

SÉMINAIRE N. BOURBAKI

JEAN-PIERRE SERRE

Groupes p -divisibles

Séminaire N. Bourbaki, 1968, exp. n° 318, p. 73-86

<http://www.numdam.org/item?id=SB_1966-1968__10__73_0>

© Association des collaborateurs de Nicolas Bourbaki, 1968, tous droits réservés.

L'accès aux archives du séminaire Bourbaki (<http://www.bourbaki.ens.fr/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). 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/>

GROUPES p -DIVISIBLES (d'après J. TATE)

par Jean-Pierre SERRE

On sait que de nombreuses propriétés des variétés abéliennes (par exemple celles liées à leur fonction zêta) peuvent se "lire" sur le groupe des points d'ordre fini de la variété, considéré comme module galoisien. Dans le cas local, l'étude de ce groupe s'est d'abord faite en utilisant le groupe formel (au sens de Dieudonné et Lazard) attaché à la variété abélienne ; c'est ainsi, par exemple, que l'on démontre le théorème de Lutz-Nagell [7], ou que l'on étudie les courbes elliptiques ayant une réduction de hauteur 2 (cf.[9]). Toutefois, on s'est aperçu récemment qu'il y a intérêt à remplacer les groupes formels par une nouvelle notion, plus souple, celle de groupe p -divisible. Le but de cet exposé est d'indiquer les principaux résultats connus sur ces groupes. Ces résultats sont en très grande partie dus à Tate - parfois en collaboration. Ils ont été exposés dans plusieurs séminaires : Woods Hole [4], Collège de France [10], Driebergen [13].

§ 1. La notion de groupe p -divisible.

Dans tout ce qui suit, p désigne un nombre premier.

Soit R un anneau commutatif (ou un schéma, si l'on préfère) et soit h un entier ≥ 0 . Un groupe p -divisible de hauteur h sur R est un système

$$G = (G_n, i_n), \quad n \geq 1,$$

vérifiant les conditions suivantes :

(a) G_n est un schéma en groupes commutatif [1] sur R , localement libre de rang p^{nh} .

(b) $i_n : G_n \rightarrow G_{n+1}$ est un homomorphisme de schémas en groupes.

(c) La suite

$$0 \rightarrow G_n \xrightarrow{i_n} G_{n+1} \xrightarrow{p^n} G_{n+1}$$

est exacte.

Si A_n désigne l'algèbre affine associée à G_n , la condition (a) signifie que A_n est muni d'une structure de bigèbre vérifiant certaines conditions (bicommutativité et biassociativité, notamment), et que A_n est un R -module projectif de rang p^{nh} . Lorsque R est local (ce qui est le cas essentiel dans les applications), cette dernière condition revient simplement à dire que A_n est un R -module libre de rang p^{nh} .

Quant à (c), elle signifie simplement que G_n s'identifie, au moyen de i_n , au noyau de $p^n : G_{n+1} \rightarrow G_{n+1}$; en particulier, i_n est une immersion fermée, et l'on peut considérer G comme la "réunion" des G_n (exactement comme le groupe $\mathbb{Q}_p/\mathbb{Z}_p$ est réunion des groupes $\mathbb{Z}/p^n\mathbb{Z}$).

Remarque. Si n, m sont des entiers ≥ 0 , la multiplication par p^n applique G_{n+m} dans G_m , et l'on démontre que l'on a une suite exacte (au sens de [1], exposé IV) :

$$0 \rightarrow G_n \rightarrow G_{n+m} \rightarrow G_m \rightarrow 0.$$

Exemples de groupes p -divisibles.

1/ Groupes étales.

Supposons que $\text{Spec}(R)$ soit connexe, et soit π son groupe fondamental. Soit T un \mathbb{Z}_p -module libre de rang h sur lequel π opère continûment ;

les groupes $T_n = T/p^n T$ forment un système inductif de π -modules. On en déduit, par un procédé standard, un système (G_n, i_n) , où les G_n sont étales sur R ; ce système est un groupe p -divisible de hauteur h . Inversement, tout groupe p -divisible étale de hauteur h s'obtient ainsi, de façon essentiellement unique.

