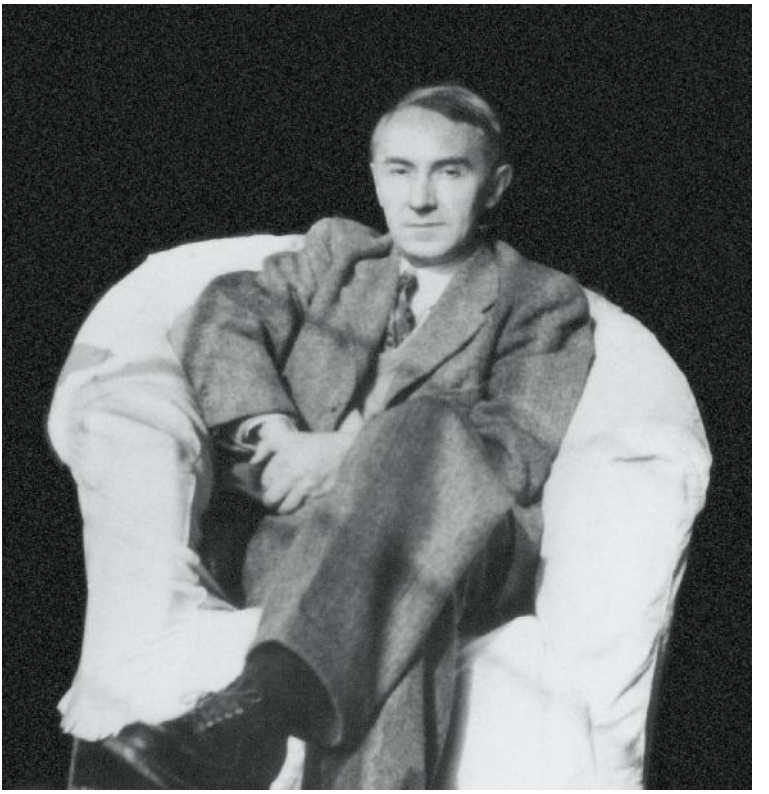
Claude Chevalley
Collected Works
Volume 3



Claude Chevalley

(avec l'aimable autorisation du Mathematisches Forschungsinstitut Oberwolfach / collection des photos de K. Jacobs)

Claude Chevalley
Avec la collaboration de
P. Cartier, A. Grothendieck, M. Lazard

Classification des Groupes Algébriques Semi-simples

The Classification of Semi-simple Algebraic Groups

Collected Works, Volume 3

Texte révisé par P. Cartier

Springer

Editor

Pierre Cartier

IHES et Institut mathématique de Jussieu
35, route de Chartres
F-91440 Bures-sur-Yvette
France
e-mail: cartier@ihes.fr

Library of Congress Control Number: 2004115729

Mathematics Subject Classification (2000): 14xx, 20xx

ISBN 3-540-23031-9 Springer Berlin Heidelberg New York

Typesetting by the author using a Springer LaTeX macro package
Production: LE-TEX Jelonek, Schmidt & Vöckler GbR, Leipzig
Cover design: E. Kirchner, Heidelberg, Germany

Printed on acid-free paper 41/3142YL - 5 4 3 2 1 0

Avertissement au lecteur

Le texte de cet ouvrage correspond au Séminaire dirigé par Claude Chevalley, à l'Ecole Normale Supérieure de Paris, pendant les années universitaires 1956/57 et 1957/58. Il prend naturellement la suite du Séminaire Cartan-Chevalley (ENS, 1955/56) consacré aux fondements de la géométrie algébrique et auquel il sera fait référence par le sigle **SCC** ; il s'appuie aussi sur la classification des algèbres de Lie simples complexes, qui est un des buts du Séminaire S. Lie, tenu à l'ENS en 1954/55. Tous ces Séminaires ont été multigraphiés et diffusés par les soins du Secrétariat Mathématique (P. Belgodère et D. Lardeux) à l'Institut Poincaré.

La réédition de ce texte supposait des choix délicats. Tout d'abord, des quatre rédacteurs, deux sont décédés (Chevalley et Lazard) et Grothendieck s'est muré dans une retraite inaccessible ; l'éventualité d'une simple reproduction en *fac-simile*[1] était à écarter vu les progrès de l'édition scientifique en 50 ans.

Une première option, fortement appuyée par A. Borel pendant plusieurs années, consistait à reprendre les textes signés de Chevalley (chapitres 8, 9, 10, 15 à 24) et à les inclure dans le volume de ses "Œuvres complètes" où seront rassemblés ses articles sur les groupes de Lie. L'inconvénient majeur était de défigurer l'ensemble ; en particulier, les chapitres 11 à 13, signés par Lazard, ont été rédigés en suivant de très près les notes fournies par Chevalley, et constituent une partie importante du développement de la théorie. Le chapitre 14, sur la structure du groupe de Weyl, était une commande de Chevalley à Cartier[2], et constituait un des résultats-clés.

Les chapitres 9 à 24 forment l'essentiel de la création de Chevalley, et représentent un des sommets de la théorie des groupes. Quant au reste du volume, en voici le contenu :

- les chapitres 1, 2 (par Cartier) et 5 (par Grothendieck) sont consacrés aux bases de la géométrie algébrique ;
- les chapitres 3 (par Lazard) et 4, 6 et 7 (par Grothendieck) contiennent un exposé détaillé des résultats de Kolchin et Borel sur les groupes algébriques ;

[1] Comme cela fut l'option retenue pour la réédition du Séminaire Bourbaki en 1996 !

[2] Nous ignorions tous deux le travail de Coxeter, paru vingt ans plus tôt !

– le chapitre 8 est une nouvelle démonstration, par Chevalley, du théorème d'existence des espaces homogènes de groupes algébriques dû à A. Weil et M. Rosenlicht.

Une fois prise la décision de publier le tout, nous hésitâmes un moment à en faire un des volumes des "Œuvres complètes" de Chevalley, vu la part importante des autres rédacteurs[3]. Chevalley lui-même avait insisté sur le fait qu'une publication de ses Œuvres supposerait une révision très soignée. Un texte, écrit et frappé semaine après semaine, par quatre auteurs différents, pour être distribué aux auditeurs au fur et à mesure, n'a pas le même caractère qu'un livre. Beaucoup de collègues consultés m'ont exprimé l'opinion que, malgré un large choix d'excellents ouvrages sur les groupes algébriques, le Séminaire Chevalley représentait, cinquante ans après sa rédaction, un des endroits où apprendre la théorie. J'ai été pris dans l'engrenage de la révision, à l'image d'un restaurateur d'une toile de Vinci ou de Rubens, rempli d'admiration pour le chef-d'œuvre, inquiet quant à ses choix et à ses responsabilités, et désireux de servir l'œuvre sans la trahir. Le lecteur jugera !

Voici, en tout cas, un catalogue des principales modifications (en dehors de la ponctuation, l'orthographe et les coquilles[4]) :

- Aux chapitres 1 et 2, on dispose de deux corps $k \subset K$, et l'on est en train d'étudier les K-points d'une k-variété. Ensuite, il n'y a plus qu'un seul corps $k = K$; les notations k et K alternaient selon les chapitres, et l'on a choisi K de manière uniforme.
- La terminologie a été unifiée et rendue conforme aux usages actuels ; quelques exemples : *réflexion*, sous-groupe *invariant*, composante *neutre*, isomorphisme spécial *attaché* à une isogénie,... Pour les notations, Chevalley introduit les excellentes notations $X^{\mathbb{Q}}(T)$, et $\langle \gamma, \alpha \rangle$ pour la dualité entre $\gamma \in \Gamma(T)$ et $\alpha \in X(T)$; mais il ne s'y tenait pas systématiquement.
- Pour Chevalley, les variétés algébriques étaient irréductibles, mais les sous-groupes fermés (irréductibles ou non) d'un groupe algébrique étaient des groupes algébriques. Il a donc fallu vérifier (et corriger à l'occasion) les hypothèses de connexité. En particulier, les groupes semi-simples doivent être connexes dans ce cadre, et ce point était assez ambigu sous la plume de Chevalley.
- La notion fondamentale de groupe algébrique semi-simple *simplement connexe* était utilisée sans aucune définition.
- La rédaction d'un texte semaine après semaine amène à des reprises et des errata ; cela a conduit à déplacer quelques sections, en particulier la section 6.1 se trouvait au chapitre 5, à une place peu naturelle. La section 4.6 est dans la même situation.

[3] Pour des raisons analogues, le séminaire H. Cartan a été publié indépendamment de ses "Œuvres complètes".

[4] Les notes de bas de pages sont nouvelles.

- Chevalley avait l'habitude d'écrire de longues tirades sans la moindre respiration. En particulier, les chapitres 8, 17, 18, 19 et 24 n'étaient pas fractionnés en sections. A quelques endroits stratégiques, on a inséré le mot "lemme" ou "proposition", pour mettre en exergue un énoncé intermédiaire qui se cachait dans un très long paragraphe.
- La modification la plus substantielle concerne la démonstration du premier théorème fondamental de Chevalley : "Un groupe de Borel B est son propre normalisateur". Cette démonstration était obscurcie par la prétention de traiter simultanément le cas d'un élément semi-simple et celui d'un élément unipotent du normalisateur de B. La récurrence finale était assez peu convaincante. Le texte de Chevalley a été remplacé par une version nouvelle, beaucoup plus détaillée.

Nous avons dû procéder à une nouvelle saisie en TEX, dont Cécile Cheikhchoukh s'est acquittée avec l'égalité d'humeur, la diligence et le soin méticuleux dont elle est coutumière.

J'aimerais dédier cet ouvrage à la mémoire de notre ami commun à Serre et moi-même, Armand Borel, décédé quelques semaines avant la complétion de ce travail, qui lui tenait extrêmement à cœur.

Enfin, je remercie Jean-Pierre Serre, qui m'a donné l'impulsion nécessaire, au printemps 2003, pour reprendre ce travail ingrat ; il s'est aussi chargé de la première lecture de la nouvelle frappe, et de la confection de l'index.

Paris, octobre 2004 *Pierre CARTIER*

Table des Matières

1. Définition des variétés algébriques 1
1.1 Espaces topologiques nœthériens 1
1.2 Systèmes locaux de fonctions 3
1.3 Résultats préliminaires d'algèbre 6
1.4 Spectre des algèbres de type fini 7
1.5 Définition des ensembles algébriques 10

2. Schémas des variétés algébriques 13
2.1 Sous-ensembles algébriques 13
2.2 Produit d'ensembles algébriques 15
2.3 Extension des scalaires 18
2.4 Applications rationnelles 20
2.5 Schémas 25
2.6 Fonctions sur un produit d'ensembles algébriques 30

3. Groupes algébriques (généralités) 33
3.1 Définition d'un groupe algébrique 33
3.2 Composantes d'un groupe algébrique 33
3.3 Engendrement de sous-groupes 34
3.4 Groupes résolubles ou nilpotents 35
3.5 Homomorphismes de groupes algébriques 36
3.6 Appendice. Lemmes de théorie des groupes 37

4. Groupes algébriques affines commutatifs 41
4.1 Généralités sur les représentations linéaires 41
4.2 Sous-groupes fermés d'un groupe algébrique affine 43
4.3 Groupes algébriques diagonalisables 44
4.4 Eléments semi-simples et unipotents 47
4.5 Groupes algébriques affines commutatifs 51
4.6 Connexité des centralisateurs 52

5. Compléments de géométrie algébrique 55
5.1 Discriminant et séparabilité 55
5.2 Ramification et normalisation 58

5.3 Forme géométrique du "Main theorem" de Zariski 61
5.4 Variétés projectives 62
5.5 Appendice I. Localités non ramifiées 65
5.6 Appendice II. Une variante du "Main theorem" de Zariski ... 67

6. Les théorèmes de structure fondamentaux pour les groupes algébriques affines 69
6.1 Espaces de transformations 69
6.2 Le théorème de Lie-Kolchin 70
6.3 Structure des groupes algébriques affines nilpotents 71
6.4 Structure des groupes algébriques affines résolubles et connexes 73
6.5 Sous-groupes de Borel, théorèmes de conjugaison 75
6.6 Théorèmes de densité 78
6.7 Théorèmes de centralisation et de normalisation 80

7. Sous-groupes de Cartan, éléments réguliers. Groupes algébriques affines de dimension 1 83
7.1 Sous-groupes de Cartan 83
7.2 Eléments réguliers 84
7.3 Théorèmes de conservation 86
7.4 Groupes affines de dimension 1 88

8. Espaces homogènes de groupes algébriques 91
8.1 Cohomomorphisme d'une application rationnelle 91
8.2 Variétés quotients 92
8.3 Existence de variétés quotients 95
8.4 Trace d'une fonction 96
8.5 Application aux groupes : construction des espaces homogènes 97
8.6 Propriétés des espaces homogènes 100

9. Le normalisateur d'un groupe de Borel 103
9.1 Un lemme de dévissage 103
9.2 Un lemme de géométrie algébrique 104
9.3 Normalisateur d'un groupe de Borel 105
9.4 Le radical 107
9.5 Les groupes à un paramètre d'un tore 108

10. Les tores singuliers 111
10.1 Cinq lemmes 111
10.2 Les groupes de Borel qui contiennent un tore 112
10.3 Groupes à un paramètre semi-réguliers 115
10.4 Chambres 118

11. Le groupe de Weyl : chambres et réflexions 121
11.1 Préliminaires géométriques (polyèdres convexes) 121
11.2 Quelques précisions sur T, $X(T)$, $\Gamma(T)$ et $\Gamma^{\mathbf{Q}}(T)$ 123
11.3 La décomposition en chambres de $\Gamma^{\mathbf{Q}}(T)$ 124
11.4 Où l'on retrouve les schémas de Dynkin 126

12. Racines 129
12.1 Groupes de Weyl d'ordre 2 129
12.2 Racines d'un groupe algébrique 131
12.3 Réunion et intersection des groupes de Borel contenant un tore maximal 134
12.4 Application aux groupes semi-simples 136

13. Groupes semi-simples : structure de B et de G/B 139
13.1 Propriétés de certains groupes nilpotents à opérateurs 139
13.2 Structure du groupe B^u 142
13.3 Racines fondamentales 145
13.4 Structure de l'espace homogène G/B 147

14. Groupes finis engendrés par des réflexions 151
14.1 Réflexions 151
14.2 Systèmes de racines 152
14.3 Racines fondamentales 152
14.4 Relation d'ordre dans V 154
14.5 Génération du groupe G 157
14.6 Chambres 159
14.7 Remarques finales 159

15. Les systèmes linéaires sur G/B 161
15.1 Compléments au théorème de Bruhat 161
15.2 Les systèmes linéaires de diviseurs 163
15.3 Représentations projectives du groupe G 166

16. Les poids dominants 171
16.1 Groupe linéaire associé à une représentation projective 171
16.2 Poids dominants des représentations projectives simples 172
16.3 Le groupe des poids 175
16.4 Les sous-groupes semi-simples de rang 1 de G 176

17. Les sous-groupes radiciels 179
17.1 Notations 179
17.2 Sous-groupe radiciel associé à un ensemble fermé de racines . . 179
17.3 Groupes quotients des groupes semi-simples 185
17.4 Caractérisation des sous-groupes invariants 187
17.5 Composantes (presque) simples 189

18. Les isogénies 191
18.1 Généralités sur les isogénies 191
18.2 Isomorphisme spécial associé à une isogénie 193
18.3 Propriétés des isomorphismes spéciaux 194
18.4 Comparaison des isogénies 197

19. Les diagrammes de Dynkin 201
19.1 Le diagramme de Dynkin d'un groupe semi-simple 201
19.2 Diagrammes admissibles 202
19.3 Système de racines associé à un diagramme admissible 204
19.4 Racines et poids fondamentaux des divers types 205

20. Les groupes de type A_n 213
20.1 Le groupe $\mathrm{SL}(V)$ 213
20.2 Poids dominants minimaux 214
20.3 Classification des groupes de type A_n 217
20.4 Les représentations simples d'un groupe de rang 1 222

21. Les groupes de type G_2 225
21.1 Deux lemmes 225
21.2 Etude d'un groupe de type G_2 227
21.3 Sur l'algèbre de Lie d'un groupe semi-simple 231
21.4 Algèbre de Lie d'un groupe de type G_2 233
21.5 Isogénies d'un groupe de type G_2 235

22. Les groupes de type C_n 237
22.1 Le groupe $\mathrm{Sp}\, n$ 237
22.2 Le groupe $\mathrm{SO}(2n+1)$ 239
22.3 Les groupes de type C_n 241
22.4 Isogénies d'un groupe de type C_2 243
22.5 Isogénies d'un groupe de type $A_1 + A_1$ 245

23. Existence d'isogénies 247
23.1 Existence de groupes simplement connexes 247
23.2 Isogénies attachées à un même isomorphisme spécial 248
23.3 Enoncé du théorème. Notations 250
23.4 Premières constructions 250
23.5 Présentation d'un groupe semi-simple 253
23.6 Fin de la démonstration du théorème 1 257
23.7 Conséquences et applications 259

24. Conclusion 263

25. Postface 265
25.1 De Galois à Lie et Cartan 265
25.2 Retour aux groupes finis 266
25.3 L'histoire du séminaire 267
25.4 Fondements de la géométrie algébrique 267
25.5 Groupes algébriques 269
25.6 Systèmes de racines 271
25.7 La méthode de Chevalley 272

Index 275

1. Définition des variétés algébriques[1]

On a suivi de près l'exposition de Serre (Ann. of Math., **61**, 1955, p.197-278) en privilégiant les *systèmes locaux de fonctions*, c'est-à-dire les sous-faisceaux du faisceau des fonctions scalaires. On fera dans le prochain exposé le lien avec la théorie des schémas de Chevalley-Nagata. Conformément à une tendance récente, on a mis l'accent sur la topologie de Zariski, qui fournit un langage géométrique plus intuitif que le langage équivalent des spécialisations.

1.1 Espaces topologiques nœthériens

On appellera *espace nœthérien* un espace topologique E, en général non séparé, dans lequel l'ensemble des ouverts vérifie la condition maximale ou encore l'ensemble des fermés la condition minimale.

Un espace topologique E tel que, de tout recouvrement ouvert, on puisse extraire un recouvrement fini, sera appelé *quasi-compact*. Un espace compact est donc un espace quasi-compact séparé. Dans ces conditions, un *espace nœthérien est un espace dans lequel tout ouvert est quasi-compact*. En effet, soit E un espace nœthérien, U un ouvert de E réunion des ouvert U_i ; si V est un élément maximal de l'ensemble des réunions finies d'ouverts U_i, on a $V \cup U_i \subset V$ pour tout i, donc $U_i \subset V$ pour tout i et par suite $V = U$. Réciproquement, soit E un espace topologique dans lequel tout ouvert est quasi-compact, et soit (U_n) une suite croissante d'ouverts de E ; comme la réunion des U_n est quasi-compacte, elle est réunion d'un nombre fini de ces ouverts, donc égale à l'un d'eux, et la suite (U_n) est stationnaire, ce qui prouve que E est nœthérien.

Proposition 1. – *Soit E un espace topologique. Si E est nœthérien, il en est de même de tout sous-espace F de E ; inversement, si E est réunion d'un nombre fini de sous-espaces nœthériens, c'est un espace nœthérien.*

Supposons E nœthérien, et soit (V_n) une suite croissante d'ouverts de F. On a $V_n = F \cap U_n$ avec U_n ouvert dans E pour tout n ; comme E est nœthérien, il existe un entier m tel que $U_n \subset \bigcup_{k \leq m} U_k$ pour $n > m$, d'où $V_n \subset V_m$ pour $n > m$. La suite (V_n) est stationnaire et F est nœthérien.

[1] Exposé de P. Cartier, le 5.11.1956

Supposons E réunion des sous-espaces nœthériens E_i $(1 \leq i \leq p)$, et soit (U_n) une suite croissante d'ouverts de E ; puisque E_i est nœthérien pour chaque i, il y a un entier k_i tel que $U_n \cap E_i$ soit indépendant de n pour $n \geq k_i$. Comme $U_n = \bigcup_i (U_n \cap E_i)$, on a $U_m = U_n$ pour $m, n \geq \sup_i k_i$, et E est nœthérien.

On dira qu'un espace topologique E est *irréductible* s'il est non vide et s'il n'est pas réunion de deux sous-espaces fermés distincts de lui-même. Ceci signifie que l'intersection de deux (et par suite d'un nombre fini) d'ouverts non vides est non vide, ou encore que tout ouvert non vide est partout dense. Il est clair que tout sous-espace ouvert non vide d'un espace irréductible est irréductible.

Proposition 2. – *Soit E un espace topologique.*

a) *Pour qu'un sous-espace F de E soit irréductible, il faut et il suffit que son adhérence $\overline{F}$ le soit.*

b) *Supposons E réunion d'une famille d'ouverts non vides E_i. Pour que E soit irréductible, il faut et il suffit que E_i soit irréductible pour tout i et que l'on ait $E_i \cap E_j \neq \varnothing$ pour tout couple (i, j).*

c) *Si E est irréductible et si f est une application continue définie dans E, $f(E)$ est irréductible.*

L'assertion a) résulte de ce qu'un sous-espace F de E est irréductible si et seulement si l'intersection de deux ouverts de E qui rencontrent F rencontre aussi F, et de ce que les ouverts rencontrant F sont les ouverts rencontrant $\overline{F}$.

La condition énoncée est nécessaire dans b) ; inversement, supposons-la satisfaite et soient U et V deux ouverts non vides de E. Comme E est réunion des E_i, on a $U \cap E_i \neq \varnothing$ et $V \cap E_j \neq \varnothing$ pour i et j convenables ; comme E_i et E_j sont irréductibles et que $E_i \cap E_j$ est un ouvert non vide de E_i et de E_j, il rencontre U et V, et donc $U \cap V$, puisqu'il est irréductible comme ouvert de l'espace irréductible E_i. On a donc prouvé que $U \cap V \neq \varnothing$ et E est irréductible.

Enfin, supposons E irréductible, et soit f une application continue définie dans E ; si U et V sont des ouverts non vides de $f(E)$, les ouverts $f^{-1}(U)$ et $f^{-1}(V)$ de E sont non vides donc $f^{-1}(U) \cap f^{-1}(V) \neq \varnothing$ et par suite $U \cap V \neq \varnothing$, ce qui prouve que $f(E)$ est irréductible.

Proposition 3. – *Soit E un espace topologique. Les parties irréductibles maximales de E sont fermées et leur réunion est E. Toute partie irréductible est contenue dans une partie irréductible maximale. Si de plus E est nœthérien, les parties irréductibles maximales de E sont en nombre fini et pour tout sous-espace F de E, les parties irréductibles maximales de $\overline{F}$ sont les adhérences des parties irréductibles maximales de F.*

Soient $\{F_i\}$ une famille totalement ordonnée de parties irréductibles de E et F leur réunion ; si deux ouverts U et V rencontrent F, ils rencontrent l'un des F_i, et comme F_i est irréductible, $U \cap V$ rencontre F_i donc aussi

F : l'ensemble F est irréductible. Il résulte alors du théorème de Zorn que toute partie irréductible est contenue dans une partie irréductible maximale. La première assertion de la proposition résulte de ce que l'adhérence d'une partie irréductible est irréductible, et de ce que tout point de E étant une partie irréductible est contenu dans une partie irréductible maximale d'après ce qui précède.

Supposons E nœthérien, et soit $\mathbf{A}$ l'ensemble des parties de E qui sont réunion d'un nombre fini de parties fermées irréductibles ; si l'on avait $E \notin \mathbf{A}$, on pourrait trouver une partie fermée G de E, minimale parmi les parties fermées de E qui n'appartiennent pas à $\mathbf{A}$. Comme $\mathbf{A}$ contient $\varnothing$ et les parties fermées irréductibles, G n'est ni vide ni irréductible, donc $G = G_1 \cup G_2$, $G_i \neq G$ étant fermée pour $i = 1, 2$; de là on tire $G_i \in \mathbf{A}$ par le caractère minimal de G ; mais on a alors $G = G_1 \cup G_2 \in \mathbf{A}$, d'où contradiction. On peut donc écrire $E = E_1 \cup \cdots \cup E_n$, les E_i étant irréductibles fermées ; si F est irréductible, comme on a $F = \bigcup_{i=1}^{n} (F \cap E_i)$, il est contenu dans l'un des E_i et par suite lui est égal s'il est irréductible maximal. Les parties irréductibles maximales de E sont donc certaines des parties E_i et sont en nombre fini.

Enfin, si F est un sous-espace de E et si F_i $(1 \leq i \leq n)$ sont les parties irréductibles maximales de F, on a $F = F_1 \cup \cdots \cup F_n$ et $F_i \not\subset F_j$ pour $i \neq j$; on en déduit $\overline{F} = \overline{F}_1 \cup \cdots \cup \overline{F}_n$. On voit comme plus haut que toute partie irréductible maximale de $\overline{F}$ est l'une des $\overline{F}_i$; mais comme $\overline{F}_i \not\subset \overline{F}_j$ pour $i \neq j$ et que toute partie irréductible de $\overline{F}$ est contenue dans une partie irréductible maximale de $\overline{F}$, il en résulte que les parties $\overline{F}_i$ sont les parties irréductibles maximales de $\overline{F}$.

Les parties irréductibles maximales de E se nomment en général les *composantes irréductibles* de E.

1.2 Systèmes locaux de fonctions

Définition 1. – *Soit A un ensemble auxiliaire. Un* système local *de fonctions sur l'espace topologique E à valeurs dans A est une fonction $\mathcal{F}$ qui à tout ouvert U de E associe un ensemble $\mathcal{F}(U)$ d'applications de U dans A satisfaisant aux conditions suivantes :*

(SL1) *Si U et V sont des ouverts tels que $V \subset U$, pour tout $f \in \mathcal{F}(U)$, la restriction $f \mid V$ de f à V appartient à $\mathcal{F}(V)$.*

(SL2) *Si l'ouvert U est réunion des ouverts U_i, toute application f de U dans A telle que $f \mid U_i \in \mathcal{F}(U_i)$ pour tout i, appartient à $\mathcal{F}(U)$.*

Un homomorphisme *du système local $\mathcal{F}$ sur l'espace E dans le système local $\mathcal{F}'$ sur l'espace E' est une application continue φ de E dans E' telle que pour tout ouvert U' de E' et tout $f' \in \mathcal{F}'(U')$, on ait $f' \circ \varphi \in \mathcal{F}(\varphi^{-1}(U'))$.*

Il est clair que le composé de deux homomorphismes est un homomorphisme, que l'application identique de l'espace E est un homomorphisme de $\mathcal{F}$ dans $\mathcal{F}$ pour tout système local $\mathcal{F}$ sur E ; de plus, pour qu'une bijection φ soit un isomorphisme, il faut et il suffit que φ et φ^{-1} soient des homomorphismes.

On va donner deux procédés de définition de systèmes locaux. Soient $\mathcal{F}$ un système local sur l'espace topologique E et T un sous-espace de E ; pour tout ouvert U de T, on notera $\mathcal{G}(U)$ l'ensemble des fonctions f de U dans A qui vérifient la condition suivante :

Pour tout $x \in U$, il existe un voisinage U_x de x dans E et $f_x \in \mathcal{F}(U_x)$ tels que f et f_x coïncident sur $T \cap U_x$.

Il est immédiat que l'application $U \to \mathcal{G}(U)$ est un système local sur T, appelé *restriction* de $\mathcal{F}$ à T et noté $\mathcal{F} \mid T$. L'application identique i de T dans E est un homomorphisme et, si $\mathcal{F}'$ est un système local sur l'espace E', les homomorphismes de $\mathcal{F}'$ dans $\mathcal{F} \mid T$ sont les applications φ de E' dans T telles que $i \circ \varphi$ soit un homomorphisme de $\mathcal{F}'$ dans $\mathcal{F}$. De là, on déduit (*cf.* Bourbaki, Ens. IV, paragraphe 2) que si T_1 est un sous-espace de T, on a $(F \mid T) \mid T_1 = F \mid T_1$.

