ANNALES SCIENTIFIQUES DE L'É.N.S.

JOHN TATE
FRANS OORT

Group schemes of prime order

Annales scientifiques de l'É.N.S. 4e série, tome 3, nº 1 (1970), p. 1-21.
<http://www.numdam.org/item?id=ASENS_1970_4_3_1_1_0>

© Gauthier-Villars (Éditions scientifiques et médicales Elsevier), 1970, tous droits réservés.

L'accès aux archives de la revue « Annales scientifiques de l'É.N.S. » (http://www.elsevier.com/locate/ansens), implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/legal.php). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Ann. scient. Éc. Norm. Sup.,
4e série, t. 3, 1970, p. 1 à 21.

GROUP SCHEMES OF PRIME ORDER

BY JOHN TATE AND FRANS OORT (*)

INTRODUCTION. — Our aim in this paper is to study group schemes G of prime order p over a rather general base scheme S. Suppose

$$G = \operatorname{Spec}(A), \qquad S = \operatorname{Spec}(R),$$

and suppose the augmentation ideal $I = \operatorname{Ker}(A \to R)$ is free of rank *one* over R (so G is of order $p = 2$), say $I = Rx$; then there exist elements a and c in R such that $x^2 = ax$ and such that the group structure on G is defined by $sx = x \otimes 1 + 1 \otimes x - cx \otimes x$. One easily checks that $ac = 2$; conversely any factorization $ac = 2 \in R$ defines a group scheme of order 2 over R. In this way all R-group schemes whose augmentation ideal is free of rank one are classified, and an easy sheaf-theoretic globalization yields a classification of group schemes of order 2 over any base S. In case $p > 2$ the difficulty is to find a good generator for the ideal I. To this end we prove first (theorem 1) that any G of order p is commutative and killed by p, i. e. is a " module scheme " over $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. In order to exploit the action of $\mathbf{F}_p^*$ on G, we assume in section 2 that the base S lies over Spec (Λ_p), where

$$\Lambda_p = \mathbf{Z}\left[\zeta, \frac{1}{p(p-1)}\right] \cap \mathbf{Z}_p,$$

ζ being a primitive $(p-1)$-th root of unity in the ring of p-adic integers $\mathbf{Z}_p$. For S over Spec (Λ_p) we prove (theorem 2) that the S-groups of order p are classified by triples (L, a, b) consisting of an invertible $\mathcal{O}_S$-module L, together with sections a and b of $L^{\otimes(p-1)}$ and $L^{\otimes(1-p)}$ such that $a \otimes b = w_p$, where w_p is the product of p and of an invertible element of Λ_p. Since the p-adic completion of Λ_p is $\mathbf{Z}_p$, this structure theorem

(*) Work on this paper was partially supported by the National Science Foundation.

applies in particular to a base of the form $S = \mathrm{Spec}(R)$, where R is a complete noetherian local ring of residue characteristic p : for such an R, the isomorphism classes of R-groups of order p correspond to equivalence classes of factorizations $p = ac$ of $p \in R$, two such factorizations $p = a_1 c_1$ and $p = a_2 c_2$ being considered equivalent if there is an invertible element u in R such that $a_2 = u^{p-1} a_1$ and $c_2 = u^{1-p} c_1$ (*cf.* remark 5 at the end of section 2). In section 3 we apply this theory to obtain a classification (theorem 3) of group schemes of order p defined over the ring of integers in a number field, in terms of idèle class characters. As a special case we recover an unpublished result of M. Artin and B. Mazur, to the effect that the only group schemes of order p over $\mathbf{Z}$ are the constant group $(\mathbf{Z}/p\mathbf{Z})_{\mathbf{Z}}$ and its Cartier dual $\boldsymbol{\mu}_{p,\mathbf{Z}}$.

Our original proof of theorem 1, insofar as the " killed by p " part is concerned, was intertwined with the proof of theorem 2. We can now avoid this procedure thanks to P. Deligne, who communicated to us a direct proof of the fact that, for any integer $m \geqq 1$, a *commutative* group scheme of order m is killed by m. We give Deligne's proof in section 1.

1. Preliminaries and two general theorems. — Let S be a prescheme and T a prescheme over S. We say that T is *of finite order* over S if T is of the form $T = \mathcal{S}pec(A)$, where A is a sheaf of $\mathcal{O}_S$-algebras which is locally free of constant rank r; and then we say that T is *of order r* over S. If S is locally noetherian and connected, then T is of finite order over S if and only if it is *finite* and *flat* over S.

Suppose $G = \mathcal{S}pec(A)$ is a group scheme of finite order over S. We denote by

(1) $$s_A = s : \quad A \to A \otimes_{\mathcal{O}_S} A \quad \text{respectively} \quad t_A = t : A \otimes_{\mathcal{O}_S} A \to A$$

the homomorphisms of $\mathcal{O}_S$-algebras which correspond to the law of composition, respectively the diagonal map

$$G \times_S G \to G, \qquad \Delta_G : \quad G \to G \times_S G.$$

Let A′ denote the $\mathcal{O}_S$-linear dual of A :

$$A' = \mathcal{H}om_{\mathcal{O}_S}(A, \mathcal{O}_S);$$

this is a locally free sheaf of the same rank as A. As A′ is locally free of finite rank, the natural map

$$A' \otimes_{\mathcal{O}_S} A' \xrightarrow{\sim} (A \otimes_{\mathcal{O}_S} A)'$$

is an isomorphism, and we obtain

(2) $$t_{A'} = (s_A)' : \quad A' \otimes_{\mathcal{O}_S} A' \to A' \qquad \text{and} \qquad s_{A'} = (t_A)' : \quad A' \to A' \otimes_{\mathcal{O}_S} A',$$

which makes A′ into an associative, coassociative, and cocommutative Hopf-algebra over $\mathcal{O}_S$, with unit and counit — the analog of the group algebra of G. The map

$$(3) \qquad G(S) = \mathrm{Hom}_{\text{unitary } \mathcal{O}_S\text{-algebras}}(A, \mathcal{O}_S) \hookrightarrow \Gamma(S, A')$$

is an isomorphism of G(S) onto the multiplicative group of invertible elements $g \in \Gamma(S, A')$ such that $s_{A'}(g) = g \otimes g$.

The group scheme G is commutative if and only if the ring A′ is commutative. Suppose this is the case. Then the S-prescheme $G' = \mathcal{S}pec(A')$, with the law of composition induced by $s_{A'}$, is a commutative S-group of the same finite order as G, the Cartier dual of G. As there is a canonical isomorphism

$$A \xrightarrow{\sim} (A')',$$

we have $G = (G')'$, and (3) can be interpreted as an isomorphism

$$(4) \qquad G(S) \cong \mathrm{Hom}_{S\text{-groups}}(G', \mathbf{G}_{m,S}),$$

where $\mathbf{G}_{m,S}$ is the multiplicative group over S. Viewed symmetrically, (4) gives a bimultiplicative morphism of schemes over S,

$$(5) \qquad G \times_S G' \to \mathbf{G}_{m,S},$$

which we call the Cartier pairing.

Let $G \to S$ be an S-group scheme. For each integer $m \in \mathbf{Z}$ we denote by

$$m_G : \quad G \to G$$

the morphism obtained by raising to the m-th power all elements of the group functor G, i. e. for all $T \to S$, and any $\xi \in G(T)$,

$$m_G(\xi) = \xi^m.$$

Suppose $G = \mathcal{S}pec(A)$, then we use $[m] : A \to A$ for the corresponding $\mathcal{O}_S$-algebra homomorphism. The "laws of exponents" $(\xi^n)^m = \xi^{nm}$ and $(\xi^m)(\xi^n) = \xi^{m+n}$ amount to the identities

$$[m].[n] = [mn] \qquad \text{and} \qquad t_A \circ ([m] \otimes [n]) \circ s_A = [m+n].$$

Of course $[1] = \mathrm{id}_A$, and $[0] = i \circ \varepsilon$, where $\varepsilon : A \to \mathcal{O}_S$ corresponds to the neutral element of G(S), and where $i : \mathcal{O}_S \to A$ corresponds to the structure morphism $G \to S$. The ideal $I = \mathrm{Ker}(\varepsilon) = \mathrm{Ker}[0]$ is called the *augmentation ideal* of A (or of G). If $m \geq 2$, clearly

$$[m] = (A \to A^{\otimes m} \to A),$$

the first arrow being defined by iteration of s_A, and the second being the multiplication.

We thank P. Deligne for letting us present here his proof of :

THEOREM (Deligne). — *A* commutative S-*group of order* m *is killed by* m (i. e. $m_G = 0_G$).