Ceci s'applique notamment lorsque R est un corps, le groupe π étant simplement le groupe de Galois de la clôture algébrique de R . D'où une équivalence "groupes p -divisibles étales" \Leftrightarrow "représentations p -adiques de π ". De plus, lorsque R est de caractéristique différente de p , tout groupe p -divisible sur R est étale.

2/ Groupes définis par des schémas abéliens.

Soit A un schéma abélien sur R , de dimension relative r . Le noyau A_n de $p^n : A \rightarrow A$ est localement libre de rang p^{nh} , avec $h = 2r$. Le système $A(p)$ formé des A_n est un groupe p -divisible de hauteur h .

Lorsque R est un corps de caractéristique $\neq p$, le groupe $A(p)$ est étale, et équivaut (d'après 1/ ci-dessus) à la donnée du "module de Tate" $T_p(A)$, considéré comme module galoisien.

3/ Dual d'un groupe p -divisible.

Soit $G = (G_n, i_n)$ un groupe p -divisible de hauteur h . Le dual (au sens de Cartier) G'_n de G_n est défini par la bigèbre duale de celle de G_n ; on peut aussi le définir comme représentant le foncteur $\underline{\text{Hom}}_{\text{gr}}(G_n, G_m)$, cf. [1], exposé VIII. Les homomorphismes $G_{n+1} \rightarrow G_n$ induits par la multiplication par p définissent par transposition des homomorphismes $i'_n : G'_n \rightarrow G'_{n+1}$. Le système $G' = (G'_n, i'_n)$ est un groupe p -divisible de hauteur h , appelé le dual de G .

Le dual d'un groupe étale est un groupe de type multiplicatif, au sens de [1], loc.cit.

4/ Groupes p-divisibles et groupes formels.

Supposons, pour simplifier, que R soit un anneau local noethérien complet, de caractéristique résiduelle p . Soit Γ un groupe formel commutatif de dimension d sur R , au sens de Dieudonné-Lazard ; l'algèbre Λ associée à Γ est isomorphe à $R[[T_1, \dots, T_d]]$. Supposons en outre que la multiplication par p dans Γ soit une isogénie de degré p^h (i.e. fasse de Λ un Λ -module libre de rang p^h). On peut alors définir le noyau Γ_n de $p^n : \Gamma \rightarrow \Gamma$ comme un schéma en groupes sur R . Le système $\Gamma(p)$ des Γ_n est un groupe p -divisible de hauteur h sur R ; sa connaissance équivaut à celle de Γ (en effet, Λ est limite projective des algèbres des Γ_n). On obtient ainsi une équivalence de catégories entre :

- groupes p -divisibles connexes
- groupes formels commutatifs où p est une isogénie.

De plus, on montre que tout groupe p -divisible G sur R est extension d'un groupe étale par un groupe connexe G° , sa composante neutre. La dimension d de G° (considéré comme groupe formel) est appelée la dimension de G . Si G' est le dual de G , et si $d' = \dim(G')$, on a :

$$h = d + d' .$$

Cela résulte des propriétés des opérateurs V et F de la théorie de Dieudonné, cf. par exemple Manin [8], ou [1], exposé VII.

Cas particulier. Soit E une courbe elliptique définie sur R , et ayant une "bonne réduction" (i.e. définissant un schéma abélien). Le groupe p -divisible $E(p)$ attaché à E a pour invariants $d = 1$, $d' = 1$ et $h = 2$. Si la réduction \tilde{E} de E est de hauteur 2 (cf.[9], § 2), $E(p)$ est connexe ; c'est un groupe formel de hauteur 2. Si \tilde{E} est de hauteur 1, $E(p)$ est une

extension d'un groupe formel de hauteur 1 (de type multiplicatif) par un groupe étale de hauteur 1 correspondant aux points d'ordre une puissance de p de \tilde{E} ; lorsque cette extension est triviale, E est le "relèvement canonique" de \tilde{E} , cf. § 5.

§ 2. Le premier théorème fondamental. (Tate [13]).

On suppose R intègre, intégralement clos, noethérien, et de corps des fractions K de caractéristique zéro. On s'intéresse au foncteur qui associe à tout groupe p -divisible G sur R le groupe correspondant $G_K = G \times_R K$ sur K .

THÉORÈME 1. Sous les hypothèses ci-dessus, le foncteur $G \mapsto G \times_R K$ est pleinement fidèle.