Le deuxième procédé est fourni par la proposition suivante :

Proposition 4. – *Soient $\mathcal{F}$ un système local sur E et $\mathcal{F}'$ un système local sur E', tous deux à valeurs dans A. Si, pour tout ouvert U de E, $\mathcal{M}(U)$ est l'ensemble des homomorphismes de $\mathcal{F} \mid U$ dans $\mathcal{F}'$, l'application $U \to \mathcal{M}(U)$ est un système local $\mathcal{M}$ de fonctions sur E à valeurs dans E'.*

Soient U un ouvert de E, f un homomorphisme de $\mathcal{F} \mid U$ dans $\mathcal{F}'$ et $V \subset U$ un ouvert ; comme l'application identique $i_{U,V}$ de V dans U est un homomorphisme de $\mathcal{F} \mid V$ dans $\mathcal{F} \mid U$, l'application $f \mid V = f \circ i_{U,V}$ de V dans E est un homomorphisme de $\mathcal{F} \mid V$ dans $\mathcal{F}'$; (SL1) est donc vérifié par $\mathcal{M}$.

Soient maintenant U un ouvert de E réunion des ouverts U_i et f une application de U dans E' telle que $f \mid U_i$ soit un homomorphisme f_i de $\mathcal{F} \mid U_i$ dans $\mathcal{F}'$ pour tout i ; soient U' un ouvert de E' et $h \in \mathcal{F}'(U')$. On a $f^{-1}(U') \cap U_i = f_i^{-1}(U')$ et $(h \circ f) \mid U_i = h \circ f_i \in \mathcal{F}(f^{-1}(U') \cap U_i)$, ce qui prouve que $f^{-1}(U') = \bigcup_i f_i^{-1}(U_i')$ est ouvert et que $h \circ f \in \mathcal{F}(f^{-1}(U') \cap U)$ d'après l'axiome (SL2) pour $\mathcal{F}$; autrement dit f est continue, et est un homomorphisme de $\mathcal{F}$ dans $\mathcal{F}'$; (SL2) est donc vérifié par $\mathcal{M}$.

Nous allons maintenant montrer comment on peut "recoller" des systèmes locaux :

Proposition 5. – *Soient E et A deux ensembles et $(E_i)_{i \in I}$ un recouvrement de E. On suppose donnés pour tout $i \in I$ un système local $\mathcal{F}_i$ sur l'espace X_i et une bijection f_i de X_i sur E_i de sorte que pour tout couple (i, j) on ait les propriétés :*

a) *$f_i^{-1}(E_i \cap E_j) = X_{ij}$ soit ouvert dans X_i ;*

b) *l'application* $f_j^{-1} \circ (f_i \mid X_{ij}) = f_{ij}$ *soit un isomorphisme de* $\mathcal{F}_i \mid X_{ij}$ *sur* $\mathcal{F}_j \mid X_{ji}$.

Il existe alors un système local $\mathcal{F}$ *sur* E *et un seul tel que pour tout* $i \in I$ E_i *soit ouvert dans* E *et que* f_i *soit un isomorphisme de* $\mathcal{F}_i$ *sur* $\mathcal{F} \mid E_i$. *Dans ces conditions, soit* $\mathcal{F}'$ *un système local sur l'espace* E' *; pour qu'une application* f *de* E *dans* E' (resp. de E' dans E) *soit un homomorphisme de* $\mathcal{F}$ *dans* $\mathcal{F}'$ (resp. de $\mathcal{F}'$ dans $\mathcal{F}$), *il faut et il suffit que pour tout* $i \in I$, *l'application* $f \circ f_i$ *de* X_i *dans* E (resp. $f_i^{-1} \circ (f \mid f^{-1}(E_i))$ de $f^{-1}(E_i)$ dans X_i) *soit un homomorphisme de* $\mathcal{F}_i$ *dans* $\mathcal{F}'$ (resp. de $\mathcal{F}' \mid f^{-1}(E_i)$ dans $\mathcal{F}$).

Démontrons d'abord la dernière assertion et notons qu'appliquée à l'application identique de E, elle démontre l'unicité de $\mathcal{F}$. La condition énoncée est nécessaire, puisque le composé de deux homomorphismes est un homomorphisme ; si elle est remplie, pour tout $i \in I$, l'application $f \circ f_i \circ f_i^{-1} = f \mid E_i$ de E_i dans E' (resp. $f_i \circ f_i^{-1} \circ (f \mid f^{-1}(E_i)) = f \mid f^{-1}(E_i)$ de $f^{-1}(E_i)$ dans E) est un homomorphisme de $\mathcal{F} \mid E_i$ dans $\mathcal{F}'$ (resp. de $\mathcal{F}' \mid f^{-1}(E_i)$ dans $\mathcal{F}$) et la proposition 4 montre que f est un homomorphisme puisque les E_i (resp. les $f^{-1}(E_i)$) recouvrent E (resp. E').

Pour démontrer l'existence, nous utiliserons le lemme suivant :

Lemme 1. – *Soient* E *un espace topologique et* $\mathbf{U}$ *une base d'ouverts de* E. *On suppose donné pour tout* $U \in \mathbf{U}$, *un ensemble* $\mathcal{F}_0(U)$ *d'application de* U *dans l'ensemble auxiliaire* A, *de sorte que les axiomes* (SL1) *et* (SL2) *soient vérifiées pour les ouverts de la base* $\mathbf{U}$. *Il existe alors un système local* $\mathcal{F}$ *sur* E *et un seul tel que* $\mathcal{F}(U) = \mathcal{F}_0(U)$ *pour* $U \in \mathbf{U}$.

Soit, pour un ouvert U de E, $\mathcal{F}(U)$ l'ensemble des applications f de U dans A telles que $f \mid V \in \mathcal{F}_0(V)$ pour tout $V \in \mathbf{U}$ contenu dans U. Si $U \in \mathbf{U}$, il est clair que $\mathcal{F}(U) = \mathcal{F}_0(U)$; de plus si $U' \subset U$ et si $f \in \mathcal{F}(U)$, il est clair que $f \mid U' \in \mathcal{F}(U')$. Soit alors (U_α) une famille d'ouverts, U leur réunion, f une application de U dans A ; supposons que l'on ait $f \mid U_\alpha \in \mathcal{F}(U_\alpha)$ pour tout α et soit $V \in \mathbf{U}$ contenu dans U. Si $\mathbf{U}_\alpha$ est l'ensemble des ouverts appartenant à $\mathbf{U}$ contenus dans $V \cap U_\alpha$, on a $f \mid W \in \mathcal{F}_0(W)$ pour $W \in \mathbf{U}_\alpha$ puisque $f \mid U_\alpha \in \mathcal{F}(U_\alpha)$; comme V est réunion de la famille $\bigcup_\alpha \mathbf{U}_\alpha$ d'ouverts, l'axiome (SL2) pour $\mathcal{F}_0$ montre que $f \mid V \in \mathcal{F}_0(V)$. Comme ceci a lieu pour tout $V \in \mathbf{U}$ contenu dans U, on a $f \in \mathcal{F}(U)$ et $\mathcal{F}$ vérifie l'axiome (SL2).

Revenons à la démonstration de la proposition 5 ; transportant par f_i à E_i la topologie de X_i et le système local $\mathcal{F}_i$, on se ramène au cas où $E_i = X_i$, f_i étant l'identité. La condition a) signifie que $E_i \cap E_j$ est ouvert dans E_i, et donc dans E_j et la condition b) que $\mathcal{F}_i \mid E_i \cap E_j = \mathcal{F}_j \mid E_i \cap E_j$. Soit alors $\mathbf{U}$ l'ensemble des parties de E qui sont ouvertes dans l'un des E_i. La condition a) montre alors que $\mathbf{U}$ est une base d'ouverts d'une topologie $\mathcal{T}$ sur E pour laquelle les E_i sont ouverts et qui induit la topologie donnée sur chaque E_i. La condition b) montre que si $U \in \mathbf{U}$, l'ensemble $\mathcal{F}_i(U)$ ne dépend pas de l'indice i tel que $U \in E_i$; on notera $\mathcal{F}_0(U)$ cet ensemble. On peut

alors appliquer le lemme 1 car la vérification des axiomes (SL1) et (SL2) ne fait intervenir que des ouverts contenus dans un même E_i et $\mathcal{F}_i$ vérifie ces axiomes. C.Q.F.D.

1.3 Résultats préliminaires d'algèbre

Rappelons le résultat classique de Hilbert sur les anneaux de polynômes (tous les anneaux sont commutatifs avec unité).

Théorème 1. – *Soient A un anneau, $\mathfrak{a}$ un idéal de A et K un corps algébriquement clos.*

a) *Si $x \in A$, pour que x appartienne à tout idéal premier $\mathfrak{p}$ contenant $\mathfrak{a}$, il faut et il suffit qu'il existe un entier $n > 0$ tel que $x^n \in \mathfrak{a}$.*

b) *Supposons A intègre, et soient A' un sous-anneau de A et x un élément $\neq 0$ de A. Supposons que la structure d'algèbre de A sur A' admette un ensemble fini de générateurs. Il existe alors un élément x' non nul de A' tel que tout homomorphisme de A' dans K qui n'annule pas x' se prolonge en un homomorphisme de A dans K qui n'annule pas x.*

Pour les démonstrations des assertions a) et b), nous renvoyons à **SCC**, exposé 2, proposition 5 et exposé 3, lemme 1.

Corollaire. – *Soient A une algèbre sur le corps k engendrée par un nombre fini d'éléments et K une extension algébriquement close de k. Soit $\mathfrak{a}$ un idéal de A ; pour que tout homomorphisme f de A dans K qui est nul sur $\mathfrak{a}$ annule un élément $x \in A$, il faut et il suffit que $\mathfrak{a}$ contienne une puissance de x.*

Supposons que $\mathfrak{a}$ ne contienne aucune puissance de x et soit $\mathfrak{p}$ un idéal premier tel que $\mathfrak{p} \supset \mathfrak{a}$ et $x \notin \mathfrak{p}$ (th. 1, a)). La classe $\overline{x}$ de x dans l'algèbre intègre $A/\mathfrak{p}$ n'est pas nulle et le b) du théorème 1 montre qu'il existe un homomorphisme $\overline{f}$ de $A/\mathfrak{p}$ dans K tel que $\overline{f}(\overline{x}) \neq 0$, d'où un homomorphisme f de A dans K tel que $f(x) \neq 0$.

Nous rappellerons la définition des anneaux de fractions dans le cas général : soient A un anneau commutatif, S une partie de A. On note $A[S^{-1}]$ le quotient de l'algèbre de polynômes $A[X_s]_{s\in S}$ par l'idéal $\mathfrak{r}$ engendré par les éléments $sX_s - 1$ pour $s \in S$. Soit ϵ_S l'homomorphisme canonique de A dans $A[S^{-1}]$; la classe de X_s mod $\mathfrak{r}$ est l'inverse de $\epsilon_S(s)$ dans $A[S^{-1}]$ et les homomorphismes f de $A[S^{-1}]$ dans un anneau B correspondent biunivoquement par la formule $f' = f \circ \epsilon_S$ aux homomorphismes f' de A dans B tels que $f(S)$ se compose d'éléments inversibles de B.

De ce qui précède, on déduit que si $S \subset S'$, il existe un homomorphisme $\epsilon_{S,S'}$ et un seul de $A[S^{-1}]$ dans $A[S'^{-1}]$ tel que $\epsilon_{S,S'} \circ \epsilon_S = \epsilon_{S'}$ et l'on a $\epsilon_{S',S''} \circ \epsilon_{S,S'} = \epsilon_{S,S''}$ pour $S \subset S' \subset S''$; si S' est l'ensemble des produits de suites finies d'éléments de S et si S'' se compose des éléments $x \in A$ tels qu'il existe $y \in A$ avec $xy \in S'$, ceci montre aussi que $\epsilon_{S,S'}$ et $\epsilon_{S',S''}$ sont des

isomorphismes. De plus, si S est réunion de la famille filtrante croissante S_α, $A[S^{-1}]$ est limite inductive des $A[S_\alpha^{-1}]$ par rapport aux homomorphismes $\epsilon_{S_\alpha,S}$. Enfin, on notera que $A[(S \cup S')^{-1}]$ est isomorphe canoniquement à $A[S^{-1}][S'^{-1}]$ et $A[x^{-1}, y^{-1}]$ à $A[(xy)^{-1}]$.

Lemme 2. – *Supposons que le produit de deux éléments de S soit dans S. Tout élément de $A[S^{-1}]$ est alors de la forme $a/s = \epsilon_S(a)\,\epsilon_S(s)^{-1}$ ($a \in A$, $s \in S$) et les opérations de $A[S^{-1}]$ se traduisent par les formules :*

$$a/s + a'/s' = (as' + a's)/ss' \tag{1}$$

$$a/s \cdot a'/s' = aa'/ss' \tag{2}$$

(3) *$a/s = a'/s'$ équivaut à l'existence de $s'' \in S$ tel que $s''(as' - a's) = 0$.*

Les formules (1) et (2) se démontrent par un calcul facile ; les éléments de la forme a/s engendrent dans tous les cas l'anneau $A[S^{-1}]$, mais si le produit de deux éléments de S est dans S, ils forment un anneau d'après les formules (1) et (2), d'où la première assertion. Nous allons démontrer que lorsque S est quelconque (*i.e.* même lorsque S n'est pas stable par multiplication), la condition $\epsilon_S(a) = 0$, qui signifie que $a \cdot 1$ appartient à l'idéal de $A[X_s]_{s\in S}$ engendré par les éléments $1 - sX_s$, équivaut à l'existence de $s_i \in S$ $(1 \le i \le n)$ tels que $s_1 \dots s_n \cdot a = 0$. On se ramène immédiatement au cas où l'ensemble S est fini et possède m éléments, puis par récurrence sur m en tenant compte de la formule $A[x_1^{-1}, \dots, x_m^{-1}] = A[x_1^{-1}, \dots, x_{m-1}^{-1}][x_m^{-1}]$ au cas où $m = 1$ et $S = \{s\}$. Si $as^p = 0$, on a $\epsilon_S(a)\,\epsilon_S(s)^p = 0$ d'où $\epsilon_S(a) = 0$ puisque $\epsilon_S(s)$ est inversible ; inversement si $\epsilon_S(a) = 0$, il y a $P(X) \in A[X]$ tel que $a \cdot 1 = (1 - sX)P(X)$, d'où $P(X) = a(1 - sX)^{-1} = \sum_{n\ge 0} as^n X^n$ dans $A[[X]]$ et par suite $as^n = 0$ pour n assez grand puisque P est un polynôme. L'assertion (3) se déduit immédiatement de là et de la formule (1) en se rappelant que $\epsilon_S(s)$ est inversible pour $s \in S$.

Remarque. – Le lemme 2 fournit un nouveau procédé de définition des anneaux $A[S^{-1}]$; il montre aussi que lorsque A est un anneau intègre et lorsque $S = A - \{0\}$, $A[S^{-1}]$ est le corps des fractions F de A et que pour tout $S \subset A$, l'anneau $A[S^{-1}]$ peut s'identifier à un sous-anneau de F.

On rappelle aussi que lorsque $S = A - \mathfrak{p}$, $\mathfrak{p}$ étant un idéal premier, on écrit $A_\mathfrak{p}$ au lieu de $A[S^{-1}]$ et que $A_\mathfrak{p}$ s'appelle l'anneau local de l'idéal premier $\mathfrak{p}$.

1.4 Spectre des algèbres de type fini

On se donne, une fois pour toutes, un corps k et une extension algébriquement close K de k. Une algèbre de type fini est une algèbre sur k engendrée

par un nombre fini d'éléments, les homomorphismes d'algèbres sont des k-homomorphismes.

L'ensemble Ω_A des homomorphismes de l'algèbre de type fini A dans K se nomme le *spectre* de A. Pour tout homomorphisme $f : B \to A$, B étant une algèbre de type fini, on note $\widehat{f}$ l'application $h \to h \circ f$ de Ω_A dans Ω_B ; on a $\widehat{(f \circ f')} = \widehat{f'} \circ \widehat{f}$ pour $f' : C \to B$. Soit $x \in A$; si ϵ est l'homomorphisme canonique de A dans $A[x^{-1}]$, $\widehat{\epsilon}$ est une bijection du spectre de $A[x^{-1}]$ sur le sous-ensemble $V(x)$ de Ω_A formé des h tels que $h(x) \neq 0$; on identifiera ces deux ensembles par $\widehat{\epsilon}$. On a alors :

$$V(0) = \varnothing\,, \qquad V(1) = \Omega_A\,, \qquad V(xy) = V(x) \cap V(y)\,; \tag{4}$$

donc si l'on pose $V(H) = \bigcup_{x \in H} V(x)$ pour $H \subset A$, les ensembles $V(H)$ sont les ensembles ouverts d'une topologie sur Ω_A, dite *topologie de Zariski*. Pour tout homomorphisme $f : B \to A$, on a

$$\widehat{f}^{-1}(V(H)) = V(f(H)) \quad \text{pour} \quad H \subset B\,, \tag{5}$$

ce qui prouve que $\widehat{f}$ est continue pour les topologies de Zariski de Ω_A et Ω_B.

Pour $x \in A$, on notera $\widehat{x}$ la fonction $h \to h(x)$ de Ω_A dans K. On a alors pour $f : B \to A$ et $y \in B$ la formule : $\widehat{y} \circ \widehat{f} = \widehat{f(y)}$. L'application $x \to \widehat{x}$ est un homomorphisme de A sur une K-algèbre $\widehat{A}$ de fonctions de Ω_A à valeurs dans K ; le corollaire du théorème 1 montre que le noyau de cet homomorphisme est l'ensemble des éléments nilpotents de A. De plus, on notera que $V(x)$ est l'ensemble des points de Ω_A où ne s'annule par $\widehat{x}$, et par conséquent la topologie de Zariski ne dépend que de l'algèbre $\widehat{A}$; de même, si l'on identifie $V(x)$ au spectre de $B = A[x^{-1}]$, l'algèbre $\widehat{B}$ de fonctions sur $V(x)$ est engendrée par les restrictions des fonctions de $\widehat{A}$ et par l'inverse de la restriction à $V(x)$ de la fonction $\widehat{x}$ qui ne s'annule par sur $V(x)$.

Proposition 6. – *Soit U un ouvert de Ω_A ; si U est de la forme $V(x)$ pour $x \in A$, l'algèbre $\mathcal{O}(U)$ de fonctions sur U définie par l'algèbre $A[x^{-1}]$ ne dépend pas de l'élément $x \in A$ tel que $U = V(x)$. De plus, il existe sur Ω_A un système local de fonctions à valeurs dans K et un seul, soit $\mathcal{O}^A$, tel que $\mathcal{O}^A(U) = \mathcal{O}(U)$ pour U de la forme $V(x)$.*

Soient (x_i) une famille d'éléments de A et $x \in A$; pour que $V(x)$ soit contenu dans la réunion des $V(x_i)$, il faut et il suffit que tout homomorphisme h de A dans K tel que $h(x_i) = 0$ pour tout i, on ait $h(x) = 0$. Si $\mathfrak{a}$ est l'idéal de A engendré par les x_i, le corollaire du théorème 1 montre que ceci équivaut à dire que $\mathfrak{a}$ contient une puissance de x. Ceci montre en particulier que $V(x)$ est contenu dans la réunion d'un nombre fini d'ouverts $V(x_i)$. Par exemple si $V(x) \subset V(y)$, il existe $a \in A$ tel que $x^n = ay$ (n entier > 0), ce qui implique que $\widehat{y}$ est non nulle sur $V(x)$ et que son inverse est dans l'algèbre de fonctions sur $V(x)$ définie par $A[x^{-1}]$. Autrement dit, les restrictions à

$V(x)$ des fonctions appartenant à $\widehat{A[y^{-1}]}$ sont dans $\widehat{A[x^{-1}]}$ ce qui prouve à la fois la première assertion de la proposition 6 et l'axiome (SL1) des systèmes locaux. Vérifions maintenant l'axiome (SL2) : soient $V(x) = \bigcup_i V(x_i)$ et f une fonction sur $V(x)$ dont la restriction à $V(x_i)$ est définie par un élément de $A[x_i^{-1}]$ pour tout i. Il existe donc des entiers $n_i > 0$ et des éléments $a_i \in A$ tels que $f\widehat{x}_i^{n_i} = \widehat{a}_i$ sur $V(x_i)$ et donc $f\widehat{x}_i^{n_i+1} = \widehat{a}_i\,\widehat{x}_i$ sur Ω_A puisque $\widehat{x}_i$ est nulle en dehors de $V(x_i)$. Posons $b_i = a_i\,x_i$ et $m_i = n_i + 1$; comme $V(x_i) = V(x_i^{m_i})$, le début de la démonstration démontre l'existence d'un $n > 0$ et de $c_i \in A$ tel que $x^n = \sum c_i\,x_i^{m_i}$, d'où $f\widehat{x}^n = \sum f\,\widehat{c}_i\,\widehat{x}_i^{m_i} = \sum \widehat{b}_i\,\widehat{c}_i$ sur $V(x)$, ce qui signifie que f appartient à l'algèbre $\widehat{A[x^{-1}]}$: l'axiome (SL2) est donc vérifié. On achève la démonstration de la proposition 6 en appliquant le lemme 1.

On vérifie immédiatement que si f est un homomorphisme de B dans A, l'application continue $\widehat{f}$ de Ω_A dans Ω_B est un homomorphisme du système local $\mathcal{O}^A$ dans $\mathcal{O}^B$. Inversement, supposons A sans élément nilpotent, de sorte que l'application $A \to \widehat{A}$ est bijective ; si φ est un homomorphisme de $\mathcal{O}^A$ dans $\mathcal{O}^B$, on peut donc définir un homomorphisme de B dans A par la formule $\widehat{f(y)} = \widehat{y} \circ \varphi$ d'où pour $h \in \Omega_A$:

$$h(f(y)) = f(y)(h) = \widehat{y}(\varphi(h)) = \varphi(h)(y)$$

soit donc $\varphi(h) = h \circ f$ et $\varphi = \widehat{f}$; dans ce cas les applications $\widehat{f}$ sont donc tous les homomorphismes de $\mathcal{O}^A$ dans $\mathcal{O}^B$.

Etudions maintenant l'effet sur le spectre de diverses constructions sur les algèbres :

1) Soit $\mathfrak{a}$ un idéal de A et π l'homomorphisme canonique de A sur $A/\mathfrak{a}$; $\widehat{\pi}$ est alors une bijection du spectre de $A/\mathfrak{a}$ sur l'ensemble $F(\mathfrak{a})$ complémentaire de l'ouvert $V(\mathfrak{a})$; comme π est surjectif, la formule (5) montre que $\widehat{\pi}$ est même un homéomorphisme si l'on munit $F(\mathfrak{a})$ de la topologie induite par celle de Ω_A. De plus, la formule $A[x^{-1}]/\mathfrak{a}A[x^{-1}] = (A/\mathfrak{a})[\pi(x)^{-1}]$ montre immédiatement que $\widehat{\pi}$ est un isomorphisme du système local $\mathcal{O}^{A/\mathfrak{a}}$ sur le système local sur $F(\mathfrak{a})$ induit par $\mathcal{O}^A$. On identifiera le plus souvent $F(\mathfrak{a})$ au spectre de $A/\mathfrak{a}$ par $\widehat{\pi}$; on notera que *tout* fermé de Ω_A est de la forme $F(\mathfrak{a})$.

2) Soient $x \in A$ et ϵ l'homomorphisme canonique de A dans $A[x^{-1}]$. L'application $\widehat{\epsilon}$ est une bijection du spectre de $A[x^{-1}]$ sur l'ouvert $V(x)$ de Ω_A. On vérifie immédiatement que c'est un isomorphisme du système local $\mathcal{O}^{A[x^{-1}]}$ sur le système induit sur $V(x)$ par $\mathcal{O}^A$. Dans ce cas, on identifiera le spectre de $A[x^{-1}]$ à $V(x)$ par l'isomorphisme $\widehat{\epsilon}$.

3) Soient A et A' deux algèbres de type fini ; on pose $f(a) = a \otimes 1$ et $f'(a') = 1 \otimes a'$. L'application $u \to (\widehat{f}(u), \widehat{f'}(u))$ est alors une bijection du spectre de $A \otimes A'$ sur $\Omega_A \times \Omega_{A'}$, mais *ce n'est pas un homéomorphisme* si Ω_A et $\Omega_{A'}$ ont plus d'un élément. On munira toujours dans la suite $\Omega_A \times \Omega_{A'}$ de la topologie obtenue par transport à partir de la topologie de $\Omega_{A\otimes A'}$, strictement plus fine que la topologie produit.

Remarque. – Le système local $\mathcal{O}^A$ sur Ω_A ne dépend que de l'algèbre de fonctions $\widehat{A}$ sur Ω_A, et non de A ; de même, comme l'algèbre $(\widehat{A \otimes A'})$ se compose des fonctions $h(x,x') = \sum_{i=1}^{n} f_i(x)\, g_i(x')$ ($x \in \Omega_A$, $x' \in \Omega_A$, $f_i \in \widehat{A}$, $g_i \in \widehat{A'}$), la topologie de Zariski sur $\Omega_A \times \Omega_{A'}$ ne dépend que des algèbres $\widehat{A}$ et $\widehat{A'}$.

1.5 Définition des ensembles algébriques

Définition 2. – *On appelle ensemble algébrique* (ou plus précisément, (k,K)-ensemble algébrique) *un ensemble E muni d'une topologie et d'un système local $\mathcal{O}^E$ de fonctions à valeurs dans K vérifiant les conditions suivantes :*

(EA1) *Il existe un recouvrement ouvert fini $(U_i)_{i\in I}$ de E, et pour chaque $i \in I$ une k-algèbre de type fini A_i, un ouvert V_i de Ω_{A_i} et un isomorphisme φ_i du système local $\mathcal{O}^E \mid U_i$ sur le système local $\mathcal{O}^{A_i} \mid V_i$.*

(EA2) *Pour tout couple $(i,j) \in I \times I$, l'ensemble des $(\varphi_i(x), \varphi_j(x))$ pour $x \in U_i \times U_j$ est fermé dans $V_i \times V_j$ muni de la topologie induite par la topologie de $\Omega_{A_i} \times \Omega_{A_j}$.*

Une application régulière (ou morphisme) *de l'ensemble algébrique E dans l'ensemble algébrique F est un homomorphisme du système local $\mathcal{O}^E$ dans $\mathcal{O}^F$.*

Exemples. – 1) Si A est une algèbre de type fini, l'ensemble Ω_A muni de la topologie de Zariski et du système local $\mathcal{O}^A$ est un ensemble algébrique ; le premier axiome étant trivialement vérifié, le second résulte de ce que la diagonale de $\Omega_A \times \Omega_A$, étant l'ensemble $F(H)$ où H se compose des éléments $a \otimes 1 - 1 \otimes a$ de $A \otimes A$, est fermée. Un ensemble algébrique isomorphe à un ensemble du type précédent est dit ensemble algébrique *affine*. Sa structure est entièrement déterminée par l'algèbre $\mathcal{O}^E(E)$ de fonctions sur E. *Pour que l'ensemble algébrique affine E soit irréductible, il faut et il suffit que l'algèbre $A = \mathcal{O}^E(E)$ soit un anneau intègre* : en effet, comme tout ouvert non vide de E contient un ouvert de la forme $V(f) =$ ensemble des $x \in E$ où $f(x) \neq 0$ pour $f \in A$ non nul convenable, l'irréductibilité de E signifie que si f et g sont des éléments non nuls de A, l'ouvert $V(fg) = V(f) \cap V(g)$ est non vide, ce qui signifie que $fg \neq 0$. Un ensemble fermé irréductible est donc l'ensemble des points où s'annulent les éléments d'un idéal premier. Les composantes irréductibles de E correspondent aux idéaux premiers minimaux de A.