The proof of the theorem is inspired by the following : let Γ be a finite commutative (abstract) group of order m, and let $x \in \Gamma$. Then

$$\prod_{\gamma\in\Gamma}\gamma = \prod_{\gamma\in\Gamma}(\gamma x) = \Big(\prod_{\gamma\in\Gamma}\gamma\Big)x^m,$$

and hence $x^m = e$.

In order to be able to apply this idea to group schemes Deligne defines the following trace map : let G be a commutative group scheme of finite order over S, and suppose $T = \mathcal{S}pec(B)$ is of order m over S, with structure morphism $f: T \to S$. Then Tr_f is the unique map such that the diagram

$$\begin{tikzcd} G(T) \arrow[r, hook] \arrow[d, "\mathrm{Tr}_f"] & \Gamma(T, \mathcal{O}_T \otimes_{\mathcal{O}_S} A') = \Gamma(S, B \otimes_{\mathcal{O}_S} A') \arrow[d, "N"] \\ G(S) \arrow[r, hook] & \Gamma(S, A') \end{tikzcd}$$

is commutative, where the (injective) horizontal arrows are as in (3), and where N denotes the norm map for the A′-algebra $B \otimes_{\mathcal{O}_S} A'$, which is locally free of rank m over A′ (here we use the commutativity of A′). From this definition we easily deduce that Tr_f is a homomorphism, and that

(6) $$\mathrm{Tr}_f(f^\star u) = u^m \quad \text{for all } u \in G(S),$$

where $f^\star = G(f) : G(S) \to G(T)$. Suppose $t : T \to T$ is an S-automorphism; then

(7) $$\mathrm{Tr}_f(\beta) = \mathrm{Tr}_f(T \xrightarrow{t} T \xrightarrow{\beta} G) \quad \text{for all } \beta \in G(T);$$

this follows immediately from the properties of a norm map.

Proof of the theorem. — In order to prove that a group scheme $H \to U$ of order m is killed by m, it is sufficient to show that for any $S \to U$, each element of H(S) has an order dividing m; as

$$H(S) = \mathrm{Hom}_S(S, H \times_U S),$$

it suffices to prove that for any $f: G \to S$, a commutative group scheme of order m, and for any *section* $u \in G(S)$ we have $u^m = 1$. We denote by $t_u : G \to G$ the translation on G by u, i. e.

$$t_u = \left(G \cong G \times_S S \xrightarrow{(1,\,u)} G \times_S G \to G\right).$$

We consider $1_G \in G(G)$ $\left(\text{the analog of } \prod_{\gamma\in\Gamma} \gamma\right)$, and using (7) we note that

$$\mathrm{Tr}_f(1_G) = \mathrm{Tr}_f\left(G \xrightarrow{t_u} G \xrightarrow{1_G} G\right).$$

As

$$1_G \circ t_u = 1_G \times (f^* u) : \quad G \to G$$

($\circ$ means composition, and $\times$ means multiplication), using (6) we obtain

$$\mathrm{Tr}_f(1_G) = \mathrm{Tr}_f(1_G \times (f^* u)) = \mathrm{Tr}_f(1_G) \times \mathrm{Tr}_f(f^* u) = \mathrm{Tr}_f(1_G) \times u^m,$$

and the theorem is proved.

Remark. — A group scheme of order m over a *reduced* base is killed by its order (*cf.* [1], VII$_A$.8.5), however we do not know whether this is true for (non-commutative) group schemes over an arbitrary base.

Example and notation. — Let Γ be a finite group, R any commutative ring with identity element, $R[\Gamma]$ the group ring of Γ, and $R^\Gamma = \mathrm{Map}(\Gamma, R)$ the ring of functions from Γ into R. The constant group scheme defined by Γ over R is $\Gamma_R = \mathrm{Spec}(R^\Gamma)$. Elements of $R[\Gamma]$ are R-linear functions on R^Γ, and we see that R^Γ and $R[\Gamma]$ are in duality. In particular the dual of the constant cyclic group scheme $(\mathbf{Z}/n\mathbf{Z})_R$ is $\boldsymbol{\mu}_{n,R}$, the group scheme representing the n-th roots of unity

$$\boldsymbol{\mu}_{n,R}(B) = \{ x \mid x \in B,\ x^n = 1 \}$$

for any R-algebra B.

Let p be a prime number. For the rest of this section we will be concerned exclusively with groups of order p.

THEOREM 1. — *An* S-*group of order* p *is commutative and killed by* p.

By Deligne's theorem we need only prove commutativity. It is clear that it suffices to treat the case $S = \mathrm{Spec}(R)$, where R is a local ring with algebraically closed residue class field.

LEMMA 1. — *Let k be an algebraically closed field, and suppose* $G = \mathrm{Spec}(A)$ *is a k-group of order p. Then either* G *is the constant group scheme, or the characteristic of k equals p and* $G = \boldsymbol{\mu}_{p,k}$ *or* $G = \boldsymbol{\alpha}_{p,k}$. *In particular,* G *is commutative and the k-algebra* A *is generated by a single element.*

Postponing the proof of the lemma for a moment we first show how theorem 1 follows from it. Let tilda (i. e.~) denote reduction modulo the maximal ideal of R. Then $\tilde{G} = G \times_S \operatorname{Spec}(k)$ is commutative by lemma 1, and we can apply that lemma to its Cartier dual $\tilde{G}' = \operatorname{Spec}(\tilde{A}')$. Let $x \in A'$ be such that its residue class $\tilde{x} \in (A')^{\sim} = (\tilde{A})'$ generates the k-algebra $\tilde{A}'$. Then $(R[x])^{\sim} = k[\tilde{x}] = (A')^{\sim}$, and by Nakayama's lemma (which is applicable because A' is a free R-module of finite rank p) we conclude that $A' = R[x]$. Hence A' is commutative, and this means G is commutative.

For the convenience of the reader we include a proof of the well-known lemma 1. Recall first that the connected component H^0 of a finite k-group H is a (normal) subgroup scheme, and if H_1 is a subgroup scheme of H, then the order of H equals the product of the orders of H_1 and of H/H_1 (*cf.* [1], $VI_A.3.2$ (iv)). Since G is of prime order, its connected component is either $\operatorname{Spec}(k)$ or all of G, and, accordingly, G is either étale or connected. If G is étale, then it is constant because k is algebraically closed, hence it is isomorphic to $(\mathbf{Z}/p\mathbf{Z})_k$, and A, the k-algebra consisting of all k-valued functions on $\mathbf{Z}/p\mathbf{Z}$, is generated by any function which takes distinct values at the points of $\mathbf{Z}/p\mathbf{Z}$.

Suppose $G = \operatorname{Spec}(A)$ is connected, i. e. the k-algebra A is a local artin ring. Its augmentation ideal $I \subset A$ is nilpotent. By Nakayama's lemma $I \neq I^2$, hence there exists a non-zero k-derivation $d : A \to k$. This means that the element $d \in I' \subset A'$ has the property $s_{A'}(d) = d \otimes 1 + 1 \otimes d$ (as $\varepsilon = 1 \in A'$). Thus $k[d] \subset A'$ is a k-sub-bialgebra of A', and as $k[d]$ is a commutative ring, we obtain a surjective k-bialgebra homomorphism $A'' \cong A \twoheadrightarrow (k[d])'$; as the order p of G is prime, this implies that the order of $k[d]$ equals p, and hence $k[d] = A'$. As before we conclude that $G' = \operatorname{Spec}(A')$ is either étale or connected. If G' is étale this means $G' \cong (\mathbf{Z}/p\mathbf{Z})_k$, and thus $G \cong \boldsymbol{\mu}_{p,k}$; as G was supposed to be connected this implies $\operatorname{char}(k) = p$. If G' is connected, d is nilpotent, and, as $k[d]$ is of rank p, we must have $d^{p-1} \neq 0$ and $d^p = 0$; as $s_{A'}$ is a ring homomorphism this implies $p = 0$ in k, hence $\operatorname{char}(k) = p$; moreover we already know that $s_{A'}(d) = d \otimes 1 + 1 \otimes d$, hence $G' \cong \boldsymbol{\alpha}_{p,k}$, and thus $G \cong \boldsymbol{\alpha}_{p,k}$ which proves the lemma. Note that the last part of the proof could have been given using p-Lie algebras (*cf.* [1], VII_A. 7).