Noter que, puisque K est de caractéristique zéro, le groupe G_K est étale, donc équivaut à la donnée d'un module galoisien $T_p G$, appelé le module de Tate de G . Le théorème 1 peut donc se reformuler ainsi :

THÉORÈME 1'. Si G_1 et G_2 sont deux groupes p -divisibles sur R , l'homomorphisme canonique

$$\text{Hom}_R(G_1, G_2) \rightarrow \text{Hom}_{\text{Gal}}(T_p G_1, T_p G_2)$$

est un isomorphisme.

COROLLAIRE 1. Si $f : G_1 \rightarrow G_2$ définit un isomorphisme de $T_p G_1$ sur $T_p G_2$, c'est un isomorphisme.

COROLLAIRE 2. Si G est un groupe p -divisible, tout endomorphisme du module galoisien $T_p G$ provient d'un endomorphisme de G .

Pour la démonstration de ces résultats, voir Tate [13]. Indiquons simplement quelles sont les différentes étapes :

(i) On se ramène au cas où R est un anneau de valuation discrète complet, de caractéristique résiduelle p , et de corps résiduel algébriquement clos.

(ii) Si d et d' désignent les dimensions de G et G' (cf. § 1, 4/), on montre que le module galoisien $T_p G$ détermine (d, d') . On utilise pour cela les propriétés de $T_p G$ données au § 4 ci-après (cor. au théorème 2).

(iii) On montre que le discriminant de l'algèbre A_n associée au groupe G_n est engendré par $p^{dnp^{hn}}$.

(iv) En combinant (ii) et (iii), on établit le cor. 1.

(v) On déduit le théorème 1' du corollaire 1 par une construction de "graphe" convenable.

Remarques.

1) On ignore si le théorème 1 reste vrai lorsque K est un corps de caractéristique p .

2) On aimerait pouvoir compléter le théorème 1' en disant quels sont les modules galoisiens qui sont de la forme $T_p G$, avec G p -divisible. Les résultats du § 4 donnent en tout cas des conditions nécessaires (cf. cor. au théorème 3).

§ 3. Quelques propriétés de la complétion de la clôture algébrique d'un corps local. (Tate [13], Sen (non-publié).)

Soit R un anneau de valuation discrète complet, de corps résiduel k de caractéristique p , et de corps des fractions K . Soit \bar{K} une clôture algébrique de K , et soit π le groupe de Galois de \bar{K}/K . On sait que la valuation de K se prolonge de manière unique en une valuation (à valeurs

dans \mathcal{Q}) de \bar{K} ; soit C le complété de \bar{K} pour la topologie correspondante. Le groupe π opère par continuité sur C . Tate s'est aperçu que les propriétés du π -module C sont intimement liées à celles des groupes p -divisibles sur R (cf. § 4, ainsi que [13]). Il a été amené en particulier aux résultats suivants :

(i) Le corps des invariants de π dans C est réduit à K .

Cela résulte de :

(ii) Il existe un entier $n(K)$ jouissant de la propriété suivante :

Pour toute extension galoisienne finie L/K , d'anneau de valuation A_L , le groupe $H^1(\text{Gal}(L/K), A_L)$ est annulé par $p^{n(K)}$.

Tate démontre (ii) en "montant" de K à \bar{K} au moyen d'une extension intermédiaire K' à groupe de Galois isomorphe à \mathbb{Z}/p (cf. [13]).

Comme autres résultats, signalons :

(iii) Le K -espace vectoriel $H^1(\pi, C)$ est de dimension 1. (Noter la différence entre C et \bar{K} !)

Soit H le module de Tate du groupe multiplicatif G_m , et soit $C(n)$ le produit tensoriel de C avec la puissance tensorielle n -ème de H . Alors :

(iv) Si $n \neq 0$, on a $H^0(\pi, C(n)) = H^1(\pi, C(n)) = 0$.

Remarque. Shankar SEN a récemment amélioré (ii), en montrant qu'on peut prendre $n(K)$ égal à 1 si $p \neq 2$ et $n(K) = 2$ si $p = 2$.

§ 4. La décomposition de $T_p G \otimes C$. (Tate [13].)