2) Supposons l'algèbre de type fini A graduée (les degrés étant ≥ 0 et les éléments de degré 0 étant les scalaires). Soit x_0 l'unique homomorphisme de A dans K nul sur les éléments de degrés > 0. Soit $h \in \Omega_A$ et $\lambda \neq 0$ dans K ; il existe un homomorphisme h_λ de A dans K bien déterminé par la condition $h_\lambda(a) = \lambda^n h(a)$ pour a homogène de degré n. On définit ainsi

le groupe multiplicatif K^* comme groupe d'opérateurs de Ω_A ; soit X le quotient de $\Omega_A - \{x_0\}$ par le groupe K^* et π l'application canonique de $\Omega_A - \{x_0\}$ sur X. On définit un ouvert de X comme un ensemble U tel que $\pi^{-1}(U)$ soit ouvert et on note $\mathcal{O}^X(U)$ l'ensemble des fonctions f de U dans K telles $f \circ \pi \in \mathcal{O}^A(\pi^{-1}(U))$. Si A est engendrée par ses éléments de degré 1, on vérifie immédiatement que l'on définit ainsi une structure d'ensemble algébrique sur X. Un ensemble algébrique isomorphe à un ensemble du type précédent est dit *projectif*.

Soit E un ensemble algébrique. On appelle *carte* définie sur un ouvert U de E un isomorphisme de $\mathcal{O}^E \mid U$ sur le système local $\mathcal{O}^A \mid V$, A étant une algèbre de type fini et V un ouvert de Ω_A. Un *ouvert affine* de E est un ouvert U tel que le système local $\mathcal{O}^E \mid U$ soit isomorphe à un système local de la forme $\mathcal{O}^A$, A étant une algèbre de type fini.

La topologie définie sur E s'appelle la *topologie de Zariski* ou la *k-topologie*.

Proposition 7. – *Tout ouvert de E est réunion d'un nombre fini d'ouverts affines et l'intersection de deux ouverts affines est un ouvert affine. L'espace topologique E est nœthérien. De plus, si φ et φ' sont deux cartes définies respectivement sur les ouverts U et U', l'ensemble des $(\varphi(x), \varphi'(x))$ pour $x \in U \cap U'$ est fermé dans $\varphi(U) \times \varphi'(U')$.*

Supposons d'abord $E = \Omega_A$, A étant une algèbre de type fini. Soit $F(H) = E - V(H)$ $(H \subset A)$ un ensemble fermé de Ω_A ; il est clair que si H engendre l'idéal $\mathfrak{a}$, on a $F(H) = F(\mathfrak{a})$, mais si $\mathfrak{a}$ est engendré par les éléments $x_1, \ldots, x_n$ (noter que A est un anneau nœthérien), on aura $F(\mathfrak{a}) = \bigcap_{i=1}^{n} F(x_i)$ et par suite l'ouvert $V(H)$ est réunion des ouverts affines $V(x_i)$ $(1 \leq i \leq n)$ et on peut supposer que $x_i \in H$. De là résulte aussitôt que Ω_A est nœthérien. Dans le cas général, l'existence d'un recouvrement ouvert fini (U_i) de E ayant les propriétés (EA1) et (EA2) prouve que E est nœthérien (prop. 1) et que tout ouvert U de E est réunion d'un nombre fini d'ouverts affines puisqu'il en est ainsi de chacun des ouverts $\varphi_i(U \cap U_i)$.

Si φ et φ' sont deux cartes définies respectivement sur U et U', l'axiome (EA2) montre que l'ensemble des $(\varphi_i(x), \varphi_j(x))$ pour $x \in U \cap U' \cap U_i \cap U_j$ est fermé dans $\varphi_i(U \cap U_i) \times \varphi_j(U' \cap U_j)$. Comme la restriction de $\varphi \circ \varphi_i^{-1}$ (resp. $\varphi \circ \varphi_j^{-1}$) à $U \cap U_i$ (resp. $U' \cap U_j$) est un homéomorphisme, l'ensemble des $(\varphi(x), \varphi'(x))$ pour $x \in U \cap U' \cap U_i \cap U_j$ est fermé dans $\varphi(U \cap U_i) \times \varphi'(U' \cap U_j)$. La dernière assertion de la prop. 7 résulte de là immédiatement.

Si enfin U et U' sont des ouverts affines, on peut supposer $\varphi(U) = \Omega_A$ et $\varphi'(U') = \Omega_{A'}$; soit Δ l'ensemble fermé de $\Omega_A \times \Omega_{A'}$ formé des $(\varphi(x), \varphi'(x))$ pour $x \in U \cap U'$. La restriction de φ à $U \cap U'$ est composée de l'application $\psi : x \to (\varphi(x), \varphi'(x))$ de $U \cap U'$ sur Δ et de la projection de $\Omega_A \times \Omega_{A'}$ sur Ω_A. Comme $\varphi \mid U \cap U'$ est un isomorphisme, il en est de même de ψ et $U \cap U'$ est isomorphe au sous-ensemble algébrique affine Δ de $\Omega_A \times \Omega_{A'}$. L'ouvert $U \cap U'$ est donc affine. C.Q.F.D.

2. Schémas des variétés algébriques[1]

2.1 Sous-ensembles algébriques

Pour simplifier le langage, on dira qu'un sous-ensemble d'un espace topologique est *localement fermé* s'il est intersection d'un ouvert et d'un fermé, ou, ce qui revient au même, s'il est ouvert dans son adhérence.

Proposition 1. – *Soient E un ensemble algébrique et T un sous-ensemble de E. Pour que T muni de la topologie induite par celle de E et du système local $\mathcal{O}^E \mid T = \mathcal{O}^T$ soit un ensemble algébrique, il faut et il suffit qu'il soit localement fermé, ou encore que pour tout $x \in T$, il existe un voisinage U de x dans E et $f_i \in \mathcal{O}^E(U)$ $(1 \leq i \leq m)$ telles que $T \cap U$ soit l'ensemble des points de U où s'annulent les fonctions f_i.*

Soit (U_i) un recouvrement ouvert de E ayant les propriétés énoncées dans les axiomes (EA1) et (EA2) du n° 1.5.

Si U est un ouvert de E, on a $\mathcal{O}^E \mid U_i \cap U = (\mathcal{O}^E \mid U) \mid (U_i \cap U)$ et $U \cap U_i$ est ouvert dans U ; comme $\varphi_i(U \cap U_i)$ est ouvert dans Ω_{A_i}, le recouvrement ouvert fini $(U \cap U_i)_{i \in I}$ de U vérifie l'axiome (EA1). La vérification de l'axiome (EA2) est immédiate, et ceci prouve que le système local $\mathcal{O}^E \mid U$ définit une structure d'ensemble algébrique sur U.

Soit maintenant F un fermé de E ; on a $\mathcal{O}^E \mid (F \cap U_i) = (\mathcal{O}^E \mid F) \mid (F \cap U_i)$ et $F \cap U_i$ est ouvert dans F ; de plus $F_i = \varphi_i(F \cap U_i)$ est fermé dans V_i, donc $F_i = V_i \cap \overline{F}_i$ ($\overline{F}_i$ désignant l'adhérence de F_i dans Ω_{A_i}) et F_i est un ouvert de $\overline{F}_i$; mais on sait que $\overline{F}_i$ peut être identifié au spectre d'une algèbre de type fini B_i et que $\mathcal{O}^{B_i} = \mathcal{O}^{A_i} \mid \overline{F}_i$; ceci prouve que la restriction de φ_i à $F \cap U_i$ est un isomorphisme de $\mathcal{O}^E \mid (F \cap U_i)$ sur $\mathcal{O}^{B_i} \mid F_i = \mathcal{O}^{A_i} \mid F_i$. Autrement dit, le recouvrement ouvert fini $(F \cap U_i)_{i \in I}$ de F vérifie l'axiome (EA1). La vérification de l'axiome (EA2) repose sur le fait que la topologie de $\Omega_{B_i} \times \Omega_{B_j}$ étant définie par les fonctions de $\widehat{(B_i \otimes B_j)}$ est induite par la topologie de $\Omega_{A_i} \times \Omega_{A_j}$.

Enfin supposons que l'on ait $T = F \cap U$, avec F fermé et U ouvert dans E. Comme $F \cap U$ est fermé dans U et que $\mathcal{O}^E \mid T = (\mathcal{O}^E \mid U) \mid (F \cap U)$, ce qui précède montre que le système local $\mathcal{O}^E \mid T$ définit une structure d'ensemble algébrique sur T.

Réciproquement, supposons que le sous-ensemble T de E soit tel que le système local $\mathcal{O}^E \mid T$ définisse une structure d'ensemble algébrique sur T.

[1] Exposé de P. Cartier, le 12.11.1956

Soit $\overline{T}$ l'adhérence de T dans E ; il suffira de prouver que T est ouvert dans $\overline{T}$, car il sera alors de la forme $U \cap \overline{T}$ avec U ouvert dans E. Mais $\overline{T}$ est un ensemble algébrique si on le munit du système local $\mathcal{O}^E \mid \overline{T}$ et l'on a $\mathcal{O}^E \mid T = (\mathcal{O}^E \mid \overline{T}) \mid T$; on est donc ramené à prouver que, si T est dense dans E, il est ouvert dans E.

Supposons donc T dense dans E et soient T_j les composantes irréductibles de T, donc $\overline{T}_j$ les composantes irréductibles de E (n° 1.1, prop. 3). Comme T_j est fermé dans T, le système local $(\mathcal{O}^E \mid T) \mid T_j = \mathcal{O}^E \mid T_j$ définit une structure d'ensemble algébrique sur T_j ; mais, $\overline{T}_j$ étant fermé dans E, le système local $\mathcal{O}^E \mid \overline{T}_j$ y définit une structure d'ensemble algébrique. Comme $\mathcal{O}^E \mid T_j = (\mathcal{O}^E \mid \overline{T}_j) \mid T_j$, on est ramené à prouver que si T est dense dans E irréductible, alors T est ouvert dans E, car alors $T_j = T \cap \overline{T}_j$ sera ouvert dans $\overline{T}_j$ et $T = \bigcup_j T_j$ sera ouvert dans $E = \bigcup_j \overline{T}_j$.

On peut donc supposer E irréductible et T dense dans E. Soit (V_k) un recouvrement fini de E par des ouverts affines ; comme $(V_k \cap T)$ est un recouvrement ouvert de T, et comme le système local $(\mathcal{O}^E \mid V_k) \mid (T \cap V_k) = \mathcal{O}^E \mid (T \cap V_k) = (\mathcal{O}^E \mid T) \mid (T \cap V_k)$ y définit une structure d'ensemble algébrique, il suffira de prouver que $T \cap V_k$ est ouvert dans V_k pour prouver que T est ouvert dans E. Autrement dit, on peut supposer E affine. Enfin comme T est réunion d'ouverts affines W_m de T, et que le système local $\mathcal{O}^E \mid W_m = (\mathcal{O}^E \mid T) \mid W_m$ définit une structure d'ensemble algébrique sur W_m, on peut supposer T affine.

Supposons donc que E et T soient des ensembles algébriques affines, que E soit irréductible et T dense dans E. Soit $f \in \mathcal{O}^T(T)$. D'après la définition du système local $\mathcal{O}^E \mid T$, pour tout $x \in T$, il existe un voisinage U_x de x dans E et une fonction $f_x \in \mathcal{O}^E(U_x)$ telle que f et f_x coïncident sur $U_x \cap T$; mais E étant irréductible, pour tous $x, y \in T$, l'ensemble $T \cap U_x \cap U_y$ est dense dans $U_x \cap U_y$, donc les fonctions continues f_x et f_y coïncident dans $U_x \cap U_y$; par suite si V est la réunion des U_x, il existe $g \in \mathcal{O}^E(V)$ induisant f_x sur U_x pour $x \in T$ et par conséquent induisant f sur T. Si (f_i) est un système fini de générateurs de l'algèbre $\mathcal{O}^T(T)$, on peut par suite trouver un ouvert V contenant T et des fonctions $g_i \in \mathcal{O}^E(V)$ prolongeant les f_i. Soit A la sous-algèbre de $\mathcal{O}^E(V)$ engendrée par les g_i ; comme T est dense dans V et comme les éléments de A sont des fonctions continues, l'opération $f \to f \mid T$ est une bijection[2] de A sur $\mathcal{O}^T(T)$. Soit alors $x \in V$; l'application $f \to f(x)$ de A dans K étant un homomorphisme, il existe puisque T est affine $x' \in T$ tel que $f(x) = f(x')$ pour tout $f \in A$ et en particulier pour $f \in \mathcal{O}^E(E)$; comme E est affine, on en déduit $x = x'$ donc $x \in T$ et $T = V$. On a donc prouvé que T est ouvert dans E.

[2] Cette application de restriction est surjective par construction. Montrons que son noyau est réduit à 0 : si $f \in A$ est telle que $f \mid T = 0$, l'ensemble $f^{-1}(0)$ est fermé dans V car f est continue et $\{0\}$ fermé dans K, il contient T et T est dense dans V; on a donc $f^{-1}(0) = V$, c'est-à-dire $f = 0$. C.Q.F.D.

Pour achever la démonstration, il reste à démontrer que, pour que T soit localement fermé, il faut et il suffit qu'il vérifie la dernière condition de la proposition 1. Supposons d'abord $T = F \cap U$ avec U ouvert et F fermé dans E ; pour tout $x \in T$, il existe un ouvert affine U_x contenant x et contenu dans U d'après la proposition 7 de l'exposé 1. L'ensemble $T \cap U_x = F \cap U_x$ étant fermé dans U_x est de la forme $\complement \bigcup_i V(f_i)$ avec $f_i \in \mathcal{O}^E(U_x)$, et c'est donc l'ensemble des points de U_x où s'annulent les f_i.

Inversement, supposons que tout $x \in T$ ait un voisinage ouvert U_x tel que $T \cap U_x$ soit l'ensemble des points où s'annulent des fonctions $f_i \in \mathcal{O}^E(U_x)$; il s'ensuit que $T \cap U_x$ est fermé dans U_x, et comme T est recouvert par un nombre fini d'ouverts U_{x_j}, il est fermé dans l'ouvert $\bigcup_i U_{x_j}$. C.Q.F.D.

Si T est un sous-ensemble localement fermé de l'ensemble algébrique E, on appellera *sous-ensemble algébrique* T de E, l'ensemble T muni de la topologie induite par celle de E et du système local $\mathcal{O}^E \mid T$.

Remarque. – Chevalley a démontré que si T est un sous-ensemble d'un ensemble algébrique E sur lequel existe une structure induite au sens de N. Bourbaki (Ens. IV, §2), T est localement fermé, ce qui justifie la terminologie introduite. La démonstration précédente montre qu'on peut se limiter au cas où E et T sont affines, où E est irréductible et T dense dans E.

2.2 Produit d'ensembles algébriques

Remarquons pour commencer que, si U est un ouvert d'un ensemble algébrique E, l'ensemble $\mathcal{O}^E(U)$ est une k-algèbre de fonctions sur U et que si $f \in \mathcal{O}^E(U)$ ne s'annule par sur U, son inverse appartient à $\mathcal{O}^E(U)$: ces assertions résultent en effet du cas où U est un ouvert affine d'après l'axiome (SL2) et la proposition 7 du n° 1.5, tandis que dans le cas affine elles résultent de la proposition 6 du n° 1.4.

De plus, l'algèbre des fonctions polynômes sur K à coefficients dans k définit sur l'ensemble K une structure d'ensemble algébrique affine pour laquelle les ensembles fermés $\neq K$ sont les ensembles finis invariants par le groupe des k-automorphismes de K. On peut donc identifier K au spectre $\Omega_{k[X]}$ de l'algèbre de polynômes $k[X]$ en une variable.

Proposition 2. – *Soient E un ensemble algébrique et A une algèbre de type fini sur k ; pour qu'une application f de E dans Ω_A soit régulière, il faut et il suffit que, pour tout $x \in A$, on ait $\widehat{x} \circ f \in \mathcal{O}^E(E)$.*

La condition est évidemment nécessaire. Inversement, supposons-la vérifiée par f et soit $x \in A$; l'ensemble $U = f^{-1}(V(x))$ est l'ensemble des points où ne s'annule pas $\widehat{x} \circ f$, donc est ouvert, ce qui prouve que f est continue. De plus la fonction $\widehat{x} \circ f$ ne s'annulant pas sur U, son inverse est dans $\mathcal{O}^E(U)$ et

évidemment égal à $\widehat{x}^{-1} \circ f$. Comme $\mathcal{O}^A(V(x))$ est engendrée par les restrictions à $V(x)$ des fonctions appartenant à $\widehat{A}$ et par $\widehat{x}^{-1}$, on a $h \circ f \in \mathcal{O}^E(U)$ pour $h \in \mathcal{O}^A(V(x))$; ceci prouve que f est régulière, puisque les $V(x)$ forment une base d'ouverts de Ω_A.

Corollaire 1. – *Les applications régulières de E dans K muni de la structure définie plus haut sont les éléments de $\mathcal{O}^E(E)$.*

Corollaire 2. – *Pour qu'une application $x \to (f_1(x), f_2(x))$ de l'ensemble algébrique E dans $\Omega_{A_1} \times \Omega_{A_2}$ soit régulière, il faut et il suffit que f_1 et f_2 soient régulières.*

Ceci résulte immédiatement de la remarque du n° 1.4.

En vertu du corollaire 1, les éléments de $\mathcal{O}^E(U)$ pour U ouvert dans E peuvent s'appeler *fonctions* (numériques) *régulières* sur U.

Proposition 3. – *Soient E_1 et E_2 deux ensembles algébriques. Il existe sur $E_1 \times E_2$ une structure d'ensemble algébrique et une seule vérifiant la condition suivante :*

(P) *Si pour $i = 1, 2$, φ_i est une carte de l'ouvert U_i de E_i sur l'ouvert V_i de Ω_{A_i} (A_i étant une algèbre de type fini), l'ensemble $U_1 \times U_2$ est ouvert dans $E_1 \times E_2$ et l'application $\varphi_1 \times \varphi_2$ est une carte de $U_1 \times U_2$ sur l'ouvert $V_1 \times V_2$ de $\Omega_{A_1} \times \Omega_{A_2}$.*

Dans ces conditions, pour qu'une application $x \to (f_1(x), f_2(x))$ de l'ensemble algébrique F dans $E_1 \times E_2$ soit régulière, il faut et il suffit que les applications f_1 et f_2 soient régulières.

Soient pour $i = 1, 2$, des cartes $\varphi_i : U_i \to V_i \subset \Omega_{A_i}$ et $\varphi'_i : U'_i \to V'_i \subset \Omega_{A'_i}$ définies sur des ouverts de E_i ; l'ensemble $T_i = \varphi_i(U_i \cap U'_i)$ est ouvert dans V_i, donc dans Ω_{A_i} et, comme la topologie de $\Omega_{A_1} \times \Omega_{A_2}$ est plus fine que la topologie produit, l'ensemble

$$(\varphi_1 \times \varphi_2)((U_1 \times U_2) \cap (U'_1 \times U'_2)) = \varphi_1(U_1 \cap U'_1) \times \varphi_2(U_2 \cap U'_2) = T_1 \times T_2$$

est ouvert dans $\Omega_{A_1} \times \Omega_{A_2}$. De plus l'application $\varphi_i \circ \varphi_i'^{-1}$ est une application régulière de $T'_i = \varphi'_i(U_i \cap U'_i)$ sur T_i. Comme T'_i est ouvert dans V'_i donc dans $\Omega_{A'_i}$, il résulte du corollaire 2 de la proposition 2, que

$$\psi = (\varphi_1 \times \varphi_2) \circ (\varphi'_1 \times \varphi'_2)^{-1} = (\varphi_1 \circ \varphi_1'^{-1}) \times (\varphi_2 \circ \varphi_2'^{-1})$$

est une application régulière de $T'_1 \times T'_2$ sur $T_1 \times T_2$. Inversant les rôles de φ_i et φ'_i, on voit que ψ^{-1} est régulière, donc que ψ est un isomorphisme.

Comme E_i est recouvert par un nombre fini d'ouverts admettant des cartes, ce qui précède permet d'appliquer la proposition 5 du n° 1.2 pour démontrer l'existence et l'unicité d'un système local sur $E_1 \times E_2$ vérifiant la condition (P), et ceci montre aussi que $E_1 \times E_2$ est recouvert par un nombre fini d'ouverts admettant des cartes. De plus, pour qu'une application

$x \to (f_1(x), f_2(x))$ de F dans $E_1 \times E_2$ soit régulière, il faut et il suffit d'après la proposition 5 du n° 1.2 que pour chaque carte φ_i définie sur l'ouvert U_i de E_i $(i = 1, 2)$, l'application $x \to (\varphi_1(f_1(x)), \varphi_2(f_2(x)))$ de $f_1^{-1}(U_1) \times f_2^{-1}(U_2)$ dans $\Omega_{A_1} \times \Omega_{A_2}$ soit régulière, donc, d'après le corollaire 2 de la proposition 2, que l'application $\varphi_i \circ f_i$ de $\varphi_i^{-1}(U_i)$ dans Ω_{A_i} soit régulière. Cette dernière condition signifie d'après la proposition 4 du n° 1.2 que f_i est régulière.

Il reste à démontrer que $E_1 \times E_2$ vérifie l'axiome (EA2) si E_1 et E_2 vérifient ce même axiome. Les notations étant les mêmes qu'au début de la démonstration, il faut montrer que l'ensemble Δ formé des

$$((\varphi_1(x_1), \varphi_2(x_2)), (\varphi_1'(x_1), \varphi_2'(x_2)))$$

pour $(x_1, x_2) \in (U_1 \times U_2) \cap (U_1' \times U_2')$ est fermé dans

$$(V_1 \times V_2) \times (V_1' \times V_2') \subset (\Omega_{A_1} \times \Omega_{A_2}) \times (\Omega_{A_1'} \times \Omega_{A_2'}) = G\,.$$

Or l'échange S des deux facteurs Ω_{A_2} et $\Omega_{A_1'}$ dans le produit G est un homéomorphisme et l'on a $S(\Delta) = \Delta_1 \times \Delta_2$ si Δ_i est l'ensemble des $(\varphi_i(x_i), \varphi_i'(x_i))$ pour $x_i \in U_i \cap U_i'$. Comme Δ_i est fermé dans $V_i \times V_i'$ puisque E_i vérifie l'axiome (EA2), l'ensemble Δ est fermé dans $(V_1 \times V_2) \times (V_1' \times V_2')$ et par suite $E_1 \times E_2$ vérifie l'axiome (EA2).

Remarques. – 1) Lorsque E_i $(i = 1, 2)$ est un ensemble muni d'une topologie et d'un système local vérifiant l'axiome (EA1), la démonstration qui précède montre qu'il existe sur $E_1 \times E_2$ un système local et un seul vérifiant la condition (P) et ce système local vérifie la condition (EA1). Dans ces conditions, l'axiome (EA2) signifie *que la diagonale Δ_E de $E \times E$ est fermée.*

2) Soient E_i $(i = 1, 2)$ deux ensembles algébriques affines et A_i l'algèbre des fonctions régulières sur E_i ; il résulte du fait que E_i est isomorphe à Ω_{A_i} et de la définition de la structure de $\Omega_{A_1} \times \Omega_{A_2}$, que les fonctions régulières sur $E_1 \times E_2$ sont les fonctions de la forme

$$h(x_1, x_2) = \sum_{k=1}^{m} f_{1,k}(x_1)\, f_{2,k}(x_2) \qquad \text{pour} \quad f_{i,k} \in A_i\,.$$

En particulier, les fonctions régulières sur K^n sont les fonctions polynômes à n variables à coefficients dans k. Comme toute algèbre de type fini sur k est isomorphe à une algèbre de la forme $k[X_1, \ldots, X_n]/(P_1, \ldots, P_m)$, on en conclut que tout ensemble algébrique affine est isomorphe à un sous-ensemble de K^n défini par des équations $P_i(x_1, \ldots, x_n) = 0$ $(1 \leq i \leq m)$ pour un n convenable et des polynômes $P_i \in k[X_1, \ldots, X_n]$ convenables.

Le critère sur les applications régulières contenu dans la proposition 3 montre que la structure définie sur $E_1 \times E_2$ est une structure produit au sens de N. Bourbaki (Ens. IV, § 2) ; il en résulte que le produit d'ensembles algébriques est une opération associative et commutative, que si f_i est une application régulière de E_i dans F_i pour $i = 1, 2$, l'application $f_1 \times f_2$ de

$E_1 \times E_2$ dans $F_1 \times F_2$ est régulière, que la projection p_i de $E_1 \times E_2$ sur E_i est régulière, et que si f est une application régulière de E dans F dont le graphe est Γ, la projection p de $E \times F$ sur E induit un isomorphisme de Γ sur E (on notera d'ailleurs que *le graphe Γ de f est fermé* comme image réciproque de la diagonale de $F \times F$ par l'application continue $(x, y) \to (f(x), y)$ de $E \times F$ dans $F \times F$). Enfin, comme la topologie sur $E_1 \times E_2$ est plus fine que la topologie produit (puisque les projections sur les facteurs sont continues), le produit de deux sous-ensembles T_1 et T_2 localement fermés de E_1 et E_2 respectivement, est localement fermé dans $E_1 \times E_2$ et il résulte de N. Bourbaki (*loc. cit.*) que la structure induite sur $T_1 \times T_2$ par la structure produit de $E_1 \times E_2$ est identique à la structure produit des structures induites sur T_1 et T_2.

2.3 Extension des scalaires

Nous allons d'abord démontrer un résultat préliminaire affirmant la possibilité de construire des ensembles algébriques par "recollement des morceaux".

Proposition 4. – *Soit $(E_i)_{i \in I}$ un recouvrement d'un ensemble E dont on puisse extraire un recouvrement fini. On suppose donnés pour tout $i \in I$ un ensemble algébrique X_i et une bijection f_i de X_i sur E_i de sorte que pour tout couple (i, j) :*

a) $f_i^{-1}(E_i \cap E_j) = X_{ij}$ soit ouvert dans X_i ;

b) l'application $f_j^{-1} \circ (f_i \mid X_{ij}) = f_{ij}$ soit une application régulière de X_{ij} sur X_{ji} ;

c) l'ensemble R_{ij} de $X_i \times X_j$ formé des couples (x, x') tels $f_i(x) = f_j(x')$ soit fermé dans $X_i \times X_j$.

Il existe alors sur E une structure d'ensemble algébrique et une seule pour laquelle les E_i soient ouverts et f_i soit un isomorphisme de X_i sur E_i. Dans ces conditions, si E' est un ensemble algébrique, pour qu'une application f de E dans E' (resp. de E' dans E) *soit régulière, il faut et il suffit que pour tout $i \in I$, l'application $f \circ f_i$ de X_i dans E'* (resp. $f^{-1}(E_i)$ soit ouvert dans E' et que l'application $f_i^{-1} \circ (f \mid f^{-1}(E_i))$ de $f^{-1}(E_i)$ dans X_i) *soit régulière.*

Cela résulte immédiatement de la proposition 5 du n° 1.2, la condition c) assurant que la diagonale de $E \times E$ est fermée et l'axiome (EA1) résultant de ce qu'un nombre fini des E_i recouvre E.

Les ensembles algébriques envisagés jusqu'ici étaient des (k, K)-ensembles algébriques. Soit k' un sous-corps de K contenant k ; nous allons montrer comment tout (k, K)-ensemble algébrique peut être muni d'une structure de (k', K)-ensemble algébrique.

Soit A une k-algèbre de type fini et $A' = k' \otimes_k A$ l'algèbre déduite de A par extension des scalaires. A tout k-homomorphisme f de A dans K associons le k'-homomorphisme $i_A(f) : \lambda \otimes x \to \lambda f(x)$ de A' dans K. L'application i_A est une bijection de Ω_A sur $\Omega_{A'}$ et elle transforme un ouvert (resp.

un fermé) de Ω_A en un ouvert (resp. un fermé) de $\Omega_{A'}$. Autrement dit, i_A^{-1} est continue.

