grothendieck: Schémas en groupes. Séminaire I.H.E.S. 1963–64.
[5] GROTHENDIECK, A.: Eléments de géométrie algébrique, I.H.E.S. Publications, Paris.
[6] MANIN, Yu. I.: Theory of formal commutative groups (translation). Russian Math. Surveys, vol. 18, p. 1–83 (1963).
[7] RAYNAUD, M.: Passage au quotient par une relation d'equivalence plate. This volume p. 78–85.
[8] SERRE, J.-P.: Corps locaux. Hermann, Paris, 1962.
[9] SERRE, J.-P.: Sur les corps locaux à corps de restes algébriquement clos. Bull. Soc. Math. de France 89, p. 105–154 (1961).
[10] SERRE, J.-P.: Sur les groupes de galois attachés aux groupes p-divisibles. This volume p. 118–131.
[11] SERRE, J.-P.: Groupes p-divisibles (d'après J. Tate). Séminaire Bourbaki, N°. 318, (Nov. 1966).
[12] SERRE, J.-P.: Lie algebras and Lie groups. New York: Benjamin 1965.