On conserve les notations et hypothèses du § 3, et l'on note \mathfrak{m} l'idéal maximal de R . On considère un groupe p -divisible G de hauteur h sur

R ; on note G' son dual.

a/ Le groupe des points de G à valeurs dans R .

Si N est un entier ≥ 1 , définissons le groupe des points de G à valeurs dans $R/m^N R$ par la formule $G(R/m^N R) = \lim_{\rightarrow} G_N(R/m^N R)$ et définissons $G(R)$ comme la limite projective des $G(R/m^N R)$ pour $N \rightarrow \infty$. Lorsque G est connexe, cette définition coïncide avec la définition habituelle des points d'un groupe formel, au moyen de coordonnées. Dans le cas général, si t_G désigne l'espace tangent à la composante neutre G° de G , le logarithme donne un isomorphisme

$$L : G(R) \otimes \mathbb{Q}_p \rightarrow t_G \otimes_R K .$$

b/ Le module $T_p G$.

Il a été défini au § 2 comme le π -module correspondant au groupe p -divisible $G \times_R K$. On peut également définir directement $T_p G/p^n T_p G$ comme le noyau de p^n dans $G(R'_n)$, où R'_n est l'anneau de valuation d'une extension finie assez grande de K .

c/ Relations entre G et G' .

Soit R_C l'anneau de valuation de C . Utilisant la définition de la dualité de Cartier, on obtient un isomorphisme

$$T_p G' \simeq \text{Hom}_{R_C}(G \times_R R_C, \mathbb{G}_m) .$$

Si $H = T_p(\mathbb{G}_m)$, on déduit d'abord de là un accouplement

$$T_p G' \times T_p G \rightarrow H ,$$

dont on montre facilement qu'il met ces deux modules en dualité.

Si U_C est le groupe des éléments inversibles de R_C congrus à 1, on en déduit aussi un homomorphisme.

$$G(R_C) \rightarrow \text{Hom}(T_p G' , U_C) ,$$

d'où, par restriction à $G(R)$, un homomorphisme

$$\alpha : G(R) \rightarrow \text{Hom}_{\pi}(\mathbb{T}_p G', U_C) .$$

Par passage au logarithme, α définit une application K -linéaire

$$d\alpha : t_G \otimes K \rightarrow \text{Hom}_{\pi}(\mathbb{T}_p G', C) .$$

THÉORÈME 2. Les applications α et $d\alpha$ sont des isomorphismes.

La démonstration utilise l'égalité $h = d + d'$, ainsi que les propriétés de C énoncées au § 3 (cf. [13]).

COROLLAIRE. Le module galoisien $\mathbb{T}_p G$ détermine les invariants d et d' de G .

En effet, $\mathbb{T}_p G$ détermine $\mathbb{T}_p G'$, et le th. 2 montre que $d = \text{rg.} t_G$ est égal à la dimension du K -espace vectoriel $\text{Hom}_{\pi}(\mathbb{T}_p G', C)$.

$d/$ La décomposition de Hodge de $\mathbb{T}_p G \otimes C$.

THÉORÈME 3. Le π -module $\mathbb{T}_p G \otimes C$ est canoniquement isomorphe à la somme directe

$$t_G \otimes C(1) \oplus \text{Hom}(t_{G'}, C) .$$

(On note $C(1)$ le produit tensoriel de C et de H , cf. § 3.)

Plus précisément, l'homomorphisme $d\alpha$, appliqué à G et G' , permet de définir des applications :

$$0 \rightarrow t_G \otimes C(1) \rightarrow \mathbb{T}_p G \otimes C \rightarrow \text{Hom}(t_{G'}, C) \rightarrow 0 .$$

Tate démontre, par un calcul de dimensions, que cette suite est exacte, puis, en utilisant la propriété (iv) du § 3, il montre qu'elle se scinde de façon unique.

COROLLAIRE. Le π -module $T_p G \otimes C$ est somme directe de d modules isomorphes à $C(1)$ et de d' modules isomorphes à C .

Remarque. Soit X un schéma projectif et lisse sur R , et soit G le groupe p -divisible associé à la variété d'Albanese de X . On peut interpréter $T_p G$ comme le premier groupe d'homologie p -adique (étale) de $X_C = X \times_R C$ (à torsion près), et le théorème 3 apparaît comme un analogue p -adique de la décomposition de Hodge

$$H^1(X_C) = H^{1,0}(X_C) \oplus H^{0,1}(X_C),$$

le corps C jouant le rôle du corps des nombres complexes.