Proposition 5. – *Soient E un (k,K)-ensemble algébrique et k' un sous-corps de K contenant k. Il existe sur E une structure de (k',K)-ensemble algébrique $E^{k'}$ et une seule telle que tout ouvert U de E soit un ouvert de $E^{k'}$ et que pour toute carte $\varphi : U \to V \subset \Omega_A$ de E l'application*

$$i_A \circ \varphi : U \to \varphi(V) \to \Omega_{A'} ,$$

soit une carte de $E^{k'}$. Pour qu'une application f d'un (k',K)-ensemble algébrique F dans $E^{k'}$ soit régulière, il faut et il suffit que f soit un homomorphisme du système local $\mathcal{O}^F$ dans le système local $\mathcal{O}^E$.

On va appliquer la proposition 4 à la classe (qui n'est pas un ensemble) de toutes les applications $(i_A \circ \varphi)^{-1}$ pour toutes les cartes φ de E. Les conditions a) et c) sont remplies du fait que i_A transforme ouvert en ouvert et fermé en fermé et que c'est une bijection. La condition b) sera remplie en vertu du lemme suivant :

Lemme 1. – *Soient A et B deux k-algèbres de type fini, f une application régulière d'un ouvert U de Ω_A dans Ω_B. Il existe une application régulière f' et une seule de $U' = i_A(U) \subset \Omega_{A'}$ dans $\Omega_{B'}$ (avec $A' = k' \otimes_k A$ et $B' = k' \otimes_k B$) telle que $i_B \circ f = f' \circ i_A$.*

Comme i_A et i_B sont des bijections, l'application ensembliste f' existe bien. Comme tout ouvert de Ω_A est réunion d'ouverts de la forme $V(x)$ avec $x \in A$, la proposition 7 du n° 1.5 montre qu'on peut se limiter au cas où $U = V(x)$. De plus la définition de i_A montre que si $x \in A$, on a $x = (\widehat{1 \otimes x}) \circ i_A$ et par suite $i_A(V(x)) = V(1 \otimes x)$. Nous allons appliquer la proposition 2 ; il suffira de montrer que, pour $y \in B$, $(1 \otimes y) \circ f'$ est régulière sur U', mais on a $((\widehat{1 \otimes y}) \circ f') \circ i_A = (\widehat{1 \otimes y}) \circ i_B \circ f = \widehat{y} \circ f$. Comme f est régulière et $U = V(x)$, la fonction $\widehat{y} \circ f$ est de la forme $\widehat{x}'/\widehat{x}^m$ et par suite $(\widehat{i \otimes y}) \circ f$ est de la forme $(\widehat{1 \otimes x'})/(\widehat{1 \otimes x})^m$, donc est régulière sur U'.

L'existence et l'unicité de la structure de $E^{k'}$ sont donc démontrées. Soit f une application du (k',K)-ensemble algébrique F dans E. Pour que f soit régulière de F dans $E^{k'}$, il faut et il suffit d'après la proposition 4 que pour toute carte $\varphi : U \to \Omega_A$ de E, l'application $i_A \circ \varphi \circ f$ de $f^{-1}(U)$ dans $\Omega_{A'}$ soit régulière. Comme les fonctions régulières sur $\Omega_{A'}$ sont les combinaisons linéaires à coefficients dans k' des fonctions $h \circ i_A^{-1}$ avec $h \in \widehat{A}$, ceci signifie d'après la proposition 2 que pour tout $h' \in \mathcal{O}^E(U)$, la fonction $h' \circ f$ est régulière sur $f^{-1}(U)$, *i.e.* que f est un homomorphisme de $\mathcal{O}^F$ dans $\mathcal{O}^E$. C.Q.F.D.

On notera que si U est un ouvert affine de E, les fonctions régulières sur l'ouvert U de $E^{k'}$ sont les combinaisons linéaires à coefficients dans k' des éléments de $\mathcal{O}^E(U)$.

La topologie sur E définie par la structure de $E^{k'}$ s'appellera la k'-*topologie de* E. On parlera ainsi de k'-fermé, etc. De même, on dira par abus de langage qu'une application f de E dans un (k, K)-ensemble algébrique E' est une application régulière de E dans E' définie sur k' si c'est une application régulière de $E^{k'}$ dans $E'^{k'}$.

On dira de plus qu'un ensemble algébrique est *absolument irréductible* s'il est irréductible pour la K-topologie. Il résultera en fait des résultats démontrés plus loin (corollaire 3 du théorème 1) que l'absolue irréductibilité signifie l'irréductibilité pour la k'-topologie, pourvu que k' soit algébriquement clos.

2.4 Applications rationnelles

Soient E et F deux ensembles algébriques ; si f_i $(i = 1, 2)$ est une application régulière de l'ouvert U_i de E dans F, nous dirons comme d'habitude que "f_2 prolonge f_1" si $U_1 \subset U_2$ et si $f_2 \mid U_1 = f_1$. On définit ainsi une relation d'ordre entre fonctions régulières définies dans un ouvert (variable) de E.

Lemme 2. – *Toute fonction f régulière définie dans un ouvert U de E à valeurs dans F admet un prolongement maximal. Si U est partout dense ce prolongement est unique. Pour que deux fonctions f et f' régulières définies sur des ouverts partout denses admettent le même prolongement maximal, il faut et il suffit qu'elles coïncident sur un ouvert partout dense où elles sont toutes deux définies.*

La première assertion résulte du théorème de Zorn, applicable ici car l'axiome (SL2) des systèmes locaux montre que l'ensemble des applications régulières d'un ouvert de E dans F, ordonné par la relation "f_2 prolonge f_1" est inductif.

Supposons donc f régulière définie sur l'ouvert U partout dense et soient f_1 et f_2 deux prolongements maximaux de f définis respectivement sur les ouverts U_1 et U_2 ; l'ensemble D des points x de $U_1 \cap U_2$ tels que $f_1(x) = f_2(x)$ est fermé[3] dans $U_1 \cap U_2$ et contient U qui est dense dans $U_1 \cap U_2$, d'où $D = U_1 \cap U_2$; les fonctions f_1 et f_2 coïncident dans $U_1 \cap U_2$. L'axiome (SL2) démontre l'existence d'une fonction régulière sur $U_1 \cup U_2$ prolongeant f_1 et f_2 ; comme les f_i sont maximaux, ceci impose $U_1 \cup U_2 = U_1 = U_2$ et par suite $f_1 = f_2$.

Si f et f' admettent le même prolongement maximal, elles coïncident sur l'intersection de leurs domaines de définition qui est un ouvert partout dense. Inversement, si f et f' sont les prolongements d'une même fonction g régulière sur un ouvert partout dense de E, et si $\overline{f}$ et $\overline{f}'$ sont des prolongements maximaux de f et f' respectivement, ce sont tous deux des prolongements maximaux de g, et ils sont donc égaux.

[3] La preuve (facile) s'appuie sur le fait que la diagonale est fermée dans $F \times F$.

Ceci dit, on peut poser la définition suivante :

Définition 1. – *Soient E et F deux ensembles algébriques. On appelle application rationnelle f de E dans F une application régulière d'un ouvert partout dense de E à valeurs dans F qui n'admet aucun prolongement strict. Le domaine de définition de f sera noté $D(f)$. Une application rationnelle de E dans K sera appelée une fonction rationnelle* (numérique) *sur E.*

Démontrons d'abord un lemme sur la topologie des ensembles algébriques :

Lemme 3. – *Soient E un ensemble algébrique et E_i ses composantes irréductibles. Pour qu'un ouvert U de E soit partout dense, il faut et il suffit qu'il rencontre chaque E_i. Dans ces conditions, U est réunion d'un nombre fini d'ouverts affines partout denses U_j et si E est affine, on peut supposer U_j de la forme $V(f_j)$ avec $f_j \in \mathcal{O}^E(E)$.*

Supposons qu'on ait $U \cap E_i \neq \varnothing$ pour tout i et soit V un ouvert non vide de E. Il y a un indice i_0 tel que $V \cap E_{i_o} \neq \varnothing$, d'où comme E_{i_0} est irréductible $U \cap V \cap E_{i_0} \neq \varnothing$ et *a fortiori* $U \cap V \neq \varnothing$; U est donc partout dense. Supposons inversement U partout dense et soit $F_i = \bigcap_{j \neq i} \complement E_j \subset E_i$; comme F_i est un ouvert non vide, on a $F_i \cap U \neq \varnothing$ et donc $E_i \cap U \neq \varnothing$.

Supposons U partout dense dans E. Soient $x \in E$ et $V \subset U$ un ouvert affine contenant x ; pour chaque i, soit G_i un ouvert affine non vide contenu dans $F_i \cap U$ et soit W la réunion de V et des G_i qui ne rencontrent pas V ; alors W est réunion d'ouverts affines disjoints, donc est lui-même affine, comme on le voit avec l'axiome (SL2), et il est partout dense car il rencontre visiblement chaque E_i. En vertu de la quasi-compacité de U, l'ouvert U est donc réunion d'un nombre fini d'ouverts affines partout denses.

Lorsque E est affine, on peut supposer V et les G_i de la forme $V(f)$. Or on voit facilement que toute réunion d'ouverts disjoints de la forme $V(f)$ est aussi de cette forme. C.Q.F.D.

Soient f et g deux fonctions rationnelles sur l'ensemble algébrique E ; d'après le lemme 2, il existe des fonctions rationnelles $f+g$ et fg bien définies par les conditions :

$$(f+g)(x) = f(x) + g(x)\,, \qquad (fg)(x) = f(x)g(x)$$

pour tout $x \in D(f) \cap D(g)$. Le lemme 3 montre alors que les fonctions rationnelles sur E forment une k-algèbre notée $k(E)$.

Soient f et g deux applications rationnelles de E dans F et F dans G respectivement ; si l'ouvert $f^{-1}(D(g))$ est partout dense dans E, il existe une application rationnelle bien définie $g \odot f$ par la condition $(g \odot f)(x) = g(f(x))$ chaque fois que $f(x)$ et $g(f(x))$ sont définis. Lorsque h est une application rationnelle de G dans H, si $h \odot (g \odot f)$ et $(h \odot g) \odot f$ sont tous deux définis, ils sont égaux et on peut les noter $h \odot g \odot f$. En particulier si F est un sous-ensemble localement fermé de E, pour que la restriction $f \mid F$ de $f \in k(E)$ à

F soit définie, il faut et il suffit que $D(f) \cap F$ soit dense dans F ; ces fonctions forment une sous-algèbre $\mathcal{O}(E, F)$ de $k(E)$ et l'opération $f \to f \mid F$ est un homomorphisme $\rho_{E,F}$ de $\mathcal{O}(E, F)$ dans $k(F)$. Si G est un sous-ensemble localement fermé de F, c'est un sous-ensemble localement fermé de E, et l'on a $\mathcal{O}(E, G) \subset \mathcal{O}(E, F)$, l'homomorphisme $\rho_{E,F}$ applique $\mathcal{O}(E, G)$ dans $\mathcal{O}(F, G)$ et la restriction à $\mathcal{O}(E, G)$ de $\rho_{F,G} \circ \rho_{E,F}$ est égale à $\rho_{E,G}$. Enfin, si U est un ouvert partout dense de E, on a évidemment $\mathcal{O}(E, U) = k(E)$ et l'homomorphisme $\rho_{E,U}$ est un isomorphisme de $k(E)$ sur $k(U)$. Le lemme 3 montre que, dans les questions concernant les fonctions rationnelles, on peut se limiter le plus souvent au cas des ensembles algébriques affines.

Théorème 1. – *Soient E un ensemble algébrique et E_i ses composantes irréductibles.*

a) *L'homomorphisme canonique de $k(E)$ dans $\prod_i k(E_i)$ défini par les restrictions ρ_{E,E_i} est un isomorphisme ; l'algèbre $k(E_i)$ est un corps, extension de type fini de k. En particulier, $k(E)$ est une algèbre semi-simple.*

b) *Supposons E affine et soit F un fermé de E ; on note A l'algèbre des fonctions régulières sur E, $\mathfrak{a}$ l'idéal de A formé des fonctions nulles sur F, $\mathfrak{p}_i$ les idéaux premiers minimaux de (0) et $\mathfrak{q}_j$ les idéaux premiers minimaux de $\mathfrak{a}$, $S = (\bigcap_i \complement\mathfrak{p}_i) \cap (\bigcap_j \complement\mathfrak{q}_j)$. L'injection de A dans $k(E)$ se prolonge en un isomorphisme de $A[S^{-1}]$ sur $\mathcal{O}(E, F)$.*

Démontrons b) et déterminons d'abord la structure de $k(E)$. Posons $T = \bigcap_i \complement\mathfrak{p}_i = \complement(\bigcup_i \mathfrak{p}_i)$. Il est classique que T se compose des non diviseurs de 0 dans A. On peut énumérer les composantes irréductibles de E de sorte que E_i soit l'ensemble fermé associé à l'idéal $\mathfrak{p}_i$. Un élément f de A appartient à T si et seulement s'il n'appartient à aucun des idéaux $\mathfrak{p}_i$, c'est-à-dire s'il n'induit la fonction nulle sur aucun des E_i ; d'après le lemme 3, ceci signifie que l'ouvert $V(f)$ formé des $x \in E$ avec $f(x) \neq 0$ est partout dense dans E. Si $f \in T$, la fonction f^{-1} est définie sur l'ouvert partout dense $V(f)$ et se prolonge en une fonction rationnelle, inverse de f dans $k(E)$; l'injection de A dans $k(E)$ se prolonge donc en une injection de $A[T^{-1}]$ dans $k(E)$. De plus si $f \in k(E)$, l'ouvert partout dense $D(f)$ contient un ouvert de la forme $V(g)$ avec $g \in T$ d'après le lemme 3, et par suite on a $f = h/g^m$ ($h \in A$, m entier ≥ 0) sur $V(g)$; ceci prouve que f appartient à l'image de $A[T^{-1}]$. On a donc identifié $k(E)$ à l'anneau de fractions $A[T^{-1}]$; en particulier, *si E est irréductible, l'anneau A est intègre et $k(E)$ est son corps des fractions.*

Soit $f \in k(E)$; pour que l'on ait $V(g) \subset D(f)$ pour $g \in A$, il faut et il suffit qu'il existe un entier m tel que $fg^m \in A$; comme $V(g) = V(g^m)$, le complémentaire de $D(f)$ est l'ensemble des points où s'annulent tous les $g \in A$ tels que $fg \in A$. Ces g forment un idéal $\mathfrak{b}$ de A. Pour que $D(f) \cap F$ soit dense dans F, il faut et il suffit que $D(f)$ rencontre chacune des composantes irréductibles F_j de F, ou encore que $\complement D(f)$ ne contienne aucune des F_j, ce

qui signifie que $\mathfrak{b}$ n'est contenu dans aucun des $\mathfrak{q}_j$. Comme $\mathfrak{b}$ rencontre T (lemme 3), il n'est contenu dans aucun des $\mathfrak{p}_i$. Or on a le lemme :

Lemme 4. – *Soient A un anneau commutatif, $\mathfrak{c}$ un idéal de A et $\mathfrak{r}_i$ des idéaux premiers de A en nombre fini. Pour que $\mathfrak{c}$ ne soit contenu dans aucun des $\mathfrak{r}_i$, il faut et il suffit qu'il existe $a \in \mathfrak{c}$ qui n'appartienne à aucun des $\mathfrak{r}_i$.*

La condition est manifestement suffisante. Inversement supposons que $\mathfrak{c}$ ne soit contenu dans aucun des $\mathfrak{r}_i$ et supposons, ce qui est licite, que $\mathfrak{r}_i \not\subset \mathfrak{r}_j$ si $i \neq j$. Soit $a_i \in \mathfrak{c}$, $a_i \notin \mathfrak{r}_i$ et $s_{ij} \notin \mathfrak{r}_i$ mais $s_{ij} \in \mathfrak{r}_j$ $(i \neq j)$; l'élément $s_i = \prod_{j \neq i} s_{ij}$ n'est pas dans $\mathfrak{r}_i$ mais appartient à $\mathfrak{r}_j$ pour $j \neq i$. Formons alors $a = \sum_i s_i\, a_i \in \mathfrak{c}$; pour i fixé, on a $a_i s_i \notin \mathfrak{r}_i$, mais $a_j s_j \in \mathfrak{r}_i$ pour $j \neq i$ et donc $a \notin \mathfrak{r}_i$.

Le lemme 4 montre donc que, pour que f induise une fonction rationnelle sur F, il faut et il suffit que $\mathfrak{b}$ rencontre S, ce qui démontre l'assertion b).

Démontrons l'assertion a) ; soit U_i un ouvert affine non vide ne rencontrant aucune des composantes E_j pour $j \neq i$ et soit U la réunion des U_i. Comme les U_i sont disjoints, il résulte de l'axiome (SL2) que les fonctions régulières définies sur un ouvert V de U sont les fonctions régulières sur $V \cap U_i$ pour chaque i ; il en résulte que l'application $k(U) \to \prod_i k(U_i)$ est bijective. Comme U est partout dense dans E et U_i partout dense dans E_i, les flèches horizontales du diagramme commutatif suivant représentent des isomorphismes, d'où découle le fait que $k(E) \to \prod_i k(E_i)$ est un isomorphisme :

$$\begin{array}{ccc} k(E) & \longrightarrow & k(U) \\ \downarrow & & \downarrow \\ \prod_i k(E_i) & \longrightarrow & \prod_i k(U_i) \end{array}$$

Enfin $k(U_i)$ est le corps des fractions de $\mathcal{O}^E(U_i)$ donc est une extension de type fini de k, et il en est de même de $k(E_i)$ qui lui est isomorphe. C.Q.F.D.

Corollaire 1. – *Si E est un ensemble algébrique affine, l'algèbre $k(E)$ des fonctions rationnelles sur E est isomorphe à l'anneau total des fractions de $\mathcal{O}^E(E)$.*

On rappelle que l'anneau *total* des fractions d'un anneau commutatif A est l'anneau $A[S^{-1}]$ où S est l'ensemble des non diviseurs de 0 dans A.

Corollaire 2. – *Soient E_1 et E_2 deux ensembles algébriques, k' un sous-corps de K contenant k. Soient*[4] *respectivement $\mathfrak{a}$ et $\mathfrak{b}$ les idéaux des éléments*

[4] On note $\otimes$ le produit tensoriel sur le corps k.

nilpotents de $k(E_1)\otimes k(E_2)$ et $k(E_1)\otimes k'$. L'algèbre des fonctions rationnelles sur $E_1 \times E_2$ (resp. $E_1^{k'}$) *est canoniquement isomorphe à l'anneau total des fractions de $(k(E_1) \otimes k(E_2))/\mathfrak{a}$* (resp. $(k(E_1) \otimes k')/\mathfrak{b}$).

On se ramène immédiatement au cas où E_1 et E_2 sont affines (*cf.* lemme 3). Si $A_i = \mathcal{O}^{E_i}(E_i)$, l'algèbre des fonctions régulières sur $E_1 \times E_2$ (resp. $E_1^{k'}$) est isomorphe à $(A_1 \otimes A_2)/\mathfrak{a}_0$ (resp. $(A_1 \otimes k')/\mathfrak{b}_0$), $\mathfrak{a}_0$ (resp. $\mathfrak{b}_0$) étant l'idéal des éléments nilpotents de $A_1 \otimes A_2$ (resp. $A_1 \otimes k'$). Il est clair que si l'on plonge $A_1 \otimes A_2$ (resp. $A_1 \otimes k'$) dans $k(E_1) \otimes k(E_2)$ (resp. $k(E_1) \otimes k'$), l'idéal $\mathfrak{a}$ (resp. $\mathfrak{b}$) est engendré par $\mathfrak{a}_0$ (resp. $\mathfrak{b}_0$). Le corollaire 2 résulte alors immédiatement du corollaire 1.

Corollaire 3. – *Soit E un ensemble algébrique. Pour que E soit irréductible* (resp. absolument irréductible)*, il faut et il suffit que $k(E)$ soit un corps* (resp. un corps extension primaire de k)*. Pour que l'algèbre semi-simple $k(E)$ soit absolument semi-simple, il faut et il suffit que, pour tout ouvert U de E, toute famille $f_i \in \mathcal{O}^E(U)$ $(1 \leq i \leq n)$ linéairement indépendante sur k soit linéairement indépendante sur K.*

La première assertion (sur les ensembles algébriques irréductibles) résulte du théorème 1, a). Pour que E soit absolument irréductible, *i.e.* pour que E^K soit irréductible, il faut et il suffit que le quotient de $k(E)\otimes K$ par l'idéal de ses éléments nilpotents soit intègre. Comme K est algébriquement clos, il résulte du théorème 1 de l'exposé 14 de **SCC** que ceci signifie que $k(E)$ est extension primaire de k. Enfin en vertu du lemme 3, l'assertion que, pour tout ouvert U de E, l'algèbre $\mathcal{O}^E(U)$ est linéairement disjointe de l'algèbre des constantes à valeurs dans K équivaut à la même assertion pour les ouverts affines. Ceci signifie que, pour tout ouvert affine U, l'algèbre $\mathcal{O}^E(U) \otimes K$ est sans élément nilpotent, donc que $k(U)\otimes K$ est sans élément nilpotent. Comme les composantes irréductibles de U sont les $U \cap E_i$ non vides (les E_i étant les composantes irréductibles de E), $k(U)$ est isomorphe au produit des $k(E_i)$ pour les i tels que $U \cap E_i$ soit non vide. L'assertion de linéaire disjonction signifie donc que $k(E_i) \otimes K$ est sans élément nilpotent, donc sans radical (**SCC**, exposé 13, théorème 3) ou encore que $k(E_i)$ est extension séparable de k (ceci pour tout i).

Définition 2. – *On appelle variété algébrique*[5] *un ensemble algébrique absolument irréductible, dans lequel, pour tout ouvert U, l'algèbre $\mathcal{O}^E(U)$ des fonctions régulières sur U est linéairement disjointe sur k de l'algèbre des constantes à valeurs dans K.*

Dire qu'un ensemble algébrique E est une variété signifie donc que E est irréductible et que l'extension $k(E)$ de k est primaire et séparable, *i.e. régulière.*

[5] Cette définition équivaut à celle de Weil.

Corollaire 4. – *Soient E_1 une variété et E_2 un ensemble algébrique ; si E_2 est irréductible* (resp. absolument irréductible, resp. une variété)*, alors $E_1 \times E_2$ est irréductible* (resp. absolument irréductible, resp. une variété)*.*

Cela résulte du corollaire 3 et des propriétés du produit tensoriel d'une extension avec une extension régulière (**SCC**, exposé 14, proposition 3).

Corollaire 5. – *Soient E un ensemble algébrique et F un fermé de E. S'il existe un ouvert affine U de E tel que $U \cap F$ soit dense dans F, toute fonction rationnelle sur F est la trace d'une fonction rationnelle sur E.*

Soit f une fonction rationnelle sur F ; on peut écrire $f = g/h$ où $h \neq 0$ est régulière sur $F \cap U$ et où g est régulière sur l'ouvert partout dense $V(h)$ de $F \cap U$. Comme U est affine, il existe une fonction régulière h' sur U qui induit h sur $F \cap U$ et comme l'ouvert $V(h')$ de U est affine, il existe une fonction régulière g' sur $V(h')$ induisant g sur $V(h)$. La fonction g'/h', régulière sur l'ouvert $V(h')$, induit alors f sur $V(h)$ et se prolonge par ailleurs d'après le lemme 1 en une fonction rationnelle sur E.

Remarque. – Le corollaire 5 s'applique lorsque E est affine, ou lorsque F est irréductible, car il y a au moins un ouvert affine recontrant F. On peut montrer qu'il en est de même lorsque E est projectif, mais la variété non projective de Nagata met le corollaire 5 en défaut dans le cas général.

2.5 Schémas

Soient L un anneau commutatif dans lequel tout élément est diviseur de 0 ou inversible et A un sous-anneau de L ; si $\mathfrak{p}$ est un idéal premier de A, on désignera par $A_\mathfrak{p}$ le sous-anneau de L formé des as^{-1} avec $a \in A$ et $s \in A \cap \complement\mathfrak{p}$, s non diviseur de zéro.

Définition 3. – *Soit L une algèbre semi-simple commutative sur le corps k. On appelle algèbre affine de L toute sous-algèbre A de type fini de L telle que tout élément de L soit de la forme ab^{-1} avec a, b dans A. Un couple $(M, \mathfrak{m})$ formé d'une sous-algèbre M de L et d'un idéal $\mathfrak{m}$ de M est appelé une localité de L s'il existe une algèbre affine A et un idéal premier $\mathfrak{p}$ de A tels que $M = A_\mathfrak{p}$ et $\mathfrak{m} = \mathfrak{p}A_\mathfrak{p}$. Deux localités $(M_i, \mathfrak{m}_i)$ $(i = 1, 2)$ de L sont dites apparentées si l'idéal $\mathfrak{m}$ engendré par $\mathfrak{m}_1$ et $\mathfrak{m}_2$ dans l'anneau M engendré par M_1 et M_2 est distinct de M.*

Lorsque L est un corps, ces définitions sont en accord avec les définitions de Chevalley (**SCC**, exposé 5). Nous allons étendre au cas qui nous intéresse des lemmes connus lorsque L est un corps.

Lemme 5. – *Si $(M, \mathfrak{m})$ est une localité de la forme $(A_\mathfrak{p}, \mathfrak{p}A_\mathfrak{p})$, l'idéal $\mathfrak{m}$ de M est maximal et $\mathfrak{m} \cap A = \mathfrak{p}$. De plus $M/\mathfrak{m}$ est canoniquement isomorphe au corps des fractions de $A/\mathfrak{p}$.*

Comme l'algèbre semi-simple L n'a pas d'élément nilpotent, il en est de même de A et l'on peut identifier A à l'algèbre des fonctions régulières sur $E = \Omega_A$ et $\mathfrak{p}$ à l'idéal des fonctions régulières nulles sur un sous-ensemble fermé irréductible F de E. Le corollaire 1 du théorème 1 montre que l'on peut identifier L et l'algèbre des fonctions rationnelles sur E, moyennant quoi M est l'ensemble des fonctions rationnelles ayant une trace sur F d'après le théorème 1,b). Pour que $f = ab^{-1}$ $(a, b \in A,\ b \notin \mathfrak{p})$ ait une trace nulle sur F, il faut et il suffit qu'elle soit nulle sur $F \cap V(b)$ donc que a soit nulle sur $F \cap V(b)$ donc sur F par raison de continuité. Ceci signifie que $a \in \mathfrak{p}$, donc que $\mathfrak{m}$ est le noyau de l'opération de restriction. Il en résulte que $\mathfrak{m} \cap A = \mathfrak{p}$, puis que $M/\mathfrak{m}$ est isomorphe à $k(F)$, *i.e.* au corps des fractions de $A/\mathfrak{p}$, donc est un corps (*cf.* corollaire 5 du théorème 1).

Lemme 6. – *Pour que deux localités* $(M_i, \mathfrak{m}_i) = (A_{\mathfrak{p}_i}, \mathfrak{p}_i A_{\mathfrak{p}_i})$ *de* L *soient apparentées, il faut et il suffit qu'il existe un idéal premier* $\mathfrak{q}$ *de l'anneau* A *engendré par* A_1 *et* A_2 *tel que* $\mathfrak{q} \cap A_i = \mathfrak{p}_i$ *pour* $i = 1, 2$.

Soit M l'anneau engendré par M_1 et M_2. Si nos deux localités sont apparentées, il existe un idéal premier $\mathfrak{r}$ de M contenant $\mathfrak{m}_1$ et $\mathfrak{m}_2$. Comme $\mathfrak{m}_i$ est maximal et $\mathfrak{r} \neq M$, on a $\mathfrak{r} \cap M_i = \mathfrak{m}_i$ d'où $(\mathfrak{r} \cap A) \cap A_i = \mathfrak{r} \cap A_i = (\mathfrak{r} \cap M_i) \cap A_i = \mathfrak{p}_i$ et l'idéal $\mathfrak{q} = \mathfrak{r} \cap A$ convient.