Remark. — In contrast with group theory there exists a group scheme of rank p which acts non-trivially on another group scheme of rank p, namely $\boldsymbol{\mu}_p$ resp. $\boldsymbol{\alpha}_p$. Hence there exist group schemes of rank p^2 which are not commutative. For example, let R be any $\mathbf{F}_p$-algebra, and define $A = R[\tau, \sigma]$, with $\tau^p = 1$, $\sigma^p = 0$, $s\tau = \tau \otimes \tau$, and $s\sigma = \tau \otimes \sigma + \sigma \otimes 1$. The R-group $G = \operatorname{Spec}(A)$ is isomorphic to the semi-direct product of the normal subgroup scheme defined by $\tau = 1$, which is isomorphic to $\boldsymbol{\alpha}_{p,\mathrm{R}}$, and the subgroup scheme defined by $\sigma = 0$, which is isomorphic to $\boldsymbol{\mu}_{p,\mathrm{R}}$.

2. A CLASSIFICATION THEOREM. — We denote by $\mathbf{Z}_p$ the ring of p-adic integers, and by

$$\chi : \quad \mathbf{F}_p \to \mathbf{Z}_p$$

the unique multiplicative section of the residue class map $\mathbf{Z}_p \to \mathbf{F}_p = \mathbf{Z}_p/p\mathbf{Z}_p$. For any $a \in \mathbf{Z}_p$, we have

$$\chi(\tilde{a}) = \lim_{\nu \to \infty} \{ a^{p^\nu} \},$$

where $\tilde{a}$ is the residue of a mod p. Thus, $\chi(0) = 0$, and for $m \in \mathbf{F}_p^*$, $\chi(m)$ is the unique $(p-1)$-th root of unity in $\mathbf{Z}_p$ whose residue (mod p) is m. The restriction of χ to $\mathbf{F}_p^*$ is a generator for the group $\mathrm{Hom}(\mathbf{F}_p^*, \mathbf{Z}_p^*)$ of " multiplicative characters of $\mathbf{F}_p^*$ ".

Let

$$\Lambda_p = \mathbf{Z}\left[\chi(\mathbf{F}_p), \frac{1}{p(p-1)}\right] \cap \mathbf{Z}_p,$$

the intersection being taken inside the fraction field $\mathbf{Q}_p$ of $\mathbf{Z}_p$. Thus Λ_p is the ring of elements in the field of $(p-1)$-th roots of unity $\mathbf{Q}(\chi(\mathbf{F}_p))$, which are integral at all places not dividing $p(p-1)$ and also at one place above p, namely that given by the inclusion $\mathbf{Q}(\chi(\mathbf{F}_p)) \subset \mathbf{Q}_p$. The prime ideal in Λ_p corresponding to this last place is

$$\Lambda_p \cap p\mathbf{Z}_p = p\Lambda_p,$$

and $\mathbf{Z}_p$ is the p-adic completion of Λ_p.

Examples :

$$p = 2, \qquad \Lambda_2 = \mathbf{Z};$$

$$p = 3, \qquad \Lambda_3 = \mathbf{Z}\left[\frac{1}{2}\right];$$

$$p = 5, \qquad \Lambda_5 = \mathbf{Z}\left[i, \frac{1}{2(2+i)}\right],$$

where $i = \chi(2)$ is the unique element of $\mathbf{Z}_5$ such that $i^2 = -1$, and $i \equiv 2 \pmod 5$.

In this section we fix a prime number p, we write $\Lambda = \Lambda_p$, and we assume our ground scheme S is over $\mathrm{Spec}(\Lambda)$. We shall often view χ as taking values in the Λ-algebra $\Gamma(\mathrm{S}, \mathcal{O}_\mathrm{S})$, writing simply $\chi(m)$ instead of $\chi(m) . 1_{\mathcal{O}_\mathrm{S}}$; for example if $p\mathcal{O}_\mathrm{S} = 0$, then $\chi(m) = m$.

Let $\mathrm{G} = \mathcal{S}pec(\mathrm{A})$ be an S-group of order p. By theorem 1, the group $\mathbf{F}_p^*$ operates on G, and we can therefore regard A, and the augmentation ideal I of G, as sheaves of modules over the group algebra $\mathcal{O}_S[\mathbf{F}_p^*]$. For each integer i, let $\mathrm{I}_i = e_i \mathrm{I}$, where e_i is the $\mathcal{O}_S$-linear operator

$$(8) \qquad e_i = \frac{1}{p-1} \sum_{m \in \mathbf{F}_p^*} \chi^{-i}(m)\,[m] \in \mathcal{O}_S[\mathbf{F}_p^*].$$

Clearly e_i, hence also I_i, depends only on i (mod$(p-1)$).

LEMMA 2. — *We have* $\mathrm{I} = \sum_{i=1}^{p-1} \mathrm{I}_i$, *direct sum. For each* i, I_i *is an invertible* $\mathcal{O}_S$*-module, consisting of the local sections of* A *such that* $[m]f = \chi^i(m) f$ *for all* $m \in \mathbf{F}_p$. *We have* $\mathrm{I}_i \mathrm{I}_j \subset \mathrm{I}_{i+j}$ *for all* i *and* j, *and* $\mathrm{I}_1^i = \mathrm{I}_i$ *for* $1 \leq i \leq p-1$.

Proof. — For $1 \leq i \leq p-1$, the elements e_i are orthogonal idempotents in the group algebra $\Lambda[\mathbf{F}_p^*]$ whose sum is 1 and which satisfy $[m]e_i = \chi^i(m) e_i$ for $m \in \mathbf{F}_p^*$. Hence I is the direct sum of the I_i, for $1 \leq i \leq p-1$, and I_i consists of the local sections f of I such that $[m]f = \chi^i(m) f$ for all $m \in \mathbf{F}_p^*$, or, what is the same since $\chi^i(0) = 0$, of the local sections f of A such that $[m]f = \chi^i(m) f$ for all $m \in \mathbf{F}_p$. From this and the rule $[m](fg) = ([m]f)([m]g)$ we see that $\mathrm{I}_i \mathrm{I}_j \subset \mathrm{I}_{i+j}$. Since the $\mathcal{O}_S$-module I is locally free of rank $p-1$, its direct summands I_i are locally free over $\mathcal{O}_S$ of ranks r_i such that $r_1 + \ldots + r_{p-1} = p-1$. To prove that $r_i = 1$ for each i, and that $\mathrm{I}_1^i = \mathrm{I}_i$ for $1 \leq i \leq p-1$, it suffices to examine the situation in case $\mathrm{S} = \mathrm{Spec}(k)$, where the Λ-algebra k is an algebraically closed field, and to exhibit in that case a section f_1 of I_1 such that $f_1^i \neq 0$ for $1 \leq i \leq p-1$; then $k f_1^i \subset \mathrm{I}_i$ shows $r_i \geq 1$ for all i, hence $r_i = 1$, and $k f_1^i = \mathrm{I}_i$. By lemma 1 there are only three cases to consider, namely $\mathrm{G} \simeq (\mathbf{Z}/p\mathbf{Z})_k$, $\boldsymbol{\alpha}_{p,k}$, or $\boldsymbol{\mu}_{p,k}$, and the last two only for char$(k) = p$, in which case $\chi(m) = m$. If $\mathrm{G} \simeq (\mathbf{Z}/p\mathbf{Z})_k$, then A is the algebra of k-valued functions on $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$, and $([m]f)(n) = f(mn)$ for $f \in \mathrm{A}$ and $m, n \in \mathbf{F}_p$; hence we may take $f_1 = \chi$. If $\mathrm{G} \simeq \boldsymbol{\alpha}_{p,k}$ (resp. $\boldsymbol{\mu}_{p,k}$), then $\mathrm{A} = k[t]$ with $t^p = 0$, $st = t \otimes 1 + 1 \otimes t$, so $[m]t = mt$ [*resp.* $s(1+t) = (1+t) \otimes (1+t)$, so $[m]t = (1+t)^m - 1$]; hence in both cases $[m]t \equiv mt = \chi(m)t$ (modt^2), we have $e_1 t \equiv t \not\equiv 0$ (modt^2), and can take $f_1 = e_1 t$. This completes the proof of lemma 2.