On peut se demander s'il existe des décompositions analogues en dimension ≥ 2 (elles ne peuvent en tout cas pas correspondre à des groupes p -divisibles - il faut trouver autre chose). Même en dimension 1, le cas d'une variété abélienne ayant une mauvaise réduction n'est pas réglé.

§ 5. Relèvement des variétés abéliennes.

Soit R un anneau artinien local de corps résiduel de caractéristique p . Soit A_0 une variété abélienne définie sur k , et soit $A_0(p)$ le groupe p -divisible correspondant. Un relèvement de A_0 sur R est un schéma abélien A sur R muni d'un isomorphisme de la réduction $\tilde{A} = A \times_R k$ sur A_0 ; définition analogue pour $A_0(p)$.

THÉOREME 4. Les relèvements de A_0 et de $A_0(p)$ se correspondent bijectivement (à isomorphisme près); cette correspondance est fonctorielle.

Plus correctement, soit \underline{C} la catégorie des schémas abéliens sur R , et $\underline{C}(p)$ la catégorie des couples (A_0, G) où A_0 est une variété abélienne sur k et G un relèvement de $A_0(p)$ sur R . Le théorème 4

signifie que le foncteur $A \mapsto (A \times_{\mathbb{R}} k, A(p))$ est une équivalence $\underline{C} \rightarrow \underline{C}(p)$.

La démonstration du théorème 4 est esquissée dans les notes de Woods Hole [4]. Elle repose essentiellement sur la technique de relèvement de Grothendieck [2], combinée avec une cohomologie fabriquée par Tate.

COROLLAIRE. Soient A et B deux schémas abéliens sur un anneau local noethérien complet, de corps résiduel k de caractéristique p , et soient A_0 et B_0 leurs réductions. Pour qu'un homomorphisme $f_0 : A_0 \rightarrow B_0$ se relève en $f : A \rightarrow B$, il faut et il suffit que l'homomorphisme correspondant de $A_0(p)$ dans $B_0(p)$ se relève en un homomorphisme de $A(p)$ dans $B(p)$.

Lorsque l'anneau est artinien, c'est un cas particulier du théorème. Le cas général en résulte, par passage à la limite, en utilisant [2].

Remarque.

Le théorème 4 équivaut à dire que la variété formelle des modules est la même pour une variété abélienne et pour le groupe p -divisible correspondant. Cela explique l'intérêt qui s'attache à la détermination des modules de groupes p -divisibles, et en particulier des modules de groupes formels (cf. [6], pour le cas de la dimension 1).

Un exemple : le relèvement canonique.

Supposons k parfait, et prenons pour A_0 une variété abélienne de dimension r , telle que le groupe de ses points d'ordre divisant p soit de rang r . (Pour une courbe elliptique, c'est le cas "général", où l'invariant de Hasse est non nul.) On montre alors facilement que $A_0(p)$ est somme directe d'un groupe étale E_0 de hauteur r et d'un groupe M_0 de type multiplicatif. Chacun de ces groupes se relève de façon unique à \mathbb{R} ; soient E et M les groupes correspondants. Vu le théorème 4, il existe

un relèvement A de A_0 tel que $A(p)$ soit isomorphe à la somme directe de E et de M (un relèvement pris au hasard donne simplement une extension de E par M). On appelle A le relèvement canonique de A_0 ; il est fonctoriel en A_0 . Etant défini sur tout anneau local artinien R , de corps résiduel k , il peut aussi être défini (par passage à la limite) sur l'anneau des vecteurs de Witt sur k ; comme l'a remarqué Mumford, le schéma formel ainsi obtenu est un schéma abélien, car toute polarisation $\lambda_0 : A_0 \rightarrow A'_0$ se relève en une polarisation λ de A .