Réciproquement, s'il existe un idéal premier $\mathfrak{q}$ de A tel que $\mathfrak{q} \cap A_i = \mathfrak{p}_i$, soit $\mathfrak{r}$ l'idéal engendré par $\mathfrak{q}$ dans M. Les éléments de M sont de la forme $a(s_1 s_2)^{-1}$ avec $a \in A$ et $s_i \in A_i \cap \complement\mathfrak{p}_i$ puisque les éléments de cette forme forment un anneau contenant M_1 et M_2 et qu'ils sont sommes d'éléments de la forme $m_1 m_2$ avec $m_i \in M_i$. Si l'on avait $\mathfrak{r} = M$, on aurait $1 \in \mathfrak{r}$ d'où un couple d'éléments $s_i \in A_i \cap \complement\mathfrak{p}_i$ tels que $s_1 s_2 \in \mathfrak{q}$; mais comme $\mathfrak{q} \cap A_i = \mathfrak{p}_i$, on a $s_i \notin \mathfrak{q}$ d'où $s_1 s_2 \notin \mathfrak{q}$, ce qui est une contradiction. C.Q.F.D.

On notera que si $A_1 = A_2$, les deux localités en question ne peuvent être apparentées que si $\mathfrak{p}_1 = \mathfrak{p}_2$ donc que si elles sont égales.

Nous pouvons maintenant étendre à notre cas la définition des schémas donnée par Chevalley.

Définition 4. – *Soit* L *une algèbre commutative semi-simple sur le corps* k. *On appelle schéma affine* $S(A)$ *de l'algèbre affine* A *de* L *l'ensemble des localités* $(A_{\mathfrak{p}}, \mathfrak{p}A_{\mathfrak{p}})$ *pour tous les idéaux premiers* $\mathfrak{p}$ *de* A. *Un ensemble* S *de localités de* L *est appelé un schéma de* L *s'il vérifie les deux conditions suivantes :*

a) S *est réunion d'un nombre fini de schémas affines.*

b) *Deux localités distinctes de* S *ne sont pas apparentées.*

Le lemme 6 montre que deux localités distinctes d'un schéma affine ne sont pas apparentées, donc qu'un schéma affine est bien un schéma.

Lemme 7. – *Soient* A *une algèbre affine de* L *et* S *un schéma de* L *contenant* $S(A)$ *; les éléments de* $S(A)$ *sont les localités* $(M, \mathfrak{m}) \in S$ *telles que* $M \supset A$.

Si $(M, \mathfrak{m}) \in S(A)$, on a évidemment $M \supset A$. Inversement, si $M \supset A$ et si $\mathfrak{p} = \mathfrak{m} \cap A$, on a $M \supset A_{\mathfrak{p}}$ car tout élément non diviseur de 0 dans M qui n'est pas dans $\mathfrak{m}$ est inversible dans M ; on a par suite $\mathfrak{m} \supset \mathfrak{p}A_{\mathfrak{p}}$, ce qui montre que les localités $(M, \mathfrak{m})$ et $(A_{\mathfrak{p}}, \mathfrak{p}A_{\mathfrak{p}})$ du schéma S sont apparentées, donc égales.

Avant de faire le lien entre les ensembles algébriques et les schémas, nous allons montrer que la structure d'un ensemble algébrique est entièrement déterminée par ses fonctions rationnelles. De manière précise, on définit une structure sur un ensemble E en se donnant un ensemble d'applications de parties de E à valeurs dans K. Nous allons d'abord montrer comment l'on peut reconstituer la topologie et le système local $\mathcal{O}^E$ à partir de l'ensemble des fonctions rationnelles de E.

Proposition 6. – *Soit E un ensemble algébrique ; pour $f \in k(E)$, on note $D_0(f)$ l'ensemble des points où f est définie et non nulle. L'ensemble des ouverts de E est engendré par les ouverts de la forme $D(f)$ ou $D_0(f)$; lorsque E est irréductible, il est même engendré par les ensembles $D(f)$. Si U est un ouvert de E, l'ensemble $\mathcal{O}^E(U)$ est formé des restrictions à U des $f \in k(E)$ tels que $U \subset D(f)$.*

La dernière assertion résulte évidemment du lemme 2 ; de plus, si E est irréductible, et si $f \in k(E)$ est $\neq 0$, $f^{-1} \in k(E)$ et il est clair que $D_0(f) = D(f) \cap D(f^{-1})$.

Soit U un ouvert affine partout dense de E et soient f_i $(1 \leq i \leq n)$ des fonctions rationnelles dont les restrictions à U engendrent l'algèbre $\mathcal{O}^E(U)$. On va montrer que l'on a $U = \bigcap_{i=1}^{n} D(f_i)$. Soit $f \in k(E)$ telle que $D(f) \supset U$; il existe donc un polynôme P à n variables tel que $f \mid U = P(f_1 \mid U, \ldots, f_n \mid U)$ donc $f = P(f_1, \ldots, f_n)$ puisque U est partout dense. Si l'on pose $U' = \bigcap_{i=1}^{n} D(f_i)$, on a donc $D(f) \supset U' \supset U$. Il résulte de ce que l'on a dit que toute fonction de $\mathcal{O}^E(U)$ est la restriction d'une fonction unique de $\mathcal{O}^E(U')$. Supposons $U \neq U'$ et soit $x' \in U' \cap \complement U$; l'application $f \to f(x')$ de $\mathcal{O}^E(U')$ dans K étant un homomorphisme, comme U est affine, il existe $x \in U$ tel que $f(x') = f(x)$ pour tout $f \in \mathcal{O}^E(U')$. Soit V un ouvert affine contenant x' et contenu dans U' ; l'ensemble des fonctions régulières sur $V \times U$ est formé des fonctions $h(z, z') = \sum_j f_j(z)\, g_j(z')$ avec $f_j \in \mathcal{O}^E(V)$ et $g_j \in \mathcal{O}^E(U')$. Pour tirer une contradiction de l'hypothèse $U \neq U'$, on remarque que $x \neq x'$ puisque $x' \notin U$ et $x \in U$ et l'on va montrer que toute fonction régulière sur $V \times U$ nulle sur $\Delta_E \cap (V \times U)$ est nulle en (x', x) contrairement à la proposition 7 de l'exposé 1. Or de $h(y, y) = 0$ pour $y \in V \cap U$, on déduit la même égalité pour $y \in V$ puisque $V \cap U$ est dense dans V et que $\mathcal{O}^E(U') \subset \mathcal{O}^E(V)$ (à un abus de langage près), d'où $h(x', x') = 0$ soit $\sum_j f_j(x')\, g_j(x') = 0$; mais comme $g_j(x') = g_j(x)$, on en déduit $h(x', x) = 0$.

E est réunion finie d'ouverts affines partout denses V_i (lemme 3) ; de plus tout ouvert de V_i est réunion d'ensembles ouverts formés de points où ne s'annule pas $f \in \mathcal{O}^E(V_i)$, *i.e.* de la forme $V_i \cap D_0(f)$. Ceci achève la démonstration.

Nous pouvons maintenant énoncer et démontrer le théorème fondamental de cet exposé.

Théorème 2. – a) *Soit E un ensemble algébrique. L'ensemble des couples $M(F) = (\mathcal{O}(E,F),\ \mathfrak{p}(E,F))$ pour tous les fermés irréductibles F de E est un schéma $\mathcal{S}(E)$ de $k(E)$* (on a noté $\mathfrak{p}(E,F)$ le noyau de $\rho_{E,F}$).

b) *Soit S un schéma d'une algèbre semi-simple L. Soit $\mathfrak{p}(S)$ l'ensemble des triples $(M,\mathfrak{m},\chi)$ où $(M,\mathfrak{m}) \in S$ et χ est un homomorphisme de M dans K nul sur l'idéal $\mathfrak{m}$. Si $f \in L$, on pose $\widehat{f}(x) = \chi(f)$ pour les $x = (M,\mathfrak{m},\chi) \in \mathfrak{p}(S)$ tels que $f \in M$; les fonctions $\widehat{f}$ sont les fonctions rationnelles pour une structure d'ensemble algébrique bien déterminée sur $\mathfrak{p}(S)$.*

c) *Pour $x \in E$, soit χ_x l'application $f \to f(x)$ de $\mathcal{O}(E,\overline{\{x\}})$ dans K. L'application $x \to (\mathfrak{o}(E,\overline{\{x\}}),\mathfrak{p}(E,\overline{\{x\}}),\chi_x)$ est un isomorphisme de E sur $\mathfrak{p}(\mathcal{S}(E))$ et l'application $f \to \widehat{f}$ est un isomorphisme de L sur $k(\mathfrak{p}(S))$ qui applique S sur $\mathcal{S}(\mathfrak{p}(S))$.*

Montrons que $\mathcal{S}(E)$ est un schéma de $k(E)$; soit d'abord U un ouvert affine partout dense de E et soit $A = \mathcal{O}^E(U)$. Le corollaire 1 du théorème 1 montre que A est une algèbre affine de $k(E)$ et comme les ensembles irréductibles fermés F rencontrent U sont en correspondance avec les idéaux premiers $\mathfrak{p}$ de A, le théorème 1, b) montre que les $(\mathcal{O}(E,F),\mathfrak{p}(E,F))$ pour $F \cap U \neq \varnothing$ forment le schéma de l'algèbre affine A. Comme E est réunion finie d'ouverts affines partout denses, $\mathcal{S}(E)$ est réunion finie de schémas affines.

Soient F_i $(i = 1,2)$ deux sous-ensembles irréductibles fermés de E et soit U_i un ouvert affine partout dense rencontrant F_i. Soit $D \subset U_1 \times U_2$ l'ensemble des (x,x) avec $x \in U_1 \cap U_2$; si $A_i = \mathcal{O}^E(U_i)$, on définit un isomorphisme de l'anneau A engendré par A_1 et A_2 dans $k(E)$ sur l'algèbre des fonctions régulières sur D en faisant correspondre à $\sum_j f_j\, g_j$ la fonction

$$(x,x) \to \sum_j f_j(x)\, g_j(x)\,.$$

Si $M(F_1)$ et $M(F_2)$ sont apparentées, en traduisant le lemme 6 en termes géométriques, on trouve un fermé irréductible non vide F de D se projetant en $F_i \cap U_i$ sur le facteur U_i de $U_1 \times U_2$. Ceci montre que F_1 et F_2 coupent $U_1 \cap U_2$ selon le même ensemble non vide, donc sont égaux puisque fermés et irréductibles. On a prouvé que $\mathcal{S}(E)$ satisfait à la condition b) de la définition 4.

Soit A une algèbre affine de L dont le schéma $S(A)$ soit contenu dans S et soit $U = \mathfrak{p}(S(A)) \subset \mathfrak{p}(S)$. Si à $x = (A_{\mathfrak{p}}, \mathfrak{p}A_{\mathfrak{p}}, \chi) \in U$, on associe l'homomorphisme $\varphi(x)$ de A dans K obtenu par restriction de χ à A, on

obtient une application φ de U dans Ω_A. L'application φ est injective car $\mathfrak{p}$ est le noyau de $\varphi(x)$ (lemme 5) et l'on a $\chi(ab^{-1}) = \varphi(x)(a)(\varphi(x)(b))^{-1}$ pour $a, b \in A$ et $b \notin \mathfrak{p}$; elle est surjective, car si χ est un homomorphisme de A dans K, il se prolonge à $A_{\mathfrak{p}}$ ($\mathfrak{p}$ étant le noyau de χ) par la formule $\chi(ab^{-1}) = \chi(a)\,\chi(b)^{-1}$ pour $a, b \in A$ et $\chi(b) \neq 0$. Si $D(f)$ désigne pour $f \in L$ l'ensemble des $(M, \mathfrak{m}, \chi) \in \mathfrak{p}(S)$ tels que $f \in M$, on va montrer que $\varphi(U \cap D(f))$ est un ouvert partout dense de Ω_A. En effet, soit $\mathfrak{a}$ l'idéal de A formé des $g \in A$ tels que $fg \in A$; comme A est une algèbre affine, $\mathfrak{a}$ contient un non diviseur de 0 dans A. Soit $\mathfrak{p}$ un idéal premier de A ; pour que $f \in A_{\mathfrak{p}}$, il faut et il suffit que $\mathfrak{a}$ contienne un élément $g \in \mathfrak{p}$ non diviseur de 0, soit d'après le lemme 4 que $\mathfrak{a} \not\subset \mathfrak{p}$. Il en résulte en particulier que $\varphi(U \cap D(f))$ est le complémentaire dans Ω_A de l'ensemble fermé $F(\mathfrak{a})$ et c'est un ouvert partout dense puisqu'il contient l'ouvert $V(g)$ pour tout $g \in \mathfrak{a}$ non diviseur de 0.

Le lemme 7 et le fait que toute algèbre affine de L est de type fini montrent que si A' est une algèbre affine de schéma $S(A')$ et si $U' = \mathfrak{p}(S(A'))$, l'ensemble $\varphi(U \cap U')$ est intersection finie d'ouverts de Ω_A de la forme $\varphi(U \cap D(f))$ avec $f \in L$, donc est un ouvert partout dense de Ω_A.

Si $x = (M, \mathfrak{m}, \chi) \in U \cap U'$, M contient l'anneau $k[A, A']$ engendré dans L par A et A' et χ induit un homomorphisme de $k[A, A']$ dans K ; il en résulte que si φ' est l'application de U' dans $\Omega_{A'}$ définie comme φ, pour tous les systèmes $f_i \in A$, $f'_i \in A'$ tels que $\sum f_i f'_i = 0$, la fonction $(z, z') \to \sum_i f_i(z)\, f_i(z')$ de $\Omega_A \times \Omega_{A'}$ dans K est nulle au point $(\varphi(x), \varphi'(x))$ pour $x \in U \cap U'$. Inversement, si toutes les fonctions en question s'annulent au point (z, z'), il existe un homomorphisme de $k[A, A']$ dans K qui induit z sur A et z' sur A' ; il existe alors un idéal premier $\mathfrak{q}$ de $k[A, A']$ tel que $\mathfrak{p} = \mathfrak{q} \cap A$ (resp. $\mathfrak{p}' = \mathfrak{q} \cap A'$) soit le noyau de z (resp. z') et (lemme 6) les localités $(A_{\mathfrak{p}}, \mathfrak{p}A_{\mathfrak{p}})$ et $(A'_{\mathfrak{p}'}, \mathfrak{p}'A'_{\mathfrak{p}'})$ sont apparentées, donc égales ; ceci prouve qu'il existe $x \in U \cap U'$ tel que $(z, z') = (\varphi(x), \varphi'(x))$.

La proposition 4 démontre alors l'existence d'une structure d'ensemble algébrique et d'une seule sur $\mathfrak{p}(S)$ pour laquelle les applications canoniques $\mathfrak{p}(S(A)) \to \Omega_A$ soient des cartes pour toute algèbre affine A. De plus, comme dans les notations précédentes $\varphi(U \cap U')$ est dense dans Ω_A, $\mathfrak{p}(S(A))$ est dense dans $\mathfrak{p}(S)$.

Le corollaire 1 du théorème 1 démontre que l'application $f \to \widehat{f}$ de A dans l'algèbre des fonctions régulières sur $\mathfrak{p}(S(A))$ se prolonge en un isomorphisme r de L sur $k(\mathfrak{p}(S(A)))$. Le théorème 1, b) montre aussi que, si F est le fermé irréductible associé à l'idéal premier $\mathfrak{p}$ de A, la localité $(A_{\mathfrak{p}}, \mathfrak{p}A_{\mathfrak{p}})$ est appliquée par r sur la localité $M(F)$ de $k(\mathfrak{p}(S(A)))$. En particulier, si F est l'adhérence du point $x \in \mathfrak{p}(S(A))$, ceci montre que $x \in D(f)$ équivaut à "x appartient au domaine de définition de $r(f)$", donc l'application r est $f \to \widehat{f}$ pour $f \in L$. Comme $\mathfrak{p}(S)$ est recouvert par un nombre fini d'ouverts partout denses $\mathfrak{p}(S(A_i))$, on voit tout de suite que l'application

$f \to \widehat{f}$ est un isomorphisme de L sur $k(\mathfrak{p}(S))$ qui applique S sur le schéma de $\mathfrak{p}(S)$.

Enfin, lorsque U est un ouvert affine de E d'algèbre $A = \mathcal{O}^E(U)$, on voit tout de suite que l'application $x \to (M(\overline{\{x\}}), \chi_x)$ est un isomorphisme de U sur $\mathfrak{p}(S(A))$, et l'on déduit immédiatement de là la première assertion de c). C.Q.F.D.

2.6 Fonctions sur un produit d'ensembles algébriques

Le résultat qu'on va démontrer est un lemme pour un exposé ultérieur. On trouvera dans Weil, *Foundations*, corollaire 2 du théorème 10, p. 241, un résultat sensiblement plus fort, mais de démonstration beaucoup plus délicate.

Soit f_i $(i = 1, 2)$ une fonction rationnelle sur l'ensemble algébrique E_i ; il existe une fonction rationnelle $f_1 \times f_2$ bien déterminée sur l'ensemble $E_1 \times E_2$ par la condition :

$$(f_1 \times f_2)(x_1, x_2) = f_1(x_1)\, f_2(x_2) \qquad \text{pour } x_i \in D(f_i)\,.$$

Proposition 7. – *Soient E_1 et E_2 deux ensembles algébriques. On suppose que $k(E_1)$ ou $k(E_2)$ est une algèbre absolument semi-simple. Il existe un homomorphisme unique φ de*[6] *$k(E_1) \otimes k(E_2)$ dans $k(E_1 \times E_2)$ tel que $\varphi(f_1 \otimes f_2) = f_1 \times f_2$; φ est injectif. De plus si U_i est un ouvert partout dense de E_i $(i = 1, 2)$, φ définit un isomorphisme de $\mathcal{O}^{E_1}(U_1) \otimes \mathcal{O}^{E_2}(U_2)$ sur $\mathcal{O}^{E_1 \times E_2}(U_1 \times U_2)$. En particulier, φ définit un isomorphisme de $\mathcal{O}^{E_1}(E_1) \otimes \mathcal{O}^{E_2}(E_2)$ sur $\mathcal{O}^{E_1 \times E_2}(E_1 \times E_2)$.*

Il est clair que $f_1 \times f_2$ dépend bilinéairement de f_1 et f_2 et qu'on a $(f_1 \times f_2)(f_1' \times f_2') = f_1 f_1' \times f_2 f_2'$, d'où l'existence et l'unicité de φ. Supposons $k(E_1)$ absolument semi-simple et soient $f_{j,1}$ $(1 \leq j \leq m)$ des fonctions rationnelles sur E_1, linéairement indépendantes sur k, donc aussi sur K (corollaire 3 du théorème 1). Soient de plus des fonctions $f_{j,2}$ $(1 \leq j \leq m)$ rationnelles sur E_2 telles que $\sum_{j=1}^{m} f_{j,1} \times f_{j,2} = 0$. On peut supposer les fonctions $f_{j,i}$ définies sur un ouvert partout dense U_i' de E_i $(i = 1, 2)$; on aura alors $\sum_{j=1}^{m} f_{j,1}(x_1)\, f_{j,2}(x_2) = 0$ pour tout $x_i \in U_i'$. Pour x_2 fixé ceci est une relation linéaire à coefficients dans K entre les $f_{j,1}$; d'après l'hypothèse faite, on a donc $f_{j,2}(x_2) = 0$ pour $x_2 \in U_2'$ donc $f_{j,2} = 0$. Ceci montre que φ est injectif. On peut donc identifier $k(E_1) \otimes k(E_2)$ à son image par φ.

Soit g une fonction rationnelle sur $E_1 \times E_2$ dont le domaine de définition contient l'ouvert $U_1 \times U_2$ et soit $V_i \subset U_i$ un ouvert affine partout dense de E_i

[6] On note $\otimes$ le produit tensoriel sur le corps k.

$(i = 1, 2)$ (lemme 3). Comme g induit une fonction régulière sur le produit des ensembles affines V_1 et V_2, il existe des fonctions rationnelles $f_{j,i}$ sur E_i dont le domaine de définition contient V_i telles que $g \mid V_1 \times V_2 = (\sum_{j=1}^{m} f_{j,1} \times f_{j,2}) \mid V_1 \times V_2$, donc $g = \sum_j f_{j,1} \times f_{j,2}$; autrement dit $g \in \mathcal{O}^{E_1}(V_1) \otimes \mathcal{O}^{E_2}(V_2)$. Mais on a $\mathcal{O}^{E_i}(U_i) = \bigcap_{V_i \subset U_i} \mathcal{O}^{E_i}(V_i)$ (où V_i parcourt l'ensemble des ouverts affines partout denses dans U_i) et la proposition résultera du lemme suivant (utile dans d'autres contextes !) :

Lemme 8. – *Soient P et Q deux espaces vectoriels sur le corps k, (P_α) et (Q_β) des familles de sous-espaces de P et Q respectivement. On a :*

$$\left(\bigcap_\alpha P_\alpha\right) \otimes \left(\bigcap_\beta Q_\beta\right) = \bigcap_{\alpha,\beta} (P_\alpha \otimes Q_\beta)\,. \tag{1}$$

Supposons d'abord tous les Q_β égaux à un même sous-espace Q' de Q et soit (y_i) une base de Q'. Les éléments de $P \otimes Q'$ s'écrivent de manière unique sous la forme $\sum_i x_i \otimes y_i$ avec $x_i \in P$; pour qu'un tel élément soit dans $P_\alpha \otimes Q'$, il faut et il suffit que l'on ait $x_i \in P_\alpha$ pour tout i, d'où la formule :

$$\left(\bigcap_\alpha P_\alpha\right) \otimes Q' = \bigcap_\alpha (P_\alpha \otimes Q')\,. \tag{2}$$

On en déduit :

$$\bigcap_{\alpha,\beta} (P_\alpha \otimes Q_\beta) = \bigcap_\beta \left(\bigcap_\alpha (P_\alpha \otimes Q_\beta)\right) = \bigcap_\beta \left(\left(\bigcap_\alpha P_\alpha\right) \otimes Q_\beta\right) = \left(\bigcap_\alpha P_\alpha\right) \otimes \left(\bigcap_\beta Q_\beta\right).$$

C.Q.F.D.

Par un raisonnement analoque et même plus simple, on démontre la proposition suivante :

Proposition 7 bis. – *Soit E un ensemble algébrique tel que $k(E)$ soit une algèbre absolument semi-simple et soit k' un sous-corps de K contenant k. L'homomorphisme φ de $k' \otimes k(E)$ dans $k'(E^{k'})$ qui applique $\lambda \otimes f$ sur λf est injectif. De plus, si U est un ouvert partout dense de E, φ définit un isomorphisme de $k' \otimes \mathcal{O}^E(U)$ sur $\mathcal{O}^{E^{k'}}(U)$.*

3. Groupes algébriques (généralités)[1]

3.1 Définition d'un groupe algébrique

Lorsqu'on sait définir une catégorie de variétés, les produits de variétés et les morphismes (applications régulières), on en déduit par un procédé standard une catégorie de groupes.

Définition 1. – *Un ensemble G est appelé un groupe algébrique sur le corps (algébriquement clos) K s'il est muni d'une structure d'ensemble algébrique*[2] *(sur K) et d'une structure de groupe telles que les applications :*

$$G \times G \to G \quad \textit{définie par} \quad (x, y) \to xy$$

et

$$G \to G \quad \textit{définie par} \quad x \to x^{-1}$$

soient des morphismes.

Exemple. – Le groupe des automorphismes linéaires d'un espace vectoriel V de dimension n sur K est un groupe algébrique, que nous noterons $\mathrm{GL}(V)$; on posera $\mathrm{GL}(n, K) = \mathrm{GL}(K^n)$. Un élément de $\mathrm{GL}(n, K)$ peut être déterminé par les coefficients u_{ij} de la matrice correspondante ; $\mathrm{GL}(n, K)$ apparaît alors comme un ouvert de K^{n^2} (d'où il faut retrancher la sous-variété d'équation $\det(u_{ij}) = 0$). On peut aussi identifier $\mathrm{GL}(n, K)$ à une variété affine dans K^{n^2+1}, en introduisant une coordonnée v, avec $v = (\det(u_{ij}))^{-1}$.

Les sous-groupes algébriques de $\mathrm{GL}(n, K)$ sont, par définition, les groupes algébriques de matrices (par exemple les groupes orthogonaux, symplectiques, le groupe des matrices diagonales,...).

3.2 Composantes d'un groupe algébrique

Théorème 1. – *Soit H un sous-groupe fermé d'un groupe algébrique G. Alors H possède un sous-groupe H_0 et un seul qui est à la fois fermé, irréductible et d'indice fini ; H_0 est invariant dans H. C'est la composante connexe de*

[1] Exposé de M. Lazard, le 19.11.1956

[2] Il s'agit d'une structure de (K, K)-ensemble algébrique au sens de la définition 2 du n° 1.5. On laisse au lecteur le soin de généraliser les résultats de cet exposé au cas des (k, K)-groupes algébriques.

l'élément neutre dans H, et les composantes irréductibles (ou connexes) de H sont les classes modulo H_0.

Démonstration. – L'ensemble H est la réunion finie de ses composantes irréductibles. Soient $A_1, \ldots, A_r$ celles de ces composantes qui contiennent l'élément neutre e. Dans $G^r = G \times \ldots \times G$, la partie $A_1 \times \ldots \times A_r$ est fermée et irréductible. Le morphisme $G^r \to G : (x_1, \ldots, x_r) \to x_1 \ldots x_r$ applique $A_1 \times \ldots \times A_r$ sur $A_1 \ldots A_r$ qui est par suite irréductible ; cet ensemble est donc contenu dans l'une des composantes irréductibles de H, soit dans A_1. Comme tous les A_i contiennent e, on a $A_1 \cup \ldots \cup A_r \subset A_1 \ldots A_r \subset A_1$, ce qui prouve que $r = 1$ et que A_1 (noté désormais H_0) est l'unique composante irréductible de H contenant e. Puisque $y \to xy$ et $y \to yx$ sont des morphismes, l'unique composante irréductible de H contenant un $x \in H$ est $xH_0 = H_0x$, ce qui prouve que H_0 est un sous-groupe invariant d'indice fini. Si H' est un sous-groupe fermé, irréductible et d'indice fini de H, on a $H' \subset H_0$, $[H_0 : H'] < \infty$; comme H_0 est irréductible et est la réunion de ses classes modulo H', on a $H' = H_0$.

Nous dirons désormais que H_0 est la *composante neutre* de H. Les sous-groupes fermés d'indice fini de H sont les sous-groupes qui contiennent H_0. Remarquons qu'un groupe algébrique est irréductible si et seulement s'il est connexe.

3.3 Engendrement de sous-groupes

Rappelons qu'un sous-ensemble A d'un ensemble algébrique est dit *épais* s'il est irréductible et s'il contient une partie relativement ouverte non vide de son adhérence $\overline{A}$.

Si V et W sont des ensembles algébriques, A et B des parties épaisses de V et de W respectivement, alors $A \times B$ est épais dans $V \times W$.

Si A est épais dans V, et si f est un morphisme de V dans W, $f(A)$ est épais dans W (pour la démonstration, *cf.* **SCC**, exposé 7, théorème 3).

Lemme 1. – *Soient H un sous-groupe fermé connexe d'un groupe algébrique et A un ensemble épais dense dans H. Alors on a $H = AA$, autrement dit tout élément de H est un produit de deux éléments de A.*

Soit $x \in H$. Les parties A et xA^{-1} sont épaisses et ont pour adhérence H ; elles contiennent donc deux parties relativement ouvertes dans H, et leur intersection est non vide puisque H est irréductible (comme sous-groupe connexe). Si $a_1 \in A \cap xA^{-1}$, on a $x = a_1a_2$ avec $a_2 \in A$.

Corollaire. – *Tout sous-groupe épais d'un groupe algébrique est fermé.*

Théorème 2. – *Soient G un groupe algébrique, et $(A_1, \ldots, A_r)$ une famille finie de parties épaisses de G contenant chacune l'élément neutre e. Alors le sous-groupe H engendré par $A_1 \cup \ldots \cup A_r$ est fermé connexe.*

Démonstration. – On voit d'abord en utilisant le morphisme $(x_1, \ldots, x_r) \to x_1 \ldots x_r$ que H est engendré par l'unique ensemble épais $A_1 \ldots A_r = A$ contenant e. On peut de même remplacer A par $B = AA^{-1}$. Tout élément de H est alors produit d'une famille finie d'éléments de B, soit $H = \cup_n B^n$, où B^n est l'ensemble des produits de n éléments de B. Or, pour tout entier n, B^n est épais (donc irréductible) et $B^n \subset B^{n+1}$. La suite des adhérences $\overline{B} \subset \ldots \subset \overline{B^n} \subset \overline{B^{n+1}} \subset \ldots$ est stationnaire, sinon les dimensions de ces sous-variétés iraient en croissant indéfiniment. Par conséquent, il existe un n tel que $\overline{B^n} = \overline{B^{n+m}}$ pour $m \geq 0$. Il est clair que $\overline{B^n} = \overline{H}$, puisque H est la réunion des B^{n+m} ; donc B^n est épais et son adhérence est le sous-groupe connexe $\overline{H}$. D'après le lemme, $B^{2n} = \overline{H}$, donc, en particulier, $H = B^{2n} = \overline{H}$.

Corollaire. – *Soient A et B deux sous-groupes fermés d'un groupe algébrique tels que B soit dans le normalisateur de A. Alors le sous-groupe AB est fermé.*

Soient en effet A_0 et B_0 les composantes neutres de A et de B respectivement. Puisque $bAb^{-1} = A$ si $b \in B$, on a $bA_0b^{-1} = A_0$ (théorème 1). Donc A_0B_0 est un sous-groupe fermé connexe (théorème 2). Si $a_1, \ldots, a_r$ et $b_1, \ldots, b_s$ sont des représentants des classes de A et de B modulo A_0 et B_0 respectivement, AB est la réunion finie des fermés $a_iA_0B_0b_j$, et est par suite fermé.

3.4 Groupes résolubles ou nilpotents

Etant donnés deux sous-groupes A et B d'un groupe G, leur groupe de commutateurs (A, B) est engendré par les éléments $aba^{-1}b^{-1}$, où $a \in A$, $b \in B$.

Rappelons qu'un groupe ("abstrait") G est dit résoluble (resp. nilpotent) s'il admet une suite de composition

$$G = H_1 \supset H_2 \supset \ldots \supset H_n \supset H_{n+1} = \{e\} \tag{1}$$

telle que

$$(H_i, H_i) \subset H_{i+1} \qquad (\text{resp. } (G, H_i) \subset H_{i+1})\,. \tag{2}$$

Définition 2. – *Un groupe algébrique G est dit résoluble (*resp. nilpotent*) s'il admet une suite de composition* (1) *constituée par des sous-groupes fermés et vérifiant la condition* (2).

Théorème 3. – *Pour qu'un groupe algébrique soit résoluble (*resp. nilpotent*), il faut et il suffit qu'il soit résoluble (*resp. nilpotent*) en tant que groupe abstrait.*

Démonstration. – Parmi les suites de composition (1) satisfaisant aux conditions (2), il en est qui décroissent plus vite que toutes les autres. On les obtient en posant, dans le cas des groupes résolubles, $H_2 = (G, G), \ldots, H_{i+1} =$

$(H_i, H_i), \ldots$ et, dans le cas des groupes nilpotents, $H_2 = (G, G), \ldots, H_{i+1} = (G, H_i)$. Le théorème 3 est alors une conséquence du résultat suivant :

Proposition 1. – *Si A et B sont deux sous-groupes invariants fermés d'un groupe algébrique, leur groupe des commutateurs (A, B) est fermé.*

Traitons d'abord le cas où A est connexe. Soient $B_0, B_1, \ldots, B_n$ les composantes connexes de B. Pour tout i, l'ensemble des $aba^{-1}b^{-1}$ (avec $a \in A$, $b \in B_i$) est épais, comme image de $A \times B_i$ par un morphisme ; de plus, il contient e (faire $a = e$). Nous sommes donc dans les conditions d'application du théorème 2, et le groupe (A, B) est fermé connexe.

Dans le cas général, soient A_0 et B_0 les composantes neutres de A et B respectivement. Nous venons de voir que (A_0, B) et (A, B_0) sont fermés connexes. Il en est de même de leur produit $(A_0, B)(A, B_0)$ (cor. du th. 2). Or $[A : A_0]$ et $[B : B_0]$ sont finis, et un résultat de R. Baer (*cf.* Appendice, proposition 2) montre que $AB/((A_0, B)(A, B_0))$ est fini. Il en résulte que (A, B) est fermé et que $(A_0, B)(A, B_0)$ est sa composante neutre.

Remarque. – Soient G un groupe algébrique, A et B deux sous-groupes invariants de G, d'adhérences respectives $\overline{A}$ et $\overline{B}$. On déduit facilement de la proposition 1 que $(\overline{A}, \overline{B})$ est l'adhérence de (A, B). On en déduit que le groupe A est commutatif (resp. nilpotent, résoluble) si et seulement si le groupe algébrique $\overline{A}$ possède cette propriété.

3.5 Homomorphismes de groupes algébriques

Théorème 4. – *Soient G et G' deux groupes algébriques, $f : G \to G'$ un homomorphisme de groupes algébriques (i.e.* un homomorphisme en tant que groupes "abstraits" et un morphisme en tant qu'ensembles algébriques*). Alors :*

1) *le noyau N de f est un sous-groupe fermé de G ;*

2) *l'image $f(G)$ est un sous-groupe fermé de G', et sa composante neutre est l'image $f(G_0)$ de la composante neutre de G ;*

3) $\dim N + \dim f(G) = \dim G$.

Démonstration. – Le noyau N est l'image réciproque de l'élément neutre e' de G'. Il est donc fermé.

L'image $f(G_0)$ du sous-groupe connexe G_0 est un sous-groupe épais, donc fermé. De plus G_0 est d'indice fini dans G, d'où aussitôt l'assertion 2) d'après le théorème 1.

Pour démontrer 3), nous utiliserons un résultat de **SCC** (exposé 8, théorème 2), qui peut se traduire ainsi dans le langage des variétés[3] que nous considérons : soient $f : V \to W$ un morphisme de variétés tel que $\overline{f(V)} = W$,

[3] Dans le cas des ensembles (K, K)-algébriques considéré dans cet exposé, une variété est un ensemble algébrique irréductible (*cf.* définition 2 du n° 2.4).

et $e = \dim V - \dim W$. Alors, si W' est une sous-variété de W et V' une composante de $f^{-1}(W')$ telle que $W' = \overline{f(V')}$, on a $\dim V' \geq \dim W' + e$; de plus, la réunion des sous-variétés V' de V telles que $\dim V' > \dim \overline{f(V')} + e$ est un fermé distinct de V. Nous pouvons prendre $V = G_0$, $W = f(G_0)$, avec $\dim V = \dim G$, $\dim W = \dim f(G)$, $\dim N = \dim (N \cap V)$. La première partie du théorème donne, pour $W' = e'$: $\dim N \geq \dim G - \dim f(G)$. La seconde partie donne, pour un x convenable de G, $\dim xN \leq \dim G - \dim f(G)$; comme $\dim xN = \dim N$, la démonstration est achevée.

Enonçons enfin un théorème qui sera démontré ultérieurement (théorème 4 du n° 8.5).

Théorème 5. – *Soient G un groupe algébrique connexe, $H \subset G$ un sous-groupe fermé. Il existe une variété G/H et un morphisme $\pi : G \to G/H$ tels que :*

1) *la relation $\pi(x) = \pi(y)$ est équivalente à $x^{-1}y \in H$ $(x, y \in G)$;*

2) *si $f : G \to V$ est un morphisme de G dans une variété V tel que $x^{-1}y \in H$ entraîne $f(x) = f(y)$, f se factorise sous la forme $g \circ \pi$, où $g : G/H \to V$ est un morphisme. Si H est invariant dans G, G/H est un groupe algébrique et π un homomorphisme.*

3.6 Appendice. Lemmes de théorie des groupes

Soient G un groupe et H un sous-groupe de G. Un système de représentants des classes à gauche xH est une application de G sur une partie $\overline{G}$ de G (application notée $x \to \overline{x}$) telle que : 1) si $x \in G$, $x^{-1}\overline{x} \in H$; 2) si $x, y \in G$, une condition nécessaire et suffisante pour que $x^{-1}y \in H$ est que $\overline{x} = \overline{y}$. Il en résulte que $\overline{\overline{x}} = \overline{x}$ et $\overline{x\,\overline{y}} = \overline{xy}$. Un autre système de représentants $x \to \overline{x}^*$ est défini d'une manière générale en posant $\overline{x}^* = \overline{x}\,\varphi(\overline{x})$, où $\varphi : \overline{G} \to H$ est une application quelconque.

Supposons maintenant H abélien et d'indice $[G : H]$ fini. On définit une application $T : G \to H$ (transfert de G dans H) en posant, pour $x \in G$,

$$T(x) = \prod_{\overline{y} \in \overline{G}} (\overline{x\overline{y}})^{-1}\, x\overline{y}\,. \tag{1}$$

Le transfert ne dépend pas du choix du système de représentants. En effet $\overline{y} \to \overline{xy}$ est, pour tout $x \in G$, une permutation de $\overline{G}$. Si on remplace $\overline{y}$ par $\overline{y}\,\varphi(\overline{y})$, comme plus haut, $T(x)$ est remplacé par

$$\prod_{\overline{y} \in \overline{G}} \varphi(\overline{xy})^{-1}\, (\overline{xy})^{-1}\, x\overline{y}\,\varphi(\overline{y}) = \big(\prod_{\overline{y} \in \overline{G}} \varphi(\overline{xy})^{-1}\, \varphi(\overline{y})\big)\, T(x) = T(x)\,.$$

De plus, T est un homomorphisme. En effet, si $x, x' \in G$, on a

$$T(xx') = \prod_{\overline{y}\in\overline{G}} (\overline{xx'y})^{-1}\, xx'\overline{y} = \prod_{\overline{y}\in\overline{G}} ((\overline{x\overline{x'y}})^{-1}\, x\overline{x'y})((\overline{x'y})^{-1}\, x'\overline{y}) = T(x)\,T(x')\,.$$

Supposons maintenant que H soit le centre Z de G et que $[G : Z] = n$. Soient x un élément de G et j l'ordre de x modulo Z. Nous choisirons un système de représentants des classes suivant Z composé de n/j familles de la forme $(\overline{y}, x\overline{y}, \ldots, x^{j-1}\overline{y})$. Le produit des facteurs correspondants dans $T(x)$ est alors $\overline{y}^{-1}\, x^j\, \overline{y} = x^j$ puisque $x^j \in Z$; donc $T(x) = (x^j)^{n/j} = x^n$. On en conclut que, si $[G : Z] = n < \infty$, l'application $T : x \to x^n$ est un homomorphisme de G dans Z ; comme Z est abélien, $T(x) = 1$ pour x dans le groupe des commutateurs de G.

Revenons au cas d'un groupe G et d'un sous-groupe H d'indice $n = [G : H]$ fini. Supposons que G possède un système de p générateurs $s_1, \ldots, s_p$ et choisissons un système de représentants $\overline{y}$ de G modulo H tel que $\overline{1} = 1$ (et donc $\overline{x} = 1$ pour $x \in H$). Alors les np éléments $(\overline{s_i y})^{-1}\, s_i\, \overline{y}$ $(1 \le i \le p,$ $\overline{y} \in \overline{G})$ engendrent H. En effet, soit $x = s_{i_1}^{e(1)} \ldots s_{i_r}^{e(r)}$ un élément de H $(1 \le i_1, \ldots, i_r \le p,\ e(k) = \pm 1)$, d'où $\overline{x} = 1$. Posons $x_k = s_{i_k}^{e(k)} \ldots s_{i_r}^{e(r)}$, d'où $x_1 = x,\ x_{r+1} = 1$. Posons $u_k = \overline{x_k}^{-1}\, s_{i_k}^{e(k)}\, \overline{x}_{k+1}$; on a alors $x = u_1 \ldots u_r$, car $\overline{x}_1 = \overline{x}_{r+1} = 1$. Suivant que $e(k)$ est $+1$ ou -1, u_k ou son inverse est de la forme $(\overline{s_i y})^{-1}\, s_i\, \overline{y}$, ce qui démontre l'assertion. On en conclut que *tout sous-groupe d'indice fini d'un groupe de type fini est lui-même de type fini.*

Proposition 2. – *Soient G un groupe, et Z son centre, qui est supposé d'indice $n = [G : Z]$ fini. Alors le groupe des commutateurs $(G, G) = G'$ est fini.*

Les commutateurs (x, y) sont définis par $(x, y) = xyx^{-1}y^{-1}$; le groupe G' est engendré par les éléments (x, y) pour $x, y \in G$. Les identités

$$\begin{aligned}(x, yy') &= (x, y)(y, (x, y'))(x, y')\\ (xx', y) &= (x, (x', y))(x', y)(x, y)\end{aligned} \tag{2}$$

montrent que (x, y) ne dépend que des classes de x et de y modulo Z ; G' est donc de type fini. L'indice de $G' \cap Z$ dans G' est $[G' : G' \cap Z] = [G'Z : Z]$ et est donc fini. Le groupe $G' \cap Z$ est alors un groupe abélien de type fini dont tout élément x vérifie $x^n = 1$ (d'après le transfert de G dans Z) ; donc $G' \cap Z$ est fini. Comme $[G' : G' \cap Z]$ est fini, il en résulte que G' est fini.

Si M et N sont deux sous-groupes invariants d'un groupe G, nous désignerons par (M, N) leur groupe des commuteurs, engendré par les (m, n) où $m \in M$, $n \in N$. On a $(M, N) \subset M \cap N$.

Proposition 3. – (Baer) *Soient M, N, M_0 et N_0 des sous-groupes invariants d'un groupe G. Si $M_0 \subset M$, $N_0 \subset N$ et si les groupes $M/(M_0(M, N_0))$ et $N/(N_0(N, M_0))$ sont finis, le groupe $(M, N)/((M, N_0)(N, M_0))$ est fini.*

Passons d'abord au quotient modulo $(M, N_0)(N, M_0)$, *i.e.* supposons que $(M, N_0) = (N, M_0) = \{1\}$; soit $[M : M_0] = i$, $[N : N_0] = j$. Il faut montrer que le groupe $H = (M, N)$ est fini.

Le groupe H est de type fini. En effet les identités (2) montrent que, pour $m \in M$ et $n \in N$, (m, n) ne dépend que des classes de m et n modulo M_0 et N_0 respectivement.

Comme $H = (M, N) \subset M \cap N$, tout élément de H commute avec tout élément de M_0 et tout élément de N_0 ; les groupes $H \cap M_0$ et $H \cap N_0$ sont donc dans le centre de H ; comme $H/(H \cap M_0)$ est isomorphe au sous-groupe HM_0/M_0 de M/M_0, il est fini, et on voit de même que $H \cap N_0$ est d'indice fini dans H. Le centre de H est donc d'indice fini dans H, d'où il résulte (proposition 1) que le groupe des commutateurs $H' = (H, H)$ est fini. Comme H/H' est abélien de type fini, il ne reste plus qu'à majorer les ordres des éléments de H/H'. Soient $m \in M$, $h \in H$. Montrons que $(m, h)^j \in H'$. On a $h^j \in N_0$, d'où $mh^j m^{-1} = h^j$. Or on a

$$mhm^{-1} = (m, h)h \quad h^j = mh^j m^{-1} \equiv (m, h)^j \, h^j \pmod{H'}.$$

Ainsi $(m, h)^j \in H'$ et de même, pour $n \in N$, $(n, h)^i \in H'$. La relation

$$(m, n^k) = (m, n^{k-1})(n^{k-1}, (m, n))(m, n)$$

montre par récurrence que

$$(m, n^k) \equiv (m, n)^k \prod_{r=1}^{k-1} (n^r, (m, n)) \pmod{H'}. \tag{3}$$

Pour $k = j$, $(m, n^k) = 1$ puisque $n^j \in N_0$. Faisons $k = j$ dans (3), puis élevons à la puissance i. Compte tenu des relations $(n^r, (m, n))^i \in H'$, il vient $(m, n)^{ij} \in H'$, ce qui prouve que (m, n) est d'ordre fini modulo H'.

4. Groupes algébriques affines commutatifs[1]

Terminologie et notations. – Pour simplifier, dans toute la suite de ce séminaire, nous supposerons qu'on s'est donné une fois pour toutes un corps de base K *algébriquement clos* (bien qu'un grand nombre de résultats soient vrais sans cette hypothèse) ; un ensemble algébrique sera alors un (K, K)-ensemble algébrique (exposé 1) et une variété est un ensemble algébrique irréductible. Un groupe algébrique n'est pas nécessairement connexe, et n'admet pas nécessairement de représentation linéaire rationnelle fidèle. On appelle *groupe algébrique linéaire* (resp. *groupe algébrique de matrices*) un sous-groupe fermé d'un groupe $\mathrm{GL}(V)$ (V espace vectoriel de dimension finie) (resp. de $\mathrm{GL}(n, K)$).

p désignera l'*exposant caractéristique* de K, égal à la caractéristique si celle-ci est $\neq 0$, à 1 dans le cas contraire.

4.1 Généralités sur les représentations linéaires

Soient G un groupe, u une représentation linéaire de G dans un espace vectoriel V ; G opère aussi dans le dual V' de V par la représentation contragrédiente de u ; le transformé d'un $x \in V$ resp. $x' \in V'$ par $s \in G$ sera noté $s \cdot x$ resp. $s \cdot x'$. Un *coefficient* de u est une fonction sur G de la forme

$$u_{x,x'}(s) = \langle s \cdot x, x' \rangle \qquad (x \in V,\ x' \in V',\ s \in G)\ ;$$

l'espace des coefficients de u est l'espace vectoriel A_u engendré par ses coefficients. Le groupe G opère sur les fonctions numériques définies sur G par les représentations régulières gauche et droite, définies par

$$L_s\, f(t) = f(s^{-1}\, t) \qquad R_s\, f(t) = f(ts)$$

et on a les formules

$$L_s\, u_{x,x'} = u_{x,s\cdot x'} \qquad R_s\, u_{x,x'} = u_{s\cdot x,x'} \tag{1}$$

ce qui prouve en particulier que l'espace des coefficients A_u est invariant par les translations à gauche et à droite. Il s'ensuit, si V est de dimension finie (donc A_u de dimension finie), que l'espace vectoriel engendré par les

[1] Exposé de A. Grothendieck, le 26.11.1956

translatées à gauche et à droite d'un coefficient de u est de dimension finie. Réciproquement, soit f une fonction sur G dont les translatées à droite engendrent un espace de dimension finie V ; alors f est un coefficient d'une représentation linéaire de dimension finie de G dont l'espace des coefficients est l'espace vectoriel engendré par les translatées à gauche et à droite de f : il suffit de prendre la représentation u induite sur V par la représentation régulière droite de G, et l'on a alors $u_{f,\epsilon}(s) = R_s f(e) = f(s)$ (ϵ désigne la forme $g \to g(e)$ sur V). Soit toujours V l'espace d'une représentation linéaire u de dimension finie de G, soit $(x'_i)_{i\in I}$ un ensemble fini de générateurs de l'espace vectoriel V' ; comme pour $x' \in V'$ fixé, $x \to u_{x,x'}$ est une représentation de G-modules de V dans A_u où G opère par les R_s (formule (1)), on obtient une représentation de G-modules $V \to A_u^I : x \to (u_{x,x'_i})_{i\in I}$, qui est évidemment injective, et une représentation de G-modules $V^I \to A_u$: $(x_i) \to \sum_{i\in I} u_{x_i,x'_i}$, qui est évidemment surjective. Donc on a le :

Lemme 1. – *Soit V l'espace d'une représentation linéaire u de dimension finie de G, et soit A_u l'espace de ses coefficients, considéré comme G-module par les translations à droite R_s de G. Alors V est isomorphe à un sous-G-module d'un A_u^n, et A_u est isomorphe à un G-module quotient de V^n. En particulier les composantes simples de V et A_u (dans une suite de composition des G-modules envisagés) sont les mêmes, et V est semi-simple si et seulement si A_u l'est.*

Supposons que G soit un groupe algébrique, et soit $A(G)$ l'algèbre des fonctions régulières sur G. Pour qu'une représentation linéaire u de G dans un espace vectoriel V de dimension finie soit rationnelle, il faut et il sufit que ses coefficients soient des fonctions régulières, *i.e.* que $A_u \subset A(G)$. D'ailleurs :

Lemme 2. – *Soit f une fonction régulière sur G. Alors l'espace vectoriel engendré par ses translatées à droite est de dimension finie (donc f est le coefficient d'une représentation linéaire rationnelle de G).*

On a en effet $R_s f(t) = f(st)$; c'est là une fonction régulière sur $G\times G$ donc de la forme $\sum g_i(s)\, h_i(t)$ (proposition 7 du n° 2.6), donc $R_s f$ est combinaison linéaire des h_i, d'où la conclusion. Conjugant les lemmes 1 et 2, on trouve :

Corollaire. – *Pour que toute représentation linéaire rationnelle de G soit semi-simple, il faut et il suffit que $A(G)$ soit semi-simple pour la représentation régulière droite de G ; les représentations simples de G sont isomorphes à des représentations induites sur les sous-espaces de $A(G)$.*

La condition envisagée sur G est vérifiée par exemple si la caractéristique est nulle et G semi-simple. Dans le cas de caractéristique quelconque, un exemple important sera étudié dans le n° 4.3.

Proposition 1. – *Pour qu'un groupe algébrique soit isomorphe à un groupe linéaire, il faut et il suffit que ce soit un ensemble algébrique affine.*

C'est évidemment nécessaire, puisque $\mathrm{GL}(n, K)$ est un ensemble algébrique affine, et qu'il en est donc de même de toute partie fermée de $\mathrm{GL}(n, K)$. Supposons inversement G affine ; alors $A(G)$ est une algèbre à engendrement fini, et, compte tenu du lemme 2, il existe donc un sous-espace vectoriel V de dimension finie de $A(G)$, engendrant l'algèbre $A(G)$, et invariant sous les R_s. Soit u la représentation rationnelle de G dans V définie par les R_s ; je dis que c'est là un isomorphisme de G dans $\mathrm{GL}(V)$, *i.e.* que toute fonction régulière sur G provient d'une fonction régulière sur $\mathrm{GL}(V)$. Or il en est ainsi des $f \in V$ puisque ce sont des coefficients de u, donc de toute $f \in A(G)$ puisque V engendre l'algèbre $A(G)$.

Nous dirons dorénavant *groupe algébrique affine* au lieu de "groupe algébrique isomorphe à un groupe linéaire". Rappelons qu'un tel groupe est connexe (pour la topologie de Zariski) si et seulement si c'est un ensemble algébrique irréductible.

4.2 Sous-groupes fermés d'un groupe algébrique affine

Théorème 1. – (Chevalley)[2] *Soient G un groupe algébrique affine, H un sous-groupe fermé. Alors il existe un nombre fini d'éléments F_i de $A(G)$ tels que H soit l'ensemble des $s \in G$ admettant les F_i comme semi-invariants dans la représentation linéaire régulière droite de G dans $A(G)$. On peut supposer que les F_i sont des semi-invariants de même poids sous H. Si G est connexe, il existe un nombre fini de fonctions rationnelles G_i sur G telles que H soit l'ensemble des $s \in G$ tels que $R_s\, G_i = G_i$ pour tout i.*

Rappelons qu'on dit qu'un élément F d'un espace vectoriel où opère un groupe est *semi-invariant* sous un $s \in G$ si sF est de la forme $\lambda(s)F$, où $\lambda(s) \in K$ est évidemment bien déterminé si $F \neq 0$; l'ensemble des $s \in G$ admettant F comme semi-invariant est évidemment un sous-groupe, et $\lambda(s)$ est un caractère multiplicatif sur ce sous-groupe, appelé *poids* du semi-invariant F.

Démontrons le théorème. Soit $\mathfrak{a}$ l'idéal dans $A(G)$ des fonctions nulles sur H ; cet idéal admet un nombre fini de générateurs, et en vertu du lemme 2, l'espace vectoriel invariant à droite V engendré par ces générateurs est de dimension finie. Soit $W = V \cap \mathfrak{a}$; ce sous-espace engendre l'idéal $\mathfrak{a}$; de plus comme $\mathfrak{a}$ est évidemment invariant sous les R_s ($s \in H$), il en est de même de W. Réciproquement, soit $s \in G$ tel que $s \cdot W \subset W$; alors $s \in H$ car pour $f \in W$ on a $R_s\, f \in W$ d'où $R_s\, f(e) = 0$ d'où $f(s) = 0$, et comme les $f \in W$ engendrent $\mathfrak{a}$, on en conclut $s \in H$. Soient d la dimension de W, E

[2] Une traduction géométrique est la suivante : *il existe une représentation projective rationnelle de G* (*cf.* n° 15.2), *agissant dans un espace projectif P, et un point de P dont H soit le stabilisateur.*

la puissance extérieure d-ième de V, u la représentation de G dans E définie par les R_s, a l'élément de E produit des éléments d'une base de W. Il est bien connu que $R_s W \subset W$ équivaut au fait que a soit un semi-invariant sous $u(s)$. Soit $(e_i)_{0\leq i\leq n}$ une base de E avec $e_0 = a$, et soit $(F_{ij}(s))$ la matrice de $u(s)$ par rapport à cette base ; on a $u(ts) = u(t)\,u(s)$, d'où

$$F_{i0}(ts) = \sum_{j=0}^{n} F_{ij}(t)\,F_{j0}(s)\,. \tag{2}$$

Posons $F_i = F_{i0}$ pour $1 \leq i \leq n$. D'après ce qui précède, $s \in H$ équivaut à $F_{i0}(s) = 0$ pour $1 \leq i \leq n$, d'où en vertu de (2)

$$R_s\,F_i(t) = F_{00}(s)\,F_i(t) \quad (s \in H)\,. \tag{3}$$

Donc les F_i sont bien des semi-invariants sous H, de même poids $F_{00}(s)$. Inversement, soit $s \in G$ tel que l'on ait $R_s\,F_i = \lambda_i\,F_i$ pour $1 \leq i \leq n$, d'où $F_i(ts) = \lambda_i\,F_i(t)$ pour tout t ; faisant $t = e$ il vient, puisque $F_i(e) = 0$ pour $i > 0$: $F_i(s) = 0$ pour $i > 0$, d'où $s \in H$. Les F_i satisfont aux conditions voulues. Si G est connexe, on voit de même que les $G_i = F_i/F_{00}$ satisfont aux conditions de l'énoncé.

Corollaire. – *Soit H un sous-groupe invariant fermé du groupe algébrique affine G. Alors il existe une représentation linéaire rationnelle de G de noyau H.*

Avec les notations du théorème 1, soit λ le poids commun des semi-invariants F_i de H. Soit E l'espace vectoriel engendré par les F_i et leurs translatées à droite par G ; il est de dimension finie (lemme 2). Soit E_0 le sous-espace vectoriel de E formé des f telles que $R_s\,f = \lambda(s)f$ pour tout $s \in H$. C'est un sous-espace vectoriel de E contenant les F_i, de plus invariant sous G grâce au fait que H est invariant ; il est donc identique à E. Soit u la représentation linéaire rationnelle de G dans E définie par les R_s ; alors $s \in H$ équivaut à dire que $u(s)$ est un scalaire, ou encore[3] que $(\overset{\vee}{u} \otimes u)(s)$ est l'identité : on prendra donc la représentation rationnelle $\overset{\vee}{u} \otimes u$ de G dans $E' \otimes E$ déduite de u, elle satisfait à la condition voulue.

4.3 Groupes algébriques diagonalisables

Soit $D(n)$ le sous-groupe de $\mathrm{GL}(n, K)$ formé des matrices diagonales ; ce sous-groupe est canoniquement isomorphe à K^{*n}, où $K^* = \mathrm{GL}(1, K)$ désigne le groupe multiplicatif des éléments non nuls de K (noté aussi $\mathbf{G}_m(K)$). Un

[3] On note $\overset{\vee}{u}$ la représentation contragrédiente de u, opérant dans le dual E' de E.

sous-groupe de $\mathrm{GL}(n, K)$ est dit *diagonal* s'il est contenu dans $D(n)$, *diagonalisable* s'il est conjugué à un sous-groupe de $D(n)$; plus généralement une représentation linéaire d'un groupe G dans un espace vectoriel V (de dimension finie) est dite diagonalisable[4] s'il existe une base telle que l'image de G soit un groupe diagonal par rapport à cette base. Enfin, un *groupe algébrique diagonalisable* G est un groupe algébrique isomorphe à un sous-groupe de $D(n)$ (il résultera du corollaire 3 au théorème 2 ci-dessous que, dans le cas où G est un groupe algébrique de matrices, cette dernière terminologie est compatible avec la précédente). Un *tore algébrique* est un groupe algébrique isomorphe à K^{*n}.

K^* s'obtient à partir de la variété affine K en enlevant la variété des zéros de la fonction X, donc (exposé 1) $A(K^*) = K[X][1/X]$, et $A(K^*)$ a pour base sur K les monômes X^k ($k \in \mathbf{Z}$), qui sont d'ailleurs des caractères rationnels multiplicatifs de K^*. Donc $A(K^{*n})$, isomorphe au produit tensoriel de n copies de $A(K^*)$, a comme base les monômes $X_1^{k_1} X_2^{k_2} \dots X_n^{k_n}$, avec $(k_i) \in \mathbf{Z}^n$. Ce sont encore des caractères rationnels de K^{*n}, et il n'y en a pas d'autres (à cause de l'indépendance linéaire des caractères). Donc :

Théorème 2. – *$A(K^{*n})$ a pour base les caractères rationnels de K^{*n}, qui sont les monômes $X_1^{k_1} \dots X_n^{k_n}$ avec $(k_i) \in \mathbf{Z}^n$. Donc (corollaire du lemme 2) toute représentation linéaire rationnelle de K^{*n} est diagonalisable.*

Utilisant maintenant le corollaire du théorème 1, on obtient :

Corollaire 1. – *Tout sous-groupe fermé de K^{*n} est l'intersection des noyaux d'un nombre fini de caractères.*

Soient D un tore isomorphe à K^{*n}, $X(D)$ le groupe de ses caractères rationnels, isomorphe au groupe additif $\mathbf{Z}^n$ d'après ce qui précède. Posons $\{x, \hat{x}\} = \hat{x}(x)$ pour $x \in D$, $\hat{x} \in X(D)$. Pour $A \subset D$, soit A^0 l'ensemble des $\hat{x} \in X(D)$ tels que $\{x, \hat{x}\} = 1$ pour tout $x \in A$; définissons de façon symétrique B^0 pour une partie $B \subset X(D)$. D'après le corollaire 1, si A est un sous-groupe fermé de D, on a $A = (A^0)^0$. D'autre part, A^0 est un sous-groupe de $X(D)$, tel que $p\hat{x} \in A^0$ implique $\hat{x} \in A^0$ (puisque toute racine p-ième de l'unité dans K est égale à 1). On peut donc trouver une base $(e_i)_{1 \le i \le n}$ de $X(D)$ et des entiers r avec $0 \le r \le n$ et k_i ($1 \le i \le r$) tels que les $k_i\, e_i$ ($1 \le i \le r$) forment une base de A^0 ; les k_i sont alors premiers à p. Les e_i définissent un isomorphisme de D sur K^{*n}, et faisant l'identification $D = K^{*n}$, A est défini par les équations $X_i^{k_i} = 1$ ($1 \le i \le r$), donc est isomorphe au produit de K^{*n-r} et des groupes $\mu(k_i)$ des racines k_i-ièmes de l'unité, qui sont des groupes cycliques d'ordre k_i (donc premier à p). Réciproquement, un groupe algébrique ayant cette structure est évidemment diagonalisable, donc :

[4] La définition donnée signifie aussi que u est somme directe de représentations de dimension 1, donc semi-simple.

Corollaire 2. – *Pour qu'un groupe algébrique G soit diagonalisable, il faut et il suffit qu'il soit isomorphe au produit d'un tore par un groupe abélien fini d'ordre premier à p.*

Corollaire 3. – *Soient D un groupe algébrique diagonalisable, $X(D)$ le groupe des caractères rationnels de D. Alors on a ce qui suit :*

a) *$X(D)$ est une base de $A(D)$, donc toute représentation linéaire rationnelle de D est diagonalisable.*

b) *$X(D)$ est un groupe abélien de type fini dont le groupe de torsion est d'ordre premier[5] à p, et tout groupe abélien de type fini sans p-torsion est isomorphe à un groupe $X(D)$. Le groupe D s'identifie à l'ensemble $\widehat{X(D)}$ des homomorphismes de $X(D)$ dans K^*.*

c) *Les applications $A \to A^0$ et $B \to B^0$ définissent des bijections réciproques l'une de l'autre entre l'ensemble des sous-groupes fermés A de D, et l'ensemble des sous-groupes B de $X(D)$ tels que $X(D)/B$ n'ait pas de p-torsion. Si A et B se correspondent ainsi, on a $X(D/A) = B$, $X(A) = X(D)/B$.*

Prouvons d'abord b). On a $D = F \times D_0$, où F est un groupe abélien fini d'ordre premier à p, et D_0 un tore, d'où $X(D) = X(F) \times X(D_0)$. Comme F est d'ordre premier à p, $X(F)$ est isomorphe au groupe dual[6] ordinaire $\hat{F}$ de F, et est donc isomorphe (non canoniquement) à F ; d'autre part $X(D_0)$ est isomorphe à un groupe $\mathbf{Z}^n$, d'où la structure annoncée pour $X(D)$. Il est classique que $\hat{\hat{F}} = F$, de plus $\widehat{X(D_0)} = D_0$ comme on voit aussitôt en faisant $D_0 = K^{*n}$, d'où aussitôt $\widehat{X(D)} = \hat{\hat{F}} \times \widehat{X(D_0)} = F \times D_0 = D$. Enfin, un groupe abélien de type fini sans p-torsion est isomorphe à un groupe $F' \times \mathbf{Z}^n$, où F' est fini d'ordre premier à p, donc le groupe envisagé est isomorphe au dual de $\hat{F}' \times K^{*n}$.

a) Soit toujours $D = F \times D_0$. Alors $X(F) = \hat{F}$ est une base de $A(F)$ pour des raisons de dimension, nous avons déjà vu que $X(D_0)$ est une base de $A(D_0)$, donc $X(D) = X(F) \times X(D_0)$ est une base de $A(D) = A(F \times D_0) = A(F) \otimes A(D_0)$.

La deuxième assertion résulte du corollaire au lemme 2.

c) Pour établir la première assertion, il suffit de prouver $A^{00} = A$ et $B^{00} = B$ pour A et B comme dans l'énoncé. La première assertion se démontre comme le corollaire 1, en utilisant le corollaire au théorème 1 et la partie a) ci-dessus. La relation $B^{00} = B$ signifie que B est l'intersection d'une famille de noyaux d'homomorphismes de $X(D)$ dans K^*, ou encore (passant au quotient par B) que si E est un groupe abélien de type fini sans p-torsion, alors l'intersection des noyaux des homomorphismes de E dans K^* est réduit à 0 ; ce qui résulte par exemple de b). Enfin la relation $X(D/A) = A^0$ est

[5] Autrement dit, $X(D)$ est sans p-torsion.

[6] Si F est un groupe abélien, son *dual* $\hat{F}$ est par définition le groupe $\mathrm{Hom}(F, K^*)$.

triviale[7], et $X(A) = X(D)/A^0$ se voit ainsi : en vertu de a) et b), $X(D)/A^0$ est le groupe des caractères rationnels du groupe des homomorphismes de $X(D)/A^0$ dans K, muni de la structure d'ensemble algébrique affine dont les fonctions régulières sont les combinaisons linéaires des caractères provenant des éléments de $X(D)/A^0$; or le groupe en question est manifestement $A^{00} = A$, muni de la structure induite par D, d'où la conclusion. C.Q.F.D.

Soient D, D' deux groupes algébriques diagonalisables, u un homomorphisme rationnel de D dans D'. On désigne par ${}^t u$ l'homomorphisme $\chi \to \chi \circ u$ de $X(D')$ dans $X(D)$; on a évidemment ${}^t(uv) = {}^t v\, {}^t u$, ${}^t(\text{identité}) = \text{identité}$ ${}^t(u+v) = {}^t u + {}^t v$ (en supposant D, D' écrits additivement). On peut de même à tout homomorphisme $\hat{u} : X(D') \to X(D)$, faire correspondre un homomorphisme rationnel ${}^t\hat{u}$ de D dans D', en utilisant le corollaire 3, b). On vérifie alors tout de suite :

Corollaire 4. – *L'application $u \to {}^t u$ est un isomorphisme du groupe des homomorphismes rationnels de D dans D' sur le groupe* $\mathrm{Hom}\,(X(D'), X(D))$.

Proposition 2. – *Soit D un groupe algébrique diagonalisable. Alors pour tout entier n, l'ensemble des éléments x de D tels que $x^n = e$ est un sous-groupe fini, et la réunion de ces sous-groupes est dense dans D. Si D est un tore, ℓ un nombre premier $\neq p$, il suffit de faire parcourir à n l'ensemble des puissances de ℓ.*

C'est là une conséquence immédiate du corollaire 2, et du fait que le sous-groupe de K^* formé des racines de l'unité d'ordre une puissance de ℓ est infini, donc dense puisque K^* est de dimension 1.

Corollaire. – *Si D est un sous-groupe fermé diagonalisable invariant dans un groupe algébrique connexe G, il est contenu dans le centre.*

En effet, pour tout n, le sous-groupe D_n de D formé des éléments d'ordre divisant n est un sous-groupe fini invariant dans G ; il est donc contenu dans le centre de G puisque G est connexe, d'après un raisonnement bien connu. La réunion des D_n étant dense dans D, et le centre de G étant fermé, la conclusion apparaît.

4.4 Eléments semi-simples et unipotents

Soit V un espace vectoriel de dimension finie. Un endomorphisme x de V est dit *semi-simple* si V est un module semi-simple sur l'algèbre avec unité engendrée par x dans $\mathrm{End}\,(V)$, ou encore (puisque K est algébriquement clos) si x est diagonalisable. Rappelons le fait bien connu : x peut se mettre de

[7] Plus précisément, le groupe quotient D/A peut être muni d'une structure de groupe algébrique quotient qui en fait un groupe diagonalisable, dont le groupe des caractères rationnels est A^0. Pour la construction générale des groupes algébriques quotients, voir l'exposé 8.

façon unique sous la forme $x_s + x_n$, somme d'un endomorphisme semi-simple x_s et d'un endomorphisme nilpotent x_n qui commutent (appelés *partie semi-simple* et *partie nilpotente* de x) ; ce sont des polynômes en x (donc tout endomorphisme commutant à x commute à x_s et x_n) ; de plus les valeurs propres de x et de x_s sont les mêmes. En particulier, x est inversible si et seulement si x_s l'est. Dans ce cas, on peut donc écrire $x = x_s\, x_u$, où $x_u = 1 + x_s^{-1}\, x_n$; x_s et x_u commutent, et $x_u = 1+$ opérateur nilpotent.

Définition 1. – *Un endomorphisme u de V est dit* unipotent *s'il est la somme de l'identité et d'un endomorphisme nilpotent,* i.e. *si toutes ses valeurs propres sont égales à* 1.

Un tel endomorphisme est donc nécessairement un automorphisme.

Proposition 3. – *Soit x un automorphisme de V. Alors x se met de façon unique sous la forme $x = x_s\, x_u$, produit d'un automorphisme semi-simple et d'un automorphisme unipotent qui commutent. De plus, x_s est la partie semi-simple de x définie plus haut. (x_u s'appelle la* partie unipotente *de x.)*

L'existence a été prouvée plus haut. Pour l'unicité, posons $x_u = 1 + n$ où n est nilpotent et commute évidemment à x_s ; on a donc $x = x_s + x_s\, n$, c'est là une décomposition de x en somme d'un opérateur semi-simple et d'un opérateur nilpotent qui commutent, donc x_s est la partie semi-simple de x et par suite bien déterminé, donc aussi $x_u = x_s^{-1}\, x = 1 + x_s^{-1}\, x_n$. De ces formules on conclut que tout endomorphisme permutant à x permute à x_s et x_u. Tenant compte du fait que le produit de deux opérateurs semi-simples (resp. unipotents) qui commutent est encore semi-simple (resp. unipotent) on conclut :

Corollaire. – *Si x et y sont deux automorphismes de V qui commutent, alors $(xy)_s = x_s\, y_s$, $(xy)_u = x_u\, y_u$.*

Notons aussi qu'un automorphisme qui est à la fois semi-simple et unipotent est l'identité.

Proposition 4. – a) *Supposons $p \neq 1$. Pour que l'automorphisme x soit unipotent, il faut et il suffit qu'il soit d'ordre fini égal à une puissance de p.*

b) *Supposons $p = 1$. Pour que l'automorphisme x soit unipotent, il faut et il suffit qu'il existe une représentation rationnelle u du groupe*[8] *algébrique K dans V dont l'image contient x. Une telle représentation est ou bien triviale, ou bien un isomorphisme de K sur son image, et si $x \neq 1$, $u(K)$ est le plus petit sous-groupe algébrique fermé de* $\mathrm{GL}(V)$ *contenant x. De plus u est donné par $u(t) = \exp(tn) = \sum_{k=0}^{\infty} t^k\, n^k/k!$, où n est un endomorphisme nilpotent bien déterminé par u.*

[8] L'ensemble K est considéré comme ensemble algébrique affine avec $A(K) = K[X]$. L'opération de groupe est l'addition $(x, y) \to x + y$ de $K \times K$ dans K. La notation actuelle (2003) est $\mathbf{G}_a(K)$, ou simplement $\mathbf{G}_a$.

Démonstration. – a) Si u est d'ordre fini égal à une puissance de p, il en est de même de ses valeurs propres, qui sont donc égales à 1, et u est donc unipotent. Si u est unipotent, on a $u = 1 + n$, n nilpotent, donc il existe une puissance q de p telle que $n^q = 0$, d'où $u^q = 1^q + n^q = 1$.

b) Soit u une représentation rationnelle de K dans l'espace vectoriel V sur le corps K ; comme le groupe K est abélien et le corps K algébriquement clos, on peut trouver une suite de sous-espaces $0 = V_0 \subset V_1 \subset \ldots \subset V_r = V$ de V stables sous $u(K)$, avec V_{i-1} de codimension 1 dans V_i $(1 \leq i \leq r)$. La représentation de K dans V_i/V_{i-1} déduite de u est une représentation rationnelle de K dans K^*, donc donnée par un polynôme P tel que $P(0) = 1$ et $P(s + t) = P(s)\,P(t)$, d'où résulte facilement $P = 1$. Ainsi les $u(t)$ sont tous unipotents.

Supposons x unipotent, donc $x = 1 + m$ avec m nilpotent ; posons $\log x = \sum_{k=1}^{\infty} (-1)^{k+1}\, m^k/k$, c'est donc un endomorphisme nilpotent, et on peut former $\exp(\log x)$. Comme on a $\exp(\log(1 + N)) = 1 + N$ (identité de séries formelles en N) on a $\exp(\log x) = x$. D'autre part, si n est un endomorphisme nilpotent, $\exp tn = \sum_{k=0}^{\infty} t^k\, n^k/k!$ est un polynôme $u_n(t)$ en t, multiplicatif d'après l'identité bien connue $\exp(T+T')N = (\exp TN)(\exp T'N)$. Prenant $n = \log x$, on obtient $u_n(1) = \exp\log x = x$.

D'ailleurs, si $x \neq 1$, on a $n \neq 0$, et on a pour tout t, on a $tn = \log\exp(tn)$ en vertu de l'identité formelle correspondante, d'où

$$tn = \log u_n(t) = \sum_{k=1}^{r} (-1)^{k+1}(u_n(t) - 1)^k/k$$

(où $r = \dim V$) ; ainsi tn s'exprime par une fonction polynomiale par rapport à $u_n(t)$, donc u_n est un isomorphisme de K sur son image. Il en résulte que cette image est le plus petit sous-groupe algébrique de $\mathrm{GL}(V)$ contenant x : en effet, cela tient au fait que si un sous-groupe fermé de K contient un élément non nul, il est identique à K (puisqu'il contient le groupe engendré par l'élément en question, qui est un sous-groupe infini, et que K est de dimension 1).

Soit enfin u une représentation linéaire rationnelle quelconque de K ; montrons qu'elle est de la forme u_n, (où n est évidemment uniquement déterminé par $n = \log u(1)$). Soit en effet $x = u(1)$; on a vu que x est unipotent, et posant $n = \log x$, on a $u_n(1) = x = u(1)$, donc u_n et u coïncident sur le groupe engendré par 1, donc sur K tout entier.

Corollaire 1. – *Soit f une représentation rationnelle d'un groupe algébrique linéaire G dans un autre G'. Alors f transforme les éléments semi-simples (resp. unipotents) en éléments semi-simples (resp. unipotents).*

Soit $x \in G$. Si x est semi-simple, x est diagonalisable, donc le sous-groupe fermé H de G qu'il engendre est un groupe algébrique diagonalisable. Donc

f induit une représentation linéaire de H qui est diagonalisable (théorème 2, corollaire 3, a)) ; en particulier $f(x)$ est diagonalisable. Si x est unipotent, distinguons deux cas : si $p \neq 1$, x est d'ordre fini égal à une puissance de p en vertu de la proposition 4, a), et il en est de même de $f(x)$ qui est donc unipotent ; si $p = 1$, x est de la forme $u(t)$, où u est une représentation rationnelle de K dont l'image est le plus petit groupe algébrique linéaire contenant x, donc contenue dans G ; par suite, u est une représentation rationnelle de K *dans* G. Donc $f(x) = (f \circ u)(t)$ est contenu dans l'image d'une représentation rationnelle de K, et est donc unipotent.

Du corollaire 1 résulte en particulier qu'on peut parler d'*éléments semi-simples et unipotents d'un groupe algébrique affine* sans référence à une réalisation explicite de ce groupe comme groupe algébrique linéaire.

Corollaire 2. – *Soit x un automorphisme unipotent de V. Alors le plus petit sous-groupe algébrique $G(x)$ de* $\mathrm{GL}(V)$ *contenant x est égal au groupe analogue $G(x^m)$ pour tout entier m* premier à p.

Ceci résulte aussitôt de la structure explicite de $G(x)$, connue grâce à la proposition 4.

Théorème 3. – *Soit G un sous-groupe fermé de* $\mathrm{GL}(V)$. *Alors pour tout $x \in G$, ses parties semi-simple x_s et unipotente x_u sont dans G.*

Pour tout $y \in \mathrm{GL}(V)$, soit $G(y)$ le plus petit sous-groupe algébrique de $\mathrm{GL}(V)$ contenant y. On peut dans l'énoncé ci-dessus remplacer G par $G(x)$, ce qui nous ramène au cas où G est *commutatif*. Soit G_s l'ensemble des parties semi-simples des $y \in G$; alors $G \cup G_s$ est un ensemble d'opérateurs deux à deux permutables. Il existe donc une suite $0 = V_0 \subset V_1 \subset \ldots \subset V_r = V$ de sous-espaces vectoriels de V stables sous $G \cup G_s$, avec V_{i-1} de codimension 1 dans V_i. Notons le :

Lemme 3. – *Soit $0 = V_0 \subset V_1 \subset \ldots \subset V_r = V$ une suite de composition de l'espace vectoriel V, avec V_{i-1} de codimension 1 dans V_i $(1 \leq i \leq r)$. Soit G un ensemble d'endomorphismes de V tels que pour tout $g \in G$, les V_i soient stables sous g et g_s ; supposons enfin l'ensemble G_s des g_s $(g \in G)$ commutatif. Alors il existe une base $(e_1, \ldots, e_r)$ de V telle que, pour tout $g \in G$, la matrice de g par rapport à cette base soit triangulaire, et celle de g_s en soit la partie diagonale.*

En effet, il est bien connu, puisque les g_s commutent entre eux et sont semi-simples, que l'algèbre d'endomorphismes de V qu'ils engendrent est semi-simple ; donc pour tout i on peut trouver un supplémentaire L_i de V_{i-1} dans V_i stable sous les g_s. Il suffit alors de prendre pour e_i un élément non nul de L_i.

Si G est de plus un groupe algébrique, il résulte alors, sous les hypothèses du lemme 3, que $g \to g_s$ est une représentation rationnelle u de G à valeurs dans le groupe diagonal $D(r)$. Nous voulons donc montrer que dans le cas

actuel (G commutatif) on a $u(G) \subset G$. Or $u(G)$ est un sous-groupe fermé de $D(r)$, et en vertu de la proposition 2, il suffit de prouver que tout élément d'ordre fini m de ce sous-groupe $u(G)$ est dans G. D'ailleurs, en vertu de la structure des groupes algébriques diagonalisables (théorème 2, corollaire 2) m est premier à p. Soit donc $x \in G$ tel que x_s soit d'ordre m ; de $x = x_s\, x_u$ on tire $x^m = x_s^m\, x_u^m = x_u^m$, d'où $x_u^m \in G$ et par suite, en vertu du corollaire 2 de la proposition 4, on a $x_u \in G$, d'où $x_s = x x_u^{-1} \in G$. C.Q.F.D.

Il résulte du théorème 3 que si G est un groupe algébrique affine, tout $x \in G$ se met de façon unique sous la forme $x = x_s\, x_u$ du produit d'un élément semi-simple et d'un élément unipotent qui commutent, et qui sont donc définis en fonction de x sans référence à une réalisation explicite de G comme groupe algébrique linéaire : on les appelle encore *partie semi-simple* et *partie unipotente* de x. Si G est un groupe affine, on désigne par G_s (resp. G_u) l'ensemble de ses éléments semi-simples (resp. unipotents). On a donc $G_s \cap G_u = \{e\}$, $G_s\, G_u = G_u\, G_s = G$.

Corollaire. – *Soit f une représentation rationnelle d'un groupe algébrique affine G dans un autre G'. Pour tout $x \in G$, on a*

$$f(x)_s = f(x_s)\,, \qquad f(x)_u = f(x)_u\,.$$

Tout élément semi-simple (resp. unipotent) de $f(G)$ est image d'un élément semi-simple (resp. unipotent) de G.

Les formules écrites sont une conséquence immédiate de la définition et du corollaire 1 de la proposition 4. La dernière assertion en résulte immédiatement.

4.5 Groupes algébriques affines commutatifs

Théorème 4. – *Soit G un groupe algébrique affine* commutatif. *Alors G_s et G_u sont des sous-groupes fermés de G, et G s'identifie à leur produit direct.*

Nous avons déjà vu, comme conséquence du lemme 3, que $x \to x_s$ est une représentation rationnelle de G dans G, et évidemment de G sur G_s, donc $x \to x_u = x x_s^{-1}$ est une représentation rationnelle de G sur G_u. Donc G_s et G_u sont des sous-groupes fermés de G ; d'autre part, l'application naturelle $(s, u) \to su$ de $G_s \times G_u$ dans G est un homomorphisme rationnel, et $x \to (x_s, x_u)$ en est un homomorphisme rationnel réciproque. C.Q.F.D.

Remarque. – L'étude de la structure des groupes algébriques affines commutatifs est donc ramenée, grâce au théorème 4 et au n° 4.3, à celle des groupes algébriques commutatifs unipotents (un groupe algébrique est dit *unipotent* si tout ses éléments sont unipotents). En caractéristique 0, il résulte facilement

de la proposition 4 qu'un tel groupe est isomorphe à un K^n (et en particulier, il est connexe). En caractéristique $\neq 0$, un groupe unipotent commutatif n'est pas nécessairement connexe (exemple : $\mathbf{Z}/(p)$) et même s'il est connexe et de dimension 2, il n'est pas nécessairement isomorphe à un K^n (ce sera alors une extension commutative non triviale de K par K). Chevalley a montré qu'on peut classifier les groupes algébriques affines commutatifs unipotents à "isogénie près" comme produits de "groupes de Witt" dont les dimensions sont bien déterminées (à l'ordre près) par le groupe donné. Notons que la source de cette différence entre le cas $p = 1$ et $p \neq 1$ semble le fait que si $p \neq 1$, il y a d'autres représentations rationnelles de K dans lui-même que les homothéties, savoir toutes les applications du type $t \to t^{p^k}$ et leurs combinaisons linéaires à coefficients dans K (on voit facilement d'ailleurs qu'il n'y en a heureusement plus d'autres). D'où dans K^n un grand nombre de sous-groupes à un paramètre d'allure bizarre ; d'autre part, les automorphismes de K^n considéré comme groupe algébrique ne sont en général pas linéaires.

4.6 Connexité des centralisateurs

Proposition 5. – *Soient G un groupe algébrique affine, et N un sous-groupe invariant fermé commutatif. Pour tout $g \in G$, soit σ_g l'automorphisme $n \to gng^{-1}$ de N qu'il définit, et soient N'_g resp. N''_g le noyau et l'image de l'endomorphisme $n \to \gamma_g n = (\sigma_g n)\, n^{-1} = gng^{-1} n^{-1}$ de N. Si g est semi-simple (resp. unipotent) et si $N = N_u$ (resp. $N = N_s$), on a $N'_g \cap N''_g = e$, et γ_g est un homomorphisme bijectif de N''_g sur lui-même ; si de plus N est connexe, on a alors $N = N'_g N''_g$ et N'_g et N''_g sont connexes.*

Comme N est commutatif, γ_g est évidemment un homomorphisme rationnel de N dans lui-même, donc N'_g et N''_g sont des sous-groupes fermés de N dont la somme des dimensions est égale à la dimension de N (théorème 4 du n° 3.5). Si l'on prouve la relation $N'_g \cap N''_g = \{e\}$, il s'ensuit que γ_g est injectif sur N''_g, donc bijectif pour des raisons de dimensions : $\gamma_g(N''_g)$ est un sous-groupe fermé de N''_g qui a même dimension que N''_g, l'image par γ_g de la composante neutre $N''_{g,0}$ dans N''_g est donc $N''_{g,0}$ tout entier, d'où $\gamma_g(N''_g) = N''_g$ puisque γ_g est injectif. De plus, l'application $(n', n'') \to n'n''$ de $N'_g \times N''_g$ dans N est alors une représentation rationnelle *injective*, dont l'image a donc la même dimension dim N, et est par suite identique à N si N est connexe. Comme la composante neutre de $N'_g \times N''_g$ est transformée en la composante neutre de N, on en conclut aussi que N'_g et N''_g sont connexes.

Il reste donc seulement à prouver, sous les conditions indiquées, que l'on a $N'_g \cap N''_g = \{e\}$. Soit donc $n \in N$ tel que $\gamma_g n \in N'_g$, et montrons que $\gamma_g n = e$. Soit M le sous-groupe fermé de N engendré par N'_g et n ; on a alors $\sigma_g n \in N'_g n$ et γ_g induit (par définition de N'_g) l'identité sur N'_g. Ainsi g normalise M, et σ_g induit l'identité sur $M' = N'_g$ et sur M/M'. Notre assertion résulte alors du :

Lemme 4. – *Soient G un groupe algébrique affine, M un sous-groupe fermé de G, M' un sous-groupe fermé invariant de M, g un élément de G appartenant au normalisateur de M, et tel que l'automorphisme $\sigma_g : m \to gmg^{-1}$ de M induise l'identité sur M', et sur M/M'. Si de plus g est semi-simple (resp. unipotent) et si $M' = M'_u$ (resp. $M' = M'_s$) alors g centralise M.*

L'ensemble des $x \in G$ normalisant M et tels que $\sigma_x : m \to xmx^{-1}$ soit un automorphisme de M induisant l'identité sur M' et sur M/M' est un sous-groupe fermé de G contenant g ; il contient donc le plus petit sous-groupe fermé H de G contenant g. Comme les g^n ($n \in \mathbf{Z}$) sont aussi semi-simples (resp. unipotents) et que H est commutatif, il s'ensuit (théorème 4) que $H = H_s$ (resp. $H = H_u$). Soit $m \in M$; nous voulons montrer que tout $x \in H$ centralise m, *i.e.* que $f_m(x) = m^{-1}xmx^{-1}$ est l'identité. Or par construction de H on a $f_m(x) \in M'$, et on vérifie aussitôt que $f_m(xy) = f_m(x)\, f_m(y)$. Donc f_m est un homomorphisme rationnel de H dans M'. Il transforme donc les éléments semi-simples en éléments semi-simples, les éléments unipotents en éléments unipotents (corollaire du théorème 3), et il est donc réduit à la représentation triviale en vertu des hypothèses faites. C.Q.F.D.

Corollaire. – *Soient G un groupe algébrique affine, M un sous-groupe fermé résoluble et connexe de G, g un élément de G normalisant M ; on suppose ou bien que g est semi-simple et $M = M_u$ ou bien que g est unipotent et $M = M_s$. Alors l'ensemble des éléments de M qui commutent à g est connexe.*

Cela résulte de la proposition 5 et du lemme 4 par récurrence sur la dimension de M.

Proposition 6. – *Soient G un groupe algébrique affine, M un sous-groupe fermé de G, M' un sous-groupe fermé invariant résoluble de M, g un élément de G qui normalise M et M', σ_g l'automorphisme de M/M' défini par $m \to gmg^{-1}$. On suppose ou bien que g est semi-simple et $M' = M'_u$ ou bien que g est unipotent et $M' = M'_s$. Alors tout élément de M/M' invariant par σ_g est image d'un élément de M qui commute à g. En particulier*[9]*, si* $\mathrm{int}(g)$ *induit l'identité sur M' et sur M/M', il induit l'identité sur M.*

Une récurrence immédiate sur la longueur de la suite des dérivés successifs de M' nous ramène au cas où M' est commutatif. Soit H le groupe fermé engendré par g. Dans le cas où g est unipotent et la caractéristique nulle, H est connexe ; comme M' est diagonalisable (étant commutatif et composé d'éléments semi-simples), H opère trivialement sur M'. En vertu du lemme 4, il opère donc trivialement sur l'image réciproque de l'ensemble des éléments de M/M' invariants par $\sigma(g)$, ce qui prouve notre assertion dans ce cas.

Ce cas étant écarté, H est l'adhérence d'une suite croissante (U_n) de groupes finis ; si g est semi-simple, donc H diagonalisable, cela résulte de la proposition 2, et si g est unipotent, cela résulte du fait que H est lui-même

[9] On note $\mathrm{int}(g)$ l'automorphisme intérieur de G défini par g.

d'ordre fini égal à une puissance de p. Soit M_n l'ensemble des éléments de M invariants par U_n ; les M_n forment une suite décroissante de sous-groupes fermés de M dont l'intersection est l'ensemble des éléments de M invariants par H. Donc il existe un n tel que M_n soit l'ensemble des éléments de M qui commutent à g. Cela nous ramène à prouver ceci : si H est un sous-groupe fini de G normalisant M et M' et si ou bien $H = H_s$, $M' = M'_u$ ou bien $H = H_u$, $M' = M'_s$, alors tout élément de M/M' invariant par H provient d'un élément de M invariant par H. Soit $m \in M$ tel que $hmh^{-1} = mf(h)$ pour $h \in H$, avec $f(h) \in M'$. Posant $\tau(h) \cdot m' = hm'h^{-1}$, on a $f(hh') = f(h) \cdot (\tau(h) \cdot f(h'))$ si $h, h' \in H$ et $f(e) = e$, *i.e.* f est un 1-cocycle normalisé de H à valeurs dans le groupe abélien M' où H opère. On cherche un $m' \in M'$ tel que mm' soit invariant par H, *i.e.* tel que $f(h) = m'(\tau(h) \cdot m')^{-1}$ pour tout h ; *i.e.* on veut prouver que le cocycle f est homologue à 0. Si $H = H_s$, tous les éléments de M' sont unipotents et ont par suite pour ordres des puissances de p, tandis que H est d'ordre premier à p ; on a donc $H^1(M, M') = 0$ dans ce cas. Si $H = H_u$, $M' = M'_s$, H est d'ordre une puissance de p, et on se ramène facilement au cas cyclique (qui suffit d'ailleurs pour établir la proposition 6). Il faut alors démontrer que tout élément de M' de "norme" 1 peut s'écrire $m'(\tau(h) \cdot m')^{-1}$, où h est un générateur de H. Comme M' est diagonalisable et comme l'ensemble N des éléments qui sont de norme 1, ainsi que l'ensemble N' des éléments de la forme $m'(\tau(h) \cdot m')^{-1}$, sont des sous-groupes fermés, on est ramené à prouver que l'ensemble N_n des éléments de N d'ordre divisant un entier donné n est contenu dans N', ce qui nous ramène au cas où M' est lui-même fini. Alors on a encore $H^1(M, M') = 0$ car l'ordre de H est premier à celui de M' ; ceci achève la démonstration.

Dans le même ordre d'idées, signalons la :

Proposition 7. – *Soient T un tore, H un sous-groupe (non nécessairement fermé) de T, u un automorphisme d'ordre fini m de T, induisant l'identité sur H et T/H. Alors u est l'identité.*

En vertu de la proposition 2, il suffit de prouver que, pour tout entier n premier à m, u induit l'identité sur le sous-groupe T_n de T formé des éléments t tels que $t^n = e$. Or si $t \in T_n$, on a $u(t) = ts$, où $s \in T_n \cap H$, d'où $u^i(t) = ts^i$ pour tout i, d'où pour $i = m$: on a $s^m = e$ d'où enfin $s = e$ puisque s est d'ordre premier à m.

5. Compléments de géométrie algébrique[1]

5.1 Discriminant et séparabilité

On note k un corps (commutatif).

Lemme 1. – *Soit T une forme bilinéaire symétrique non dégénérée sur un espace vectoriel V de dimension finie n sur le corps k. Soient x_i $(1 \leq i \leq n)$ des éléments de V ; pour qu'ils forment une base, il faut et il suffit que l'on ait* $\det(T(x_i, x_j)) \neq 0$. *Plus généralement, soient $\mathfrak{o}$ un sous-anneau de k dont k soit le corps des fractions, M un sous-$\mathfrak{o}$-module de V engendrant l'espace vectoriel V, tel que $T(x, y) \in \mathfrak{o}$ pour $x, y \in M$. Pour que M soit un $\mathfrak{o}$-module libre et que T définisse un isomorphisme de M sur le module dual M', il faut et il suffit qu'il existe n éléments x_i de M tels que* $\det(T(x_i, x_j))$ *soit un élément inversible de $\mathfrak{o}$. Alors ces sytèmes (x_i) sont identiques aux bases de M sur $\mathfrak{o}$, et M est identique à l'ensemble des $x \in V$ tels que $T(x, y) \in \mathfrak{o}$ pour tout $y \in M$.*

Evidemment la première assertion est un cas particulier des suivantes. Soit (x_i) une base de M sur $\mathfrak{o}$, et supposons que T définisse un isomorphisme de M sur le module dual M'. Comme la matrice de l'homomorphisme $M \to M'$ par rapport à la base (x_i) de M et à la base duale de M' est $(T(x_i, x_j))$, il s'ensuit que le déterminant de cette matrice est inversible dans $\mathfrak{o}$. D'ailleurs soit (x'_i) un autre système de n éléments de M, $x'_i = \sum_j c_{ij}\, x_j$; alors on vérifie aussitôt que

$$\det(T(x'_i, x'_j)) = (\det(c_{ij}))^2 \det(T(x_i, x_j)),$$

d'où résulte que le premier membre est inversible dans $\mathfrak{o}$ si et seulement si $\det(c_{ij})$ l'est, *i.e.* si (x'_i) est une base de M sur $\mathfrak{o}$. Supposons réciproquement que l'on ait n éléments x_i de M tels que $\det(T(x_i, x_j))$ soit inversible dans $\mathfrak{o}$; d'après ce qui précède les x_i forment donc une base de V sur k ; montrons qu'ils forment même une base de M sur $\mathfrak{o}$. Comme tout $x \in V$ s'écrit $x = \sum_i c_i\, x_i$, il suffit de montrer que si $x \in M$, les c_i sont dans $\mathfrak{o}$, et nous prouverons même que si x est tel que $T(x, x_i) \in \mathfrak{o}$ pour tout i, alors les c_i sont dans $\mathfrak{o}$ (ce qui prouvera aussi la dernière assertion du lemme). En effet, on aura

$$T(x, x_j) = \sum_i c_i\, T(x_i, x_j) \qquad (j = 1, \ldots, n).$$

[1] Exposé de A. Grothendieck, le 3.12.1956

C'est là un système linéaire de n équations à n inconnues c_i, à seconds membres dans $\mathfrak{o}$ et dont le déterminant est inversible dans $\mathfrak{o}$; ses solutions sont donc dans $\mathfrak{o}$. Enfin, la matrice de l'homomorphisme $M \to M'$ défini par T, par rapport à la base (x_i) de M et à la base duale de M', est $(T(x_i, x_j))$ donc inversible ; on a donc bien un isomorphisme de M sur M'. C.Q.F.D.

Soit R une algèbre sur le corps k. On dit que R est *séparable* si, quelle que soit l'extension K de k, l'algèbre $R \otimes K$ obtenue par extension des scalaires n'a pas de radical. Dans le cas où R est une extension de k, on retrouve la notion usuelle de séparabilité (**SCC**, exposé 13, théorème 3). D'ailleurs, on montre que pour vérifier que R est séparable sur k, il suffit de vérifier la condition de la définition pour *une* extension *algébriquement close* (ou même seulement parfaite) K de k ; nous ne nous servirons de cette notion que si R est commutative et de dimension finie, auquel cas la remarque précédente se démontre de façon quasi-triviale (sans radical signifiant alors : sans élément nilpotent). En ce cas, R séparable signifie que R est composé direct d'un nombre fini d'extensions *séparables* de k.

Supposons l'algèbre R commutative et de dimension finie. Soit $x \in R$; la trace de l'endomorphisme $y \to xy$ de l'espace vectoriel R est notée $\mathrm{Tr}_{R/k}x$. (Quand R est une extension *séparable* de k, cette notion coïncide avec la notion usuelle de trace). Alors $\mathrm{Tr}_{R/k}xy$ est une forme bilinéaire symétrique sur R. Si on a n éléments x_i de R, on pose

$$D_{R/k}(x_1, \ldots, x_n) = \det\left(\mathrm{Tr}_{R/k}(x_i x_j)\right).$$

Lemme 2. – *Soit R une algèbre commutative de dimension finie n sur k. Pour que R soit séparable, il faut et il suffit que la forme bilinéaire* $\mathrm{Tr}_{R/k}xy$ *sur $R \times R$ soit non dégénérée,* i.e. *que pour une base $(x_1, \ldots, x_n)$ de R, on ait $D_{R/k}(x_1, \ldots, x_n) \neq 0$.*

On est ramené immédiatement au cas où k est algébriquement clos. Si R est séparable, donc semi-simple, c'est un composé direct de corps isomorphes à k, d'où aussitôt le fait que $\mathrm{Tr}_{R/k}xy = \sum_i x_i\, y_i$ est non dégénérée. Si R n'est pas séparable, donc pas semi-simple, il a un élément nilpotent non nul a ; alors pour tout $y \in R$, ay est nilpotent d'où aussitôt $\mathrm{Tr}_{R/k}ay = 0$, et la forme $\mathrm{Tr}_{R/k}xy$ est dégénérée. C.Q.F.D.

Soit R une algèbre commutative sur k, n'ayant qu'un nombre fini d'idéaux premiers $\mathfrak{m}_i$, supposés tous maximaux. Alors le radical $\mathfrak{r}(R) = \cap_i \mathfrak{m}_i$ coïncide avec l'ensemble des éléments nilpotents de R (qui est en effet l'intersection des idéaux premiers de R), et $R/\mathfrak{r}(R)$ s'identifie au composé direct des corps $k_i = R/\mathfrak{m}_i$.

Supposons maintenant R algébrique sur k (*i.e.* tout élément de R engendre une algèbre de dimension finie) ; alors les k_i sont algébriques sur k. Rappelons qu'on appelle *degré séparable* de k_i sur k, et qu'on note $[k_i : k]_s$,

le degré (fini ou infini) de la plus grande sous-extension séparable de k_i/k ; ce nombre est égal à celui des k-isomorphismes distincts de k_i dans une fermeture algébrique de k et aussi (en vertu du théorème de l'élément primitif) à la borne supérieure des degrés sur k des éléments de k_i qui sont séparables sur k. Nous appellerons degré séparable de R, et nous noterons $[R : k]_s$, le nombre $\sum_i [k_i : k]_s$.

Lemme 3. – *Avec les notations précédentes, supposons de plus que k soit un corps* infini. *Soit d un entier fini $\leq [R : k]_s$; alors il existe $x \in R$ dont le polynôme minimal est de degré $\geq d$, et même $> d$ si R n'est pas séparable. Si R est séparable et de dimension finie, il existe un élément $x \in R$ tel que $R = k[x]$.*

Soit $\overline{R} = R/\mathfrak{r}(R) = \prod_i k_i$; soit, pour chaque i, $\overline{x}_i$ un élément de k_i ; soient f_i le polynôme minimal de $\overline{x}_i$ et d_i son degré. On va montrer qu'il existe *un élément de R dont le polynôme minimal est de degré $\geq \sum_i d_i$*. Soit e_i l'élément unité de k_i ; si $a \in k$, le polynôme minimal de $\overline{x}_i + ae_i$ est $f_i(X-a)$; comme k est infini, on peut toujours choisir a tel que $f_i(X-a)$ soit premier à un polynôme arbitraire donné à l'avance. Remplaçant de proche en proche les $\overline{x}_i$ par des éléments de la forme $\overline{x}_i + a_i\, e_i$, on voit qu'il existe des éléments $\overline{x}'_i \in k_i$ dont les polynômes minimaux f'_i sont de degré d_i et sont premiers entre eux deux à deux ; le polynôme minimal de $\overline{x} = \sum_i \overline{x}'_i$ est alors évidemment $\prod_i f'_i$, de degré $\sum_i d_i$; si x est un représentant dans R de la classe $\overline{x} \in \overline{R}$, le polynôme minimal de x est évidemment de degré $\geq \sum_i d_i$, ce qui démontre notre assertion.

Il en résulte immédiatement que si $\sum_i [k_i : k]_s = \infty$, il y a des éléments de R dont les polynômes minimaux ont des degrés arbitrairement élevés et qu'en tout état de cause il existe un élément de R dont le polynôme minimal est de degré $\geq d$. Si R est séparable de dimension finie, $\sum_i [k_i : k]_s$ est égal à la dimension n de R ; si x est un élément dont le polynôme minimal est de degré n, on a $R = k[x]$. Supposons maintenant que $\sum_i [k_i : k]_s$ soit fini et que R ne soit pas séparable. Supposons d'abord que, pour un certain i, k_i ne soit pas séparable sur k. Il existe alors un élément x_i de k_i de degré $\geq [k_i : k]_s$ par rapport à k. Soient en effet $\sigma_1, \ldots, \sigma_m$ les k-isomorphismes distincts de k_i dans une fermeture algébrique $\overline{k}$ de k ($m = [k_i : k]_s$), et soit y un élément de k_i séparable sur k tel que les $\sigma_j(y)$ soient tous distincts. Soit x un élément de k_i non séparable sur k ; comme k est infini, il existe un $a \in k$ tel que les $\sigma_j(x + ay)$ soient tous distincts ; le corps $k(x + ay)$ est alors une extension non séparable de k qui admet $m = [k_i : k]_s$ k-isomorphismes distincts dans $\overline{k}$ et qui est par suite de degré $> m$, ce qui démontre notre assertion. Pour tout $j \neq i$, il existe un élément de k_j de degré $[k_j : k]_s$ par rapport à k ; il existe donc un élément de R dont le polynôme minimal est de degré $> \sum_i [k_i : k]_s$. Supposons maintenant que les k_i soient tous séparables sur k mais que $\mathfrak{r}(R) \neq \{0\}$. Soit x un élément de R tel que le polynôme minimal $\overline{f}$ de la classe $\overline{x}$ de x modulo $\mathfrak{r}(R)$ soit de degré $\sum_i [k_i : k]_s$. Ce polynôme est évidemment sans

racine multiple. Si $a \in \mathfrak{r}(R)$, le polynôme minimal de $x + a$ est divisible par $\overline{f}$; il suffira de montrer qu'on peut choisir a tel que $\overline{f}(x + a) \neq 0$; si $\overline{f}(x) = 0$, $\overline{f}(x + a)$ est de la forme ca, où c appartient à la classe $\overline{f}'(\overline{x})$ modulo $\mathfrak{r}(R)$; comme $\overline{f}'$ est premier à $\overline{f}$, $\overline{f}'(x)$ est inversible dans $R/\mathfrak{r}(R)$, donc c inversible dans R, d'où $ca \neq 0$ si $a \neq 0$, ce qui démontre le lemme 3.

5.2 Ramification et normalisation

Théorème 1. – *Soient* $\mathfrak{o}$ *un anneau local intègre et intégralement clos,* L *son corps des fractions,* L' *une extension algébrique de degré fini* n *de* L, $\mathfrak{o}'$ *un sous-anneau de* L', *entier sur* $\mathfrak{o}$, *dont le corps des fractions soit* L', $\mathfrak{m}$ *l'idéal maximal de* $\mathfrak{o}$, $\mathfrak{m}'_i$ *les idéaux premiers de* $\mathfrak{o}'$ *prolongeant* $\mathfrak{m}$ (ils sont en nombre fini et maximaux et l'on a $\mathfrak{m}'_i \cap \mathfrak{o} = \mathfrak{m}$ d'après **SCC**, exposé 1), $\mathfrak{m}' = \mathfrak{o}'\mathfrak{m}$, $R = \mathfrak{o}'/\mathfrak{m}'$, $k_i = \mathfrak{o}'/\mathfrak{m}'_i$, $k = \mathfrak{o}/\mathfrak{m}$. *Alors* R *est une algèbre algébrique sur* k, *et on a* $[R : k]_s = \sum_i [k_i : k]_s \leq n$ *; si* $\mathfrak{o}'$ *est un module de type fini sur* $\mathfrak{o}$, *on a* $n \leq [R : k]$. *De plus les conditions suivantes* a) *et* b) *sont équivalentes, entraînent* c) *et sont même équivalentes à* c) *si* $\mathfrak{o}'$ *est un module de type fini sur* $\mathfrak{o}$ *:*

a) $[R : k]_s = n$, i.e. $\sum_i [k_i : k]_s = n$;

b) *il existe* n *éléments* x_i *de* $\mathfrak{o}'$ *tels que* $D_{L'/L}(x_1, \ldots, x_n)$ *soit un élément inversible de* $\mathfrak{o}$ *;*

c) R *est une* k*-algèbre séparable.*

Corollaire 1. – *Si* a) *et* b) *sont satisfaites,* L' *est une extension séparable de* L, $\mathfrak{o}'$ *est un* $\mathfrak{o}$*-module libre de type fini et est la fermeture intégrale de* $\mathfrak{o}$ *dans* L'.

Cela résulte des lemmes 1 et 2, tenant compte de ce que la trace par rapport à L de tout élément de L' entier sur $\mathfrak{o}$ est dans $\mathfrak{o}$.

Remarque. – La condition de finitude sur $\mathfrak{o}'$ est automatiquement satisfaite si L' est séparable sur L et $\mathfrak{o}$ nœthérien ou si $\mathfrak{o}$ est une localité de L (**SCC**, exposé 4, théorème 1). La condition c) peut se formuler comme suit : on a $\mathfrak{m}\mathfrak{o}' = \cap_i \mathfrak{m}'_i$ et les k_i sont séparables sur k. La première de ces conditions signifie aussi que $\mathfrak{r}(R) = \{0\}$, et implique manifestement que $\mathfrak{m}\mathfrak{o}'_{\mathfrak{m}'_i} = \mathfrak{m}'_i\,\mathfrak{o}'_{\mathfrak{m}'_i}$ pour tout i. La réciproque est vraie, d'où, si k est parfait, la forme classique de la condition de non ramification.

Démonstration. – *Nous ferons la démonstration en supposant* k *infini* (suffisant pour ce dont nous aurons besoin), mais on peut se débarrasser de cette hypothèse. Comme le polynôme minimal de tout élément de $\mathfrak{o}'$ sur L est à coefficients dans $\mathfrak{o}$ ($\mathfrak{o}'$ étant entier sur $\mathfrak{o}$), il s'ensuit aussitôt que tout élément de R est algébrique sur k de degré $\leq n$, donc que R satisfait à toutes les conditions envisagées pour le lemme 3. Si l'on avait $[R : k]_s > n$, il existerait

donc un élément $\overline{x}$ de R de degré sur k strictement supérieur à n, il en serait *a fortiori* de même du degré du polynôme minimal d'un représentant dans $\mathfrak{o}'$ de cet élément (les coefficients de ce polynôme étant dans $\mathfrak{o}$), ce qui est absurde. Donc $[R : k]_s \leq n$.

Prouvons a) $\Rightarrow$ c) : en effet si R n'était pas séparable, il résulterait encore du lemme 3 qu'il existerait un élément de R dont le degré sur k soit $> [R : k]_s$, ce qui est absurde puisque $[R : k]_s = n$.

Prouvons a) $\Rightarrow$ b) : en effet, en vertu du lemme 3, il existe un générateur $\overline{x}$ de R (qui est séparable de dimension n) ; on aura donc $D_{R/k}(1, \overline{x}, \ldots, \overline{x}^{n-1}) \neq 0$ (lemme 2) ; si $x \in \mathfrak{o}'$ est un représentant de $\overline{x}$, son polynôme minimal réduit mod. $\mathfrak{m}$ est multiple de celui de $\overline{x}$ sur k, donc identique à ce dernier pour des raisons de degré. Or on constate facilement que le discriminant, pour une base d'une extension monogène formée des puissances $1, \xi, \ldots, \xi^{n-1}$ d'un générateur, s'exprime en polynôme universel, à coefficients indépendants de la caractéristique, en les coefficients de l'équation minimale de ce générateur ; d'où résulte ici que $D_{R/k}(1, \overline{x}, \ldots, \overline{x}^{n-1})$ s'obtient en réduisant mod $\mathfrak{m}$ l'élément $D_{L'/L}(1, x, \ldots, x^{n-1})$, qui est donc un élément *inversible* de $\mathfrak{o}$.

Prouvons b) $\Rightarrow$ a) : soient n éléments x_i de $\mathfrak{o}'$ tels que $D_{L'/L}(x_1, \ldots, x_n)$ soit un élément inversible de $\mathfrak{o}$; il en résulte d'abord que L' est séparable sur L (lemme 2), et l'on peut alors appliquer le lemme 1, (car $\mathrm{Tr}_{L'/L} xy \in \mathfrak{o}$ si $x, y \in \mathfrak{o}'$) qui nous apprend que $\mathfrak{o}'$ admet (x_i) comme base sur $\mathfrak{o}$. Les $\overline{x}_i$ forment donc une base de R sur k, et on constate aussitôt que leur discriminant s'obtient par réduction mod $\mathfrak{m}$ de celui des x_i ; il est donc non nul, et par suite R est séparable (lemme 2). Donc $[R : k]_s = [R : k] = n$, d'où a).

Prouvons enfin que l'on a $n \leq [R : k]$ si $\mathfrak{o}'$ est un module de type fini sur $\mathfrak{o}$; il en résultera aussi, sous ces conditions, que $[R : k] = [R : k]_s$ implique $n = [R : k]_s$, où c) $\Rightarrow$ a). Soit $(\overline{x}_i)$ une base de R sur k ; il suffit de prouver que les $x_i \in \mathfrak{o}'$ engendrent le $\mathfrak{o}$-module $\mathfrak{o}'$ (et *a fortiori* engendrent le L-espace vectoriel L'). Soit M_1 le sous-$\mathfrak{o}$-module du $\mathfrak{o}$-module $\mathfrak{o}' = M$, engendré par les x_i ; on a $M_1 + \mathfrak{m}M = M$, *i.e.* en posant $Q = M/M_1$ on a $\mathfrak{m}Q = Q$; or Q est un $\mathfrak{o}$-module de type fini, d'où $Q = 0$ (**SCC**, exposé 1, appendice), *i.e.* $M_1 = M$. C.Q.F.D.

Définition 1. – *Soient $\mathfrak{o}$ un anneau local intègre et intégralement clos, L son corps des fractions, L' une extension algébrique de degré fini de L, $\mathfrak{o}'$ la fermeture intégrale de $\mathfrak{o}$ dans L'. On dit que $\mathfrak{o}$ est* non ramifié *dans L' s'il satisfait aux conditions équivalentes* a) *et* b) *du théorème* 1.

Corollaire 2. – *Soient A un anneau intègre et intégralement clos, L son corps des fractions, L' une extension algébrique de degré fini n de L, A' la fermeture intégrale de A dans L', $\mathfrak{d}_{A'/A}$ l'idéal de A engendré par les $D_{L'/L}(x_1, \ldots, x_n)$ pour tous les systèmes de n éléments x_i de A'. Soit $\mathfrak{p}$ un idéal premier de A ; pour que $A_{\mathfrak{p}}$ soit ramifié dans L', il faut et il suffit que $\mathfrak{p}$ contienne $\mathfrak{d}_{A'/A}$.*

En effet, $A_{\mathfrak{p}}$ est ramifié dans L' si et seulement si, pour n éléments quelconques de la fermeture intégrale $(A_{\mathfrak{p}})'$ de $A_{\mathfrak{p}}$, qu'on peut supposer écrits sous la forme x_i/a ($x_i \in A'$, $a \in A - \mathfrak{p}$) d'après **SCC**, exposé 1, proposition 5, l'élément $D_{L'/L}(x_1/a, \ldots, x_n/a)$ est dans l'idéal maximal de $A_{\mathfrak{p}}$. Ceci signifie (en multipliant par a^{2n}, qui est inversible dans $A_{\mathfrak{p}}$) que $D_{L'/L}(x_1, \ldots, x_n)$ appartient à $\mathfrak{p}$.

Corollaire 3. – *Soient V une variété*[2] *normale sur le corps algébriquement clos K, $L = K(V)$ son corps des fonctions rationnelles, L' une extension algébrique de degré fini n de L, V' la variété normalisée de V dans le corps L', f l'application canonique de V' dans V. Pour que l'anneau local $\mathfrak{o}_x$ d'un point x de V soit non ramifié dans L', il faut et il suffit que $f^{-1}(x)$ contienne exactement n éléments. Si L' est extension* séparable *de L, l'ensemble des éléments de V qui ont cette propriété forme un ouvert dense.*

Précisons d'abord qu'on a défini dans **SCC**, exposé 7, théorème 1, la notion de schéma dérivé S' dans L' d'un schéma S de corps des fractions L, et qu'on appelle en conséquence *variété normalisée* de V dans L' la variété définie par le schéma dérivé dans L' du schéma de V. Le morphisme canonique $S' \to S$ (*loc. cit.*) définit alors le morphisme $V' \to V$ de l'énoncé (*cf.* n° 2.5). Si $x \in V$, les points de $f^{-1}(x)$ correspondent donc aux idéaux maximaux de la fermeture normale $(\mathfrak{o}_x)'$ de $\mathfrak{o}_x$ dans L' (*loc. cit.*, théorème 2). D'ailleurs $\mathfrak{o}_x$ est normal, donc le théorème 1 s'applique, et comme le corps résiduel k de $\mathfrak{o}_x$ est K, donc algébriquement clos, les k_i sont identiques à k, de sorte que la condition $[R : k]_s = n$ signifie précisément qu'il y a n idéaux maximaux dans $(\mathfrak{o}_x)'$; ceci prouve la première assertion du corollaire.

Pour la seconde, on peut se borner au cas où V est affine, donc défini par une algèbre affine A, de sorte que V' est définie par l'algèbre affine A' fermeture normale de A dans L' (*loc. cit.*). Comme L' est séparable sur L, il existe n éléments x_i de L tels que $D_{L'/L}(x_1, \ldots, x_n) \neq 0$ (lemme 2), donc on a, avec les notations du corollaire 2, $\mathfrak