Example and Notation. — *The group* $\boldsymbol{\mu}_{p,\Lambda}$. We have $\boldsymbol{\mu}_{p,\Lambda} = \mathrm{Spec}(\mathrm{B})$, where $\mathrm{B} = \Lambda[z]$, with $z^p = 1$. The comultiplication in B is given by $sz = z \otimes z$, and $[m]z = z^m$ for all $m \in \mathbf{F}_p$. The augmentation ideal $\mathrm{I}_\mathrm{B} = \mathrm{J}$ of B is $\mathrm{J} = \mathrm{B}(z-1)$, and has a Λ-base consisting of the elements $z^m - 1$ for $m \in \mathbf{F}_p^*$:

$$\mathrm{B}(z-1) = \mathrm{J} = \Lambda(z-1) + \ldots + \Lambda(z^{p-1} - 1).$$

For each integer i we put

$$y_i = (p-1)\, e_i (1-z) = \sum_{m \in \mathbf{F}_p^*} \chi^{-i}(m)\,(1-z^m) \tag{9}$$

$$= \begin{cases} p - \displaystyle\sum_{m \in \mathbf{F}_p} z^m & \text{if } i \equiv 0 \mod (p-1), \\ -\displaystyle\sum_{m \in \mathbf{F}_p^*} \chi^{-i}(m)\, z^m & \text{if } i \not\equiv 0 \mod (p-1). \end{cases}$$

Note that y_i depends only on $i \bmod (p-1)$. Then

$$1 - z^m = \frac{1}{p-1} \sum_{i=1}^{p-1} \chi^i(m)\, y_i, \qquad \text{for } m \in \mathbf{F}_p^*, \tag{10}$$

and

$$sy_i - y_i \otimes 1 - 1 \otimes y_i = -\sum_{m \in \mathbf{F}_p^*} \chi^{-i}(m)\, \{(1-z^m) \otimes (1-z^m)\}$$

$$= \frac{-1}{(p-1)^2} \sum_m \chi^{-i}(m) \sum_{j=1}^{p-1} \sum_{k=1}^{p-1} \chi^j(m)\, \chi^k(m)\, y_j \otimes y_k$$

$$= \frac{-1}{p-1} \sum_{\substack{j+k \equiv i \\ \text{mod}\,(p-1)}} y_j \otimes y_k,$$

hence

$$sy_i = y_i \otimes 1 + 1 \otimes y_i + \frac{1}{1-p} \sum_{j=1}^{p-1} y_j \otimes y_{i-j}. \tag{11}$$

Formula (10) shows that

$$\mathrm{J} = \Lambda y_1 + \ldots + \Lambda y_{p-1}.$$

Hence $\mathrm{J}_i = e_i \mathrm{J} = \Lambda y_i$ for each i, because $e_1, \ldots, e_{p-1}$ are orthogonal idempotents. Putting $y = y_1$, we can therefore define a sequence of elements $1 = w_1, w_2, \ldots$ in Λ by

$$y^i = w_i y_i. \tag{12}$$

Proposition. — *The elements w_i are invertible in Λ for $1 \leq i \leq p-1$, and $w_p = p w_{p-1}$. We have $\mathrm{B} = \Lambda[y]$, with $y^p = w_p y$, and*

$$sy = y \otimes 1 + 1 \otimes y + \frac{1}{1-p} \sum_{i=1}^{p-1} \frac{y^i}{w_i} \otimes \frac{y^{p-i}}{w_{p-i}}; \tag{13}$$

$$[m]y = \chi(m)\, y \qquad \text{for } m \in \mathbf{F}_p; \tag{14}$$

$$w_i \equiv i! \pmod{p} \qquad \text{for } 1 \leq i \leq p-1; \tag{15}$$

$$z = 1 + \frac{1}{1-p}\left(y + \frac{y^2}{w_2} + \ldots + \frac{y^{p-1}}{w_{p-1}}\right). \tag{16}$$

Proof. — By lemma 2,

$$\Lambda y^i = (\Lambda y)^i = (J_1)^i = J_i = \Lambda y_i,$$

thus the w_i are invertible for $1 \leq i \leq p-1$. Clearly $(z-1)^p \equiv 0 \pmod p$, thus $y^p \equiv 0 \pmod p$; moreover

$$z \equiv 1 + y + \frac{y^2}{w_2} + \ldots + \frac{y^{p-1}}{w_{p-1}} \pmod p;$$

comparing the coefficients of $y^i \otimes y$, $1 \leq i < p-1$, in both sides of

$$\left(1 + y + \ldots + \frac{y^{p-1}}{w_{p-1}}\right) \otimes \left(1 + y + \ldots + \frac{y^{p-1}}{w_{p-1}}\right)$$
$$\equiv 1 + sy + \frac{1}{w_2}(sy)^2 + \ldots + \frac{1}{w_{p-1}}(sy)^{p-1} \pmod p,$$

we obtain $w_{i+1} \equiv (i+1).w_i \pmod p$ for $1 \leq i < p-1$, which proves (15).

The other formulas have been proved already, except for the identity $w_p = pw_{p-1}$. To this end, choose an embedding $\Lambda = \Lambda_p \hookrightarrow K$, where K is some field containing a primitive p-th root of unity $\zeta \in K$ (e. g. $\Lambda \subset \mathbf{Z}_p$ and choose for K an algebraic closure of $\mathbf{Q}_p$, or choose an embedding of Λ into the field $\mathbf{C}$ of complex numbers). Extend the embedding $\Lambda \hookrightarrow K$ to a homomorphism $\Lambda[z] \to K$ by $z \mapsto \zeta$; let $y_i \mapsto \eta_i$ and $\eta = \eta_1$ under this homomorphism. Then by (9) we find $\eta_{p-1} = p$; as $p \neq 0$ and $w_{p-1} \neq 0$ in Λ, we see $\eta \neq 0$, and using (12) we have

$$pw_{p-1} = \eta_{p-1} w_{p-1} = \eta^{p-1} = \frac{\eta^p}{\eta} = w_p,$$

which concludes the proof of the proposition.

Remark. — The $w_i \in \Lambda$ can be computed inductively from $w_1 = 1$ and the relations

$$(17) \qquad \frac{w_{i+j}}{w_i w_j} = \begin{cases} p & \text{if } i \equiv 0 \quad \text{or} \quad j \equiv 0, \\ (-1)^i & \text{if } i \not\equiv 0, \quad j \not\equiv 0 \quad \text{but } i+j \equiv 0, \\ (-1)^{i+j+1} \mathcal{J}(-i, -j), & \text{if } i \not\equiv 0, \quad j \not\equiv 0 \quad \text{and} \quad i+j \not\equiv 0, \end{cases}$$

where the congruences are mod$(p-1)$, and where $\mathcal{J}$ denotes the Jacobi sums

$$\mathcal{J}(i, j) = \sum_{\substack{m+n=-1 \\ m, n \in \mathbf{F}_p^*}} \chi^i(m)\, \chi^j(n).$$

Choose an embedding $\Lambda = \Lambda_p \hookrightarrow \Lambda[\zeta] \subset K$ as in the proof of the proposition; then

$$\frac{w_{i+j}}{w_i w_j} = \frac{\eta_i \eta_j}{\eta_{i+j}}.$$

The first case of (17) is clear, because $\eta_{p-1}=p$. Suppose $i\not\equiv 0$ and $j\not\equiv 0 \bmod (p-1)$; then $p\neq 2$, and $\chi(-1)=-1$; letting l, m, and n run through $\mathbf{F}_p$ we have

$$\begin{aligned}
\eta_i\eta_j &= \Big\{\sum_{m\neq 0}\chi^{-i}(m)\zeta^m\Big\}\Big\{\sum_{n\neq 0}\chi^{-j}(n)\zeta^n\Big\}\\
&= \sum_{mn\neq 0}\chi^{-i}(m)\chi^{-j}(n)\zeta^{m+n}\\
&= \sum_{l}\zeta^l \sum_{\substack{m+n=l\\ mn\neq 0}}\chi^{-i}(m)\chi^{-j}(n)\\
&= \sum_{n\neq 0}\chi^{-i}(-n)\chi^{-j}(n) + \sum_{l\neq 0}\sum_{\substack{m+n=-1\\ mn\neq 0}}\zeta^l\chi^{-i}(-lm)\chi^{-j}(-ln)\\
&= (-1)^i\sum_{n\neq 0}\chi^{-(i+j)}(n) + (-1)^{i+j}\Big\{\sum_{l\neq 0}\zeta^l\chi^{-(i+j)}(l)\Big\}\\
&\qquad\times\Big\{\sum_{\substack{m+n=-1\\ mn\neq 0}}\chi^{-i}(m)\chi^{-j}(n)\Big\}\\
&= \begin{cases}(-1)^{i+j+1}\eta_{i+j}\,\mathcal{J}(-i,-j), & \text{if } i+j\not\equiv 0,\\[4pt] (-1)^i(p-1) - \displaystyle\sum_{\substack{m+n=-1\\ mn\neq 0}}\chi^i\Big(\frac{n}{m}\Big), & \text{if } i+j\equiv 0.\end{cases}
\end{aligned}$$

This proves the third case of (17), and the second results on replacing n by mn in the last formula

$$\sum_{\substack{m+n=-1\\ mn\neq 0}}\chi^i\Big(\frac{n}{m}\Big) = \sum_{\substack{m(1+n)=-1\\ n\neq 0,\,-1}}\chi^i(n) = -\chi^i(-1) = -(-1)^i.$$

Many of the facts established in the last few paragraphs are essentially equivalent to well-known properties of the Jacobi sums $\mathcal{J}(i,j)$, and the Gauss sums $g(i)=-\eta_{-i}$ attached to the multiplicative character χ^i of the prime field (e. g. *see* [5]). As examples we mention

$p=2,\quad \Lambda_2=\mathbf{Z},\quad w_1=1,\quad w_2=2;$

$p=3,\quad \Lambda_3=\mathbf{Z}\Big[\frac{1}{2}\Big],\quad w_1=1,\quad w_2=-1,\quad w_3=-3,$

$p=5,\quad \Lambda_5=\mathbf{Z}\Big[i,\frac{1}{2(2+i)}\Big],\quad$ where $i=\chi(2)$ and $i^2=-1$,

$w_1=1,\quad w_2=-i(2+i),\quad w_3=(2+i)^2,\quad w_4=-(2+i)^2,\quad w_5=-5(2+i)^2.$

We now continue our discussion on the S-group G. Let

$$\mathbf{S}_{\mathcal{O}_S}[I_1] = \mathcal{O}_S \oplus I_1 \oplus I_1^{\otimes 2} \oplus \ldots$$

denote the symmetric algebra generated by I_1 over $\mathcal{O}_S$. Lemma 2 shows that the homomorphism $\mathbf{S}_{\mathcal{O}_S}[I_1] \to A$ induced by the inclusion $I_1 \subset A$ is *surjective*, and that its kernel is the ideal generated by $(a - 1) \otimes I_1^{\otimes p}$, where

$$(18) \qquad a \in \Gamma(S, I_1^{\otimes (1-p)}) = \mathrm{Hom}_{\mathcal{O}_S}(I_1^{\otimes p}, I_1)$$

is the element corresponding to the homomorphism $I_1^{\otimes p} \to I_1$ induced by the multiplication in A.

Let $G' = \mathcal{S}pec\ (A')$ be the Cartier dual of G and let I', I'_i, and $a' \in \Gamma(S, (I'_1)^{\otimes (1-p)})$ be the analogs for G' of I, I_i, and a for G. Note that the notation is consistent as $(I_A)' = I_{A'}$, and $(I_i)' = (e_i I_A)' = I'_i$. By theorem 1 the Cartier pairing $G \times G' \to \mathbf{G}_{m,S}$ factors through $\boldsymbol{\mu}_{p,S}$ and is therefore given by a homomorphism

$$\varphi: \quad B_S = \mathcal{O}_S \otimes_\Lambda B = \mathcal{O}_S[y] \to A \otimes_{\mathcal{O}_S} A'.$$

Lemma 3. — *The image $\varphi(y)$ of y is a generating section of $I_1 \otimes I'_1$; if we use it to identify I'_1 with $I_1^{\otimes(-1)}$, then $a \otimes a' = w_p \cdot 1_{\mathcal{O}_S}$.*

Proof. — The Cartier pairing $(\xi, \xi') \mapsto \langle \xi, \xi' \rangle$ satisfies

$$\langle \xi^m, (\xi')^n \rangle = \langle \xi, \xi' \rangle^{mn}.$$

Hence, for all $m,n \in \mathbf{F}_p$

$$([m] \otimes [n])\, \varphi y = \varphi([mn] y) = \varphi(\chi(mn) y) = \chi(m)\, \chi(n)\, \varphi y.$$

On the other hand, by lemma 2, $I_i \otimes I'_j$ consists of the local sections h of $A \otimes A'$ which satisfy $([m] \otimes [n]) h = \chi^i(m) \chi^j(n) h$; hence $\varphi y \in \Gamma(S, I_1 \otimes I'_1)$. Clearly φy does not vanish at any point $s \in S$, for if it did, then the Cartier pairing on the fibre $G_s \times G'_s \to \mathbf{G}_{m,s}$ would degenerate. Since φ is a homomorphism of algebras, $w_p . \varphi y = (\varphi y)^p = (\varphi y)^{\otimes p} \otimes a \otimes a'$, and this shows that $a \otimes a' = w_p$, if we identify $I_1 \otimes I'_1$ with $\mathcal{O}_S$ in such a way that $\varphi y = 1$. This proves the lemma.

Theorem 2. — *For any prescheme S over Spec (Λ), the map $G \mapsto (I'_1, a, a')$ discussed above gives a bijection between the isomorphism classes of S-groups of order p and the isomorphism classes of triples (L, a, b) consisting of an invertible $\mathcal{O}_S$-module L, a section $a \in \Gamma(S, L^{\otimes(p-1)})$, and a section $b \in \Gamma(S, L^{\otimes(1-p)})$, such that $a \otimes b = w_p \cdot 1_{\mathcal{O}_S}$.*

Proof. — It is clear from lemma 3 and the discussion preceeding it, that from a triple (I'_1, a, a') we can reconstruct the S-preschemes G and

G' (at first without the group structures), together with the Cartier morphism $G \times G' \to \boldsymbol{\mu}_{p,S}$. Indeed, A is the quotient of the symmetric algebra $\mathbf{S}[(I'_1)^{\otimes(-1)}]$ by an ideal determined by a, A' is the quotient of $\mathbf{S}[I'_1]$ by an ideal determined by a', and the homomorphism $\varphi : B[y] \to A \otimes A'$ is determined by $\varphi y = 1 \in (I'_1)^{\otimes(-1)} \otimes I'_1 = \mathcal{O}_S$. But the Cartier morphism determines the group structures on G and G', because it gives for each S-prescheme T a map

$$G(T) \hookrightarrow \mathrm{Hom}_{T\text{-schemes}}(G' \times_S T, \boldsymbol{\mu}_{p,T})$$

which identifies $G(T)$ with a subgroup of $\boldsymbol{\mu}_p(G' \times_S T)$. The law of composition thus induced on the functor $T \mapsto G(T)$ determines the law of composition in G (for an explicit description of the functor in terms of the data (I'_1, a, a'), *see* remark 1 below).

To complete the proof of the theorem, we have only to show that every triple (L, a, b) comes from a group scheme. The problem is obviously local on the base S, so we can suppose S is affine and that L is *free* of rank 1, say $S = \mathrm{Spec}(R)$, and $L = R$. The problem is to show that for every Λ-algebra R and for every pair of elements $a, b \in R$ such that $ab = w_p \cdot 1_R$, the triple (R, a, b) comes from an R-group of order p.

Let F denote the field of fractions of Λ, and let U be an indeterminate. By the proposition above, the group $\boldsymbol{\mu}_{p,F(U)}$ is equal to $\mathrm{Spec}(A)$, where

$$A = F(U)[y], \qquad y^p = w_p y,$$

with

$$sy = y \otimes 1 + 1 \otimes y + \frac{1}{1-p} \sum_{i=1}^{p-1} \frac{1}{w_i w_{p-i}} y^i \otimes y^{p-i}$$

and $[m]y = \chi(m)y$. Let $Y = U^{-1}y \in A$. Then

$$A = F(U)[Y], \qquad Y^p = w_p U^{1-p} Y,$$

and

$$sY = Y \otimes 1 + 1 \otimes Y + \frac{1}{1-p} \sum_{i=1}^{p-1} \frac{U^{p-1}}{w_i w_{p-i}} Y^i \otimes Y^{p-i}$$

and $[m]Y = \chi(m)Y$. Now let

$$R_0 = \Lambda[w_p U^{1-p}, U^{p-1}] \subset F(U) \qquad \text{and} \qquad C = R_0[Y] \subset A.$$

From the formulas above, we see that C is free of rank p over R_0, and that $s(C) \subset C \otimes_{R_0} C$ (we identify $C \otimes_{R_0} C$ with its image in $A \otimes_R A$). Also $[-1]C \subset C$. Hence we can define an R_0-group G of order p by $G = \mathrm{Spec}(C)$, with the multiplication induced by $s|C$. Clearly

$$R_0 \simeq \Lambda[X_1, X_2]/(X_1 X_2 - w_p).$$

Hence a triple (R, a, b) determines a homomorphism of Λ-algebras $h : R_0 \to R$ such that $h(w_p U^{1-p}) = a$ and $h(U^{p-1}) = b$, and then it follows from the explicit formulas for the structure of G that the triple (R, a, b) comes from the group $G \otimes_{R_0} R$ deduced from G by the base extension via h (*see* remark 1 below). This concludes the proof of theorem 2.

Remarks. — 1. *The functors* $G^L_{a,b}$. Let (L, a, b) be a triple as in theorem 2 for the prescheme S; it corresponds to an S-group $G^L_{a,b}$ of order p (determined up to isomorphism); hence for every prescheme $T \to S$ we are given a group $G^L_{a,b}(T)$, and we now describe this group more explicitly. Let $\xi \in G^L_{a,b}(T)$; the evaluation of local sections of I_1 by ξ gives a homomorphism

$$x = (I_1 \hookrightarrow \mathcal{O}_G \to \mathcal{O}_T), \qquad G = G^L_{a,b},$$

and, as I_1 can be identified with $L^{\otimes -1}$, this is a section

$$x \in \operatorname{Hom}_{\mathcal{O}_S}(L^{\otimes -1}, \mathcal{O}_T) = \Gamma(T, L \otimes_{\mathcal{O}_S} \mathcal{O}_T);$$

as I_1 generates the $\mathcal{O}_S$-algebra which defines G, the correspondence between $\xi \in G^L_{a,b}(T)$ and $x \in \Gamma(T, L \otimes_{\mathcal{O}_S} \mathcal{O}_T)$ is one-to-one; identifying ξ with x, we have

$$G^L_{a,b}(T) = \{ x \in \Gamma(T, L \otimes_{\mathcal{O}_S} \mathcal{O}_T) \mid x^{\otimes p} = a \otimes x \}.$$

In these terms the group structure on this group is given by the multiplication $\star$ [use (13)] :

$$x_1 \star x_2 = x_1 + x_2 + c \otimes D_p(x_1 \otimes 1, 1 \otimes x_2), \qquad c = \frac{b}{w_{p-1}}, \qquad ac = p,$$

where $D_p \in \Lambda[X_1, X_2]$ is the polynomial given by

$$D_p(X_1, X_2) = \frac{w_{p-1}}{1-p} \sum_{i=1}^{p-1} \frac{X_1^i}{w_i} \frac{X_2^{p-i}}{w_{p-i}};$$

also $x^{\star m} = [m]x = \chi(m)x$ for $m \in \mathbf{F}_p$; in particular $x = 0$ is the neutral element in $G^L_{a,b}(T)$, and $x^{\star(-1)} = -x$, for $p \neq 2$. Note that the polynomial $D_p \in \Lambda_p[X_1, X_2]$ is characterised by the following properties : each term of D_p has degree at least 1 and at most $p-1$ in both X_1 and X_2, and if $x_1^p = x_1$, $x_2^p = x_2$, then

$$(x_1 + x_2 + p D_p(x_1, x_2))^p = x_1 + x_2 + p D_p(x_1, x_2);$$

without the results of this section it can be proved easily that there exists a unique $D_p \in \mathbf{Z}_p[X_1, X_2]$ having these properties, and that

$$D_p \equiv \frac{1}{p} \{ (X_1 + X_2)^p - X_1^p - X_2^p \} \mod p.$$

2. *Cartier duality.* Let $M = L^{\otimes(-1)}$. Then $G^L_{a,b}$ and $G^M_{b,a}$ are in canonical Cartier duality via the pairing

$$G^L_{a,b}(T) \times G^M_{b,a}(T) \to G^{\mathcal{O}_S}_{w_p,1}(T) = \boldsymbol{\mu}_p(T) \hookrightarrow \Gamma(T, \mathcal{O}^*_T) = \mathbf{G}_m(T)$$

which is given by

$$x \times x' \mapsto x \otimes x' \mapsto 1 + \frac{1}{1-p} \sum_{i=1}^{p-1} \frac{(x \otimes x')^i}{w_i}.$$

3. *Characteristic p.* Suppose S is a prescheme such that $p\mathcal{O}_S = 0$. Then S is over $\mathbf{F}_p \cong \Lambda/p\Lambda$, hence over Λ, theorem 2 applies, and the condition on a and b is simply $a \otimes b = 0$. The homomorphisms F = " Frobenius " and V = " Verschiebung ",

$$G^L_{a,b} = G \underset{V}{\overset{F}{\rightleftarrows}} G^{(p)} = G^{L^{\otimes p}}_{a^{\otimes p}, b^{\otimes p}},$$

are given by $F(x) = x^{\otimes p} = a \otimes x$ and $V(x') = b \otimes x'$. Hence we are given $\mathcal{O}_S$-linear maps

$$(19) \qquad \begin{cases} F: \; L \to L^{\otimes p}, & \text{by } x \mapsto a \otimes x \in L^{\otimes(p-1)} \otimes L \cong L^{\otimes p}, \\ V: \; L^{\otimes p} \to L, & \text{by } x' \mapsto b \otimes x' \in L^{\otimes(1-p)} \otimes L^{\otimes p} = L, \end{cases}$$

such that

$$FV = [p] = VF, \qquad \text{with} \quad [p] = 0.$$

These data can be gathered together if $S = \mathrm{Spec}(k)$, where k is a perfect field : in that case they correspond in a one-to-one way to giving a module of length one over the ring $k[F, V]$ (this ring is not commutative if $\mathbf{F}_p \neq k$), namely $G^k_{a,b}$ corresponds to the Dieudonné module $k[F, V]/k[F, V].(F - a, V - b^{1/p})$. Thus one could hope that data of the same kind as (19) subject to the relation $FV = [p] = VF$ could generalize the notion of a Dieudonné module in case of arbitrary $\mathbf{F}_p$-algebras.

If moreover $F = 0$, we have $a = 0$. Then b is arbitrary, and theorem 2 shows that the S-groups G of order p for which $F = 0$ correspond to locally free sheaves L on S furnished with a p-linear endomorphism $f \mapsto b \otimes f^{\otimes p}$, that is, to p-Lie algebras $L = \mathrm{Lie}\, G$ which are locally free of rank one over $\mathcal{O}_S$. This is well known (*cf.* [1], exp. $\mathrm{VII_A}$. 7).

4. *The case p = 2.* If $p = 2$, then $\Lambda = \mathbf{Z}$, and theorem 2 gives a classification of groups of order 2 over *any* base S.

5. *Complete local rings of residue characteristic p.* Let R be a Λ_p-algebra such that any projective module of rank one over R is free; for example R could be any complete noetherian local ring with residue characteristic p.

Then we can forget about L in the statement, and we can formulate it as follows : given $a, c \in \mathrm{R}$ such that $ac = p$, let $\mathrm{G}^{c}_{a,\mathrm{R}} = \mathrm{G}^{\mathrm{R}}_{a,\, c w_{p-1}}$; then $(a, c) \mapsto \mathrm{G}^{c}_{a,\mathrm{R}}$ gives a bijection between equivalence classes of factorizations $p = ac$ of p in R and isomorphism classes of R-groups of order p, where two factorizations $p = a_1 c_1$ and $p = a_2 c_2$, are called equivalent if there exists an invertible element $u \in \mathrm{R}$ such that $a_2 = u^{p-1} a_1$ and $c_2 = u^{1-p} c_1$.

6. *The étale case.* It is easy to see that $\mathrm{G}^{\mathrm{L}}_{a,b}$ is étale over S if and only if the section a of $\mathrm{L}^{\otimes(p-1)}$ is invertible, i. e. non vanishing at every point. When this is the case, $b = w_p \otimes a^{\otimes(-1)}$ is uniquely determined by a, and we write $\mathrm{G}^{\mathrm{L}}_{a}$ (resp. $\mathrm{G}_{a,\mathrm{R}}$) instead of $\mathrm{G}^{\mathrm{L}}_{a,b}$ (resp. $\mathrm{G}^{c}_{a,\mathrm{R}}$).

Let us now digress for a moment and suppose that S is connected and non-empty, but not necessarily over $\mathrm{Spec}(\Lambda)$; let $\overline{\mathrm{S}} = \mathrm{Spec}(\overline{\mathcal{O}}_{\mathrm{S}})$ be a universal covering and $\pi = \mathrm{Gal}(\overline{\mathcal{O}}_{\mathrm{S}}/\mathcal{O}_{\mathrm{S}})$ its Galois group. Then for any étale S-group G of order p, $\mathrm{G}(\overline{\mathrm{S}})$ is a cyclic group of order p on which π operates. It is well known that G is determined up to isomorphism by the π-module $\mathrm{G}(\overline{\mathrm{S}})$, or, what is the same, by the corresponding representation $\psi : \pi \to \mathbf{F}^{*}_{p}$, and that every continuous character ψ of π with values in $\mathbf{F}^{*}_{p}$ comes from an étale group of order p over S. If S is over $\mathrm{Spec}(\Lambda)$, the connection between classification by Galois characters ψ and our classification by couples (L, a) is given by Kummer theory : for an étale $\mathrm{G}^{\mathrm{L}}_{a}$, the group $\mathrm{G}^{\mathrm{L}}_{a}(\overline{\mathrm{S}})$ consists of the sections $x \in \Gamma(\mathrm{S}, \mathrm{L} \otimes_{\mathcal{O}_{\mathrm{S}}} \overline{\mathcal{O}}_{\mathrm{S}})$ such that $x^{\otimes p} = a \otimes x$, that is, of $x = 0$, and the $(p-1)$ sections x such that $x^{\otimes(p-1)} = a$. If we designate any one of the latter by $\sqrt[p-1]{(a, \mathrm{L})}$, then the Galois character ψ^{L}_{a} attached to $\mathrm{G}^{\mathrm{L}}_{a}$ satisfies

$$\sqrt[p-1]{(a, \mathrm{L})}^{\,\sigma} = \chi(\psi^{\mathrm{L}}_{a}(\sigma))\, \sqrt[p-1]{(a, \mathrm{L})}$$

and is therefore given by

$$\psi^{\mathrm{L}}_{a}(\sigma) = \chi^{-1}\left(\sqrt[p-1]{(a, \mathrm{L})}^{\,(\sigma-1)}\right). \tag{20}$$

3. Groups of order p over rings of integers in number fields. — Let K be an algebraic number field of finite degree over $\mathbf{Q}$, and let R be an integrally closed subring of K whose field of fractions is K. Let M be the set of non-generic points of $\mathrm{Spec}(\mathrm{R})$, or, what is the same, the set of non-trivial discrete valuations v of K whose valuation ring $\mathcal{O}_v$ contains R. For each $v \in \mathrm{M}$, let R_v denote the completion of R at v, and let K_v denote the v-adic completion of K (i.e. the field of fractions of R_v).

Our aim in this section is to classify R-groups G of order p. The principle on which this classification is based is that to give such a G is the same thing as to give its generic fiber $H = G \otimes_R K$ together with, for each $v \in M$, an R_v-group $G_v = G \otimes_R R_v$ whose generic fiber is $H_v = H \otimes_K K_v$. This principle can be stated more precisely as :

LEMMA 4. — *Let p be a prime number, and let E be the functor which associates with each commutative ring with unity X the set $E(X)$ of isomorphism classes of X-groups of order p. Then the square*

$$\begin{array}{ccc} E(R) & \longrightarrow & \prod_{v \in M} E(R_v) \\ \downarrow & & \downarrow \\ E(K) & \longrightarrow & \prod_{v \in M} E(K_v) \end{array} \tag{21}$$

is cartesian.

For the proof of lemma 4 we need the following :

LEMMA 5. — *Let G be a finite S-group of order m. Suppose m is invertible in $\mathcal{O}_S$. Then G is étale over S.*

This is well-known, we sketch a proof. By EGA IV[4], 17.6.2 ($a \Leftrightarrow c''$), we are reduced to the case $S = \mathrm{Spec}(k)$, where k is an algebraically closed field. In that case, the problem is to show that the connected component G^0 of G is trivial. If $H = G^0 \neq 1$, then $\mathrm{char}(k) = p \neq 0$, and p divides the order of $G^0 = H$; in fact, as in the proof of lemma 1, a non-trivial k-derivation of $\Gamma(H, \mathcal{O}_H)$ defines a non trivial homomorphism $H' \to \mathbf{G}_a$ of the dual of H into the additive group, hence either $\boldsymbol{\alpha}_p \subset H$ or $\boldsymbol{\mu}_p \subset H$ (in fact, it is known that the order of a finite connected k-group, commutative or not, is a power of the characteristic exponent of k, *cf.* [1], $\mathrm{VII_B}$.5.2, theorem). As m is invertible in $\mathcal{O}_S$ however, the characteristic of k does not divide the order of G^0, and the lemma is proved.

Proof of lemma 4. — Suppose $G = \mathrm{Spec}(A)$ is an R-group of order p. For each $v \in M$ we have a diagram of injective maps

$$\begin{array}{ccc} A & \xrightarrow{i_v} & A \otimes_R R_v \\ \downarrow & & \downarrow \\ A \otimes_R K & \xrightarrow{i_v} & A \otimes_R K_v \end{array}$$

in which we can view the vertical arrows as inclusions. Then

$$A = \{ f \in A \otimes_R K \mid i_v f \in A \otimes_R R_v,\ \forall\, v \in M \}.$$

Indeed, this holds for any projective R-module A, because it is true for $A = R$, hence for A free, hence for A a direct summand of a free R-module.

On the other hand, the multiplication and comultiplication in A are induced by the same operations in $A \otimes_R K$. Thus we can recover G from its generic fiber $G \otimes_R K = G_K$ together with the $R_\wp$-groups $G \otimes_R R_\wp$, $\wp \in M$. Since the automorphism groups of the groups G_K, $G_{R_\wp}$ and $G_{K_\wp}$ are all isomorphic (to $\mathbf{F}_p^*$), it follows that the isomorphism class of G is determined by those of G_K and of the $G_{R_\wp}$. Thus the map of E(R) into the fibered product of E(K) and $\prod_\wp E(R_\wp)$ over $\prod_\wp E(K_\wp)$ given by the commutative square (21) is *injective*.

To prove it is surjective, let $H = \operatorname{Spec}(B)$ be a K-group of order p, and for each $\wp \in M$, let $G_\wp = \operatorname{Spec}(A_\wp)$ be an $R_\wp$-group of order p whose generic fiber is $H_\wp = H \times_K K_\wp = \operatorname{Spec}(B \otimes_K K_\wp)$. For each $\wp \in M$ we have a diagram of injective maps

$$\begin{array}{ccc} & & A_\wp \\ & & \big\downarrow \\ B & \xrightarrow{i_\wp} & B \otimes_K K_\wp \end{array}$$

in which we can view the vertical arrow as an inclusion. Since p is invertible in K, the K-algebra B is *étale*, and similarly, the $R_\wp$-algebra $A_\wp$ is étale for every $\wp \in M$ not dividing p (*cf.* lemma 5), hence for all but a finite number of $\wp$ in M. Let

$$A = \{ f \in B \mid i_\wp f \in A_\wp, \ \forall \wp \in M \},$$

and let A^c be the integral closure of A in B. From what has just been said it follows that A^c is a finitely generated R-module spanning B (i. e. is an *order* in B), and that $A_\wp = A^c \otimes_R R_\wp$ for all $\wp$ not dividing m. Since $A_\wp$ is an order in $B \otimes_K K_\wp$ for every $\wp$, we conclude that A is an order in B such that $A \otimes_R R_\wp = A_\wp$ for all $\wp$. The comultiplication in B induces one in A which makes $G = \operatorname{Spec}(A)$ an R-group of order p such that $G \times_R R_\wp = G_\wp$ for each $\wp$ and $G \times_R K = H$. This concludes the proof of lemma 4.

Let C_K denote the idèle class group of K, and for each $\wp \in M$, let $U_\wp$ denote the group of units in $R_\wp$.

LEMMA 6. — *There are canonical bijections*

(22) $$E(K) \cong \operatorname{Homcont}(C_K, \mathbf{F}_p^*),$$

(23) $$E(K_\wp) \cong \operatorname{Homcont}(K_\wp^*, \mathbf{F}_p^*) \qquad (\wp \in M),$$

and

(24) $$E(R_\wp) \cong \operatorname{Homcont}(K_\wp^*/U_\wp, \mathbf{F}_p^*) \qquad (\wp \in M, \ \wp \text{ not} \mid p),$$

where Homcont *denotes continuous homomorphisms. Via these bijections the arrows in the diagram* (21) *are induced by the canonical homomorphisms* $K_\nu^* \to C_K$ *and* $K_\nu^* \to K_\nu^*/U_\nu$.

This is clear from lemma 4 and remark (6) of section 2, using the following commutative diagram :

$$\begin{tikzcd}
C_K \arrow[r] & \pi(K)^{ab} \\
K_\nu^* \arrow[u] \arrow[d] \arrow[r] & \pi(K_\nu)^{ab} \arrow[u] \arrow[d] \\
K_\nu^*/U_\nu \arrow[r] & \pi(R_\nu)^{ab}.
\end{tikzcd}$$

The horizontal arrows are the reciprocity law homomorphisms. It is well known that they become isomorphisms if the groups on the left are replaced by their completions with respect to their open subgroups of finite index (for example, *cf.* [3], 2.7 and [4], 5.1). Hence they induce isomorphisms of the groups of continuous characters with values in a finite group like $\mathbf{F}_p$.

Let M_p denote the set of $\nu \in M$ such that ν divides p. For $\nu \in M_p$, let k_ν denote the residue field of R_ν, let q_ν be the number of elements in k_ν, and let $x \mapsto \tilde{x}$ denote the residue class map $R_\nu \to k_\nu$.

LEMMA 7. — *Suppose* $\nu \in M_p$. *Let* $a \in K_\nu^*$, *and let* $\varphi_a \in$ Homcont $(K_\nu^*, \mathbf{F}_p^*)$ *be the homomorphism which corresponds by* (23) *to the isomorphism class of the* K_ν-*group* $(G_a^{p^{a-1}})_{K_\nu}$ (*cf.* remark 5 of section 2). *Then*

$$\varphi_a(x) = \tilde{c}(a, x)^{\frac{q_\nu - 1}{p-1}} = N_{k_\nu/\mathbf{F}_p}(\tilde{c}(a, x)), \qquad \text{for } x \in K_\nu^*, \tag{25}$$

where

$$c(a, x) = (-1)^{\nu(a)\nu(x)} \frac{a^{\nu(x)}}{x^{\nu(a)}}.$$

In particular,

$$\varphi_a(u) = (\tilde{u})^{-\nu(a)} = (N_{k_\nu/\mathbf{F}_p}(\tilde{u}))^{-\nu(a)}, \qquad \text{for } u \in U_\nu. \tag{26}$$

By (20) we have

$$\varphi_a(x) = \chi_\nu^{-1}\left(\sqrt[p-1]{a}^{(\sigma_x - 1)}\right) = \left(\frac{\sigma_x \beta}{\beta}\right),$$

where σ_x is the automorphism of the maximal abelian extension K^{ab} of K which corresponds to x under the reciprocity law, and where $\beta \in K^{ab}$ with $\beta^{p-1} = a$. In other words, $\varphi_a(x) = (a, x)_\nu$, the $(p-1)$ norm residue symbol for K_ν (*cf.* [2], chap. XIV, § 2, propos. 6). The lemma now follows from the explicit formula for the tame norm residue symbol (*loc. cit.*, prop. 8 and corollary).

If G is an R-group of order p, we shall denote by $\varphi^G \in \mathrm{Hom}(C_K, \mathbf{F}_p^*)$ the idèle class character determined by $G \otimes_R K$ via (22), and by φ_ν^G the corresponding character of K_ν^*, for each $\nu \in M$. For each $\nu \in M_p$, we let $n_\nu^G = \nu(a)$, where $a \in R_\nu$ is such that $G \otimes_R R_\nu \cong (G_a^{p/a})_{R_\nu}$ in the notation of remark 5 of section 2. Note that a is determined modulo U_ν^{p-1} by $G \otimes R_\nu$, hence n_ν^G is uniquely determined by G.

THEOREM 3. — *The map* $G \mapsto (\varphi^G, (n_\nu^G)_{\nu \in M_p})$ *gives a bijection between the isomorphism classes of* R*-groups of order* p *and the systems* $(\psi, (n_\nu)_{\nu \in M_p})$ *consisting of a continuous homomorphism* $\psi : C_K \to \mathbf{F}_p^*$ *and for each* $\nu \in M_p$ *an integer* n_ν *such that* $0 \leqq n_\nu \leqq \nu(p)$, *which satisfy the following two conditions :*

(i) *For* $\nu \in M - M_p$, ψ *is unramified at* ν, *i. e.* $\psi_\nu(U_\nu) = 1$;

(ii) *For* $\nu \in M_p$, $\psi_\nu(u) = (N_{k_\nu/\mathbf{F}_p}(\tilde{u}))^{-n_\nu}$ *for all* $u \in U_\nu$;

here $\psi_\nu : K_\nu^* \to \mathbf{F}_p^*$ *denotes the local character induced by* ψ *via the canonical map* $K_\nu^* \to C_K$.

Proof. — Let G be an R-group of order p. Then $0 \leqq n_\nu^G \leqq \nu(p)$ because $n_\nu^G = \nu(a)$ where a is an element of R_ν dividing p in R_ν. The character φ_ν^G is unramified at each $\nu \in M - M_p$ by (24). For $\nu \in M_p$, the character φ_ν^G satisfies (ii) by (26). Hence the system $(\varphi^G, (n_\nu^G)_{\nu \in M_p})$ satisfies the conditions of the theorem.

Conversely, let $(\psi, (n_\nu)_{\nu \in M_p})$ be a system satisfying the conditions of the theorem. By lemma 6, there exists a K-group H of order p, determined up to isomorphism, which isomorphism class corresponds to ψ under the bijection (22). Similarly, by (i) and lemma 6, there exists for each $\nu \in M - M_p$ an R_ν-group G_ν, determined up to isomorphism, whose isomorphism class corresponds to ψ_ν under the bijection (24), and we have, again by lemma 6,

$$G_\nu \otimes_{R_\nu} K_\nu \cong H \otimes_K K_\nu. \tag{27}$$

By lemma 4, the theorem will be proved if we can show for each $\nu \in M_p$ that there exists an R_ν-group $G_\nu \cong G_{a,R}^{p/a}$ (*cf.* remark 5 of section 2) determined up to isomorphism, such that $\nu(a) = n_\nu$ and such that (27) holds. By remark 5 and lemma 7, this amounts to showing that there exists an a dividing p in R_ν such that $\nu(a) = n_\nu$, and $\psi_\nu = \varphi_a$ (in the notation of lemma 7), and that these conditions determine a up to multiplication by an element of U_ν^{p-1}. Since the pairing

$$(\ ,\ )_\nu : \ K_\nu^*/(K_\nu^*)^{p-1} \times K_\nu^*/(K_\nu^*)^{p-1} \to \mathbf{F}_p$$

is non-degenerate (*cf.* [2], chap. XIV, § 2, propos. 7 (vi)), there exists an $a \in K_v$, unique $\bmod (K_v^*)^{p-1}$, such that $\varphi_a = \psi_v$. Comparison of (26) and (ii) shows then that $v(a) \equiv n_v \bmod (p-1)$, because the norm homomorphism $k_v^* \to \mathbf{F}_p^*$ is surjective and $\mathbf{F}_p^*$ is cyclic of order $p-1$. Changing a by a $(p-1)$-th power, we can achieve that $v(a) = n_v$, and a is then determined $\bmod (K_v^{p-1} \cap U_v)$, i. e. $\bmod U_v^{p-1}$. Since $0 \leqq n_v \leqq v(p)$, a is an element of R_v dividing p. This completes the proof of theorem 3.

As an example, let us consider the case in which R is the ring of algebraic integers in K. Then, for a given family of integers $(n_v)_{v \in M_p}$, there is either no idèle class character ψ satisfying (i) and (ii), or the set of all such is a principal homogeneous space under the group of homomorphisms of the ideal class group of K into $\mathbf{F}_p^*$. In particular, if the class number of K is prime to $(p-1)$, then there is at most one ψ for each family (n_v). The number of families (n_v) is $\prod_{v \in M_p} (v(p) + 1)$. If p is prime in R, then there are just two families, namely $n_v = 0$, or $n_v = 1$, for the unique v above p. Hence :

COROLLARY. — *If* $R = \mathbf{Z}$, *or more generally, if* R *is the ring of integers in a field of class number prime to* $p-1$ *such that* pR *is a prime ideal in* R, *then the only* R-*groups of order* p *are* $(\mathbf{Z}/p\mathbf{Z})_R$ *and* $\boldsymbol{\mu}_{p,R}$.

REFERENCES.

[1] P. GABRIEL, *Généralités sur les groupes algébriques. Étude infinitésimale des schémas en groupes et groupes formels. Groupes formels*, Exp. VI_A, VII_A and VII_B, Séminaire de Géométrie algébrique, 1963-1964; I. H. E. S. : *Schémas en groupes*, Séminaire dirigé par M. Demazure et A. Grothendieck; fasc. 2 *b*.

[EGA] A. GROTHENDIECK et J. DIEUDONNÉ, *Éléments de géométrie algébrique*. Chap. IV : *Étude locale des schémas et des morphismes de schémas* (4e partie), I. H. E. S., Publ. Math. No. 32, 1967.

[2] J.-P. SERRE, *Corps locaux*, Act. Sc. Ind., 1296, Hermann, Paris, 1962.

[3] J.-P. SERRE, *Local class field theory*; Chap. VI of : *Algebraic number theory*. Edited by J. W. S. Cassels and A. Fröhlich, Academic Press, 1967.

[4] J. T. TATE, *Global class field theory*; Chap. VII of the volume mentioned in the preceding reference.

[5] A. WEIL, *Numbers of solutions of equations in finite fields* (*Bull. Amer. Math. Soc.*, vol. 55, 1949, p. 497-508.)

(Manuscrit reçu le 8 juillet 1969.)

John T. TATE,
Department of Mathematics,
Harvard University,
Cambridge, Mass. 02138, U. S. A.

Frans OORT,
Mathematisch Instituut,
Roetersstraat 15, Amsterdam C,
The Netherlands.