Le foncteur "relèvement canonique" a de nombreuses propriétés agréables. Par exemple, lorsque le corps résiduel k est fini, il fournit des variétés abéliennes de type (CM) au sens de Shimura-Taniyama ; cela résulte de la fonctorialité, combinée avec un résultat récent de Tate [12]. Dans le cas elliptique, il n'est nullement facile d'explicitier les relations entre les invariants modulaires j_0 et j de la courbe et de son relèvement canonique. Pour $p = 5$, par exemple, et $j_0 = 1, 2, 3, 4$, on trouve que la courbe a pour anneau d'endomorphismes $\mathbb{Z} \oplus 2i\mathbb{Z}$, $\mathbb{Z} \oplus \frac{1 + \sqrt{-11}}{2} \mathbb{Z}$, $\mathbb{Z} \oplus i\mathbb{Z}$, et $\mathbb{Z} \oplus \frac{1 + \sqrt{-19}}{2} \mathbb{Z}$; on en déduit que j est égal à $2^3 3^3 11^3$, -2^{15} , $2^6 3^3$ et $-2^{15} 3^3$ respectivement.

§ 6. Applications et compléments.

Signalons :

(1) Un théorème de prolongement des morphismes de schémas abéliens, utilisant essentiellement les théorèmes 1 et 4 (Grothendieck [3]).

(2) Les hypothèses et notations étant celles du § 4, supposons que G soit connexe, et de dimension 1. Soit L l'anneau des endomorphismes de G

sur $R_{\overline{K}}$, et soit π_p l'image du groupe de Galois π dans $\text{Aut}(T_p G)$. Le groupe π_p contient un sous-groupe ouvert du groupe $\text{Aut}_L(T_p G)$; plus précisément les algèbres de Lie de ces deux groupes p -adiques coïncident. (La démonstration utilise la décomposition de Hodge de $T_p G \otimes \mathbb{C}$, cf. [11].)

Lorsque L est de rang h sur \mathbb{Z}_p , $\text{Aut}_L(T_p G)$ s'identifie au groupe L^* , et l'on a des résultats beaucoup plus précis (ils se déduisent facilement de ceux de Lubin-Tate [5]).

Terminons par une question (cf. [13]) :

(3) Y a-t-il d'autres groupes p -divisibles sur \mathbb{Z} que les groupes "triviaux" ?

BIBLIOGRAPHIE

- [1] M. DEMAZURE et A. GROTHENDIECK - Schémas en groupes, Séminaire de Géom. alg., I.H.E.S., 1963-64.
- [2] A. GROTHENDIECK - Géométrie formelle et géométrie algébrique, Séminaire Bourbaki, Mai 1959, n° 182.
- [3] A. GROTHENDIECK - Un théorème sur les homomorphismes de schémas abéliens, Invent. Math., 2, 1966, p. 59-78.
- [4] J. LUBIN, J.-P. SERRE et J. TATE - Elliptic curves and formal groups, Woods Hole Summer Institute, 1964 (notes de séminaire polycopiées, tirées à un nombre restreint d'exemplaires).
- [5] J. LUBIN et J. TATE - One-parameter formal Lie groups over p-adic integer rings, Ann. of Maths., 80, 1964, p. 464-484.
- [6] J. LUBIN et J. TATE - Formal moduli for one-parameter formal Lie groups, Bull. Soc. Math. France, 94, 1966, p. 49-60.
- [7] E. LUTZ - Sur l'équation $y^2 = x^2 - Ax - B$ dans les corps p-adiques, J. reine ang. Math., 177, 1937, p. 237-247.
- [8] J.I. MANIN - La théorie des groupes formels commutatifs sur les corps de caractéristique finie (en russe), Usp. Mat. Nauk, 18, 1963, p. 3-90 [traduction anglaise : Russian Math. Surv., 18, n° 6, p. 1-83].
- [9] J.-P. SERRE - Groupes de Lie ℓ -adiques attachés aux courbes elliptiques, Coll. CNRS, n° 143, Clermont-Ferrand, 1964, p. 239-256.
- [10] J.-P. SERRE - Résumé des cours 1965-66, Annuaire du Collège de France, 1966-67.
- [11] J.-P. SERRE - Sur les groupes de Galois attachés aux groupes p-divisibles, Ecole d'été de Driebergen, 1966.
- [12] J. TATE - Endomorphisms of Abelian varieties over finite fields, Invent. Math., 2, 1966, p. 134-144.
- [13] J. TATE - p-divisible groups, Ecole d'été de Driebergen, 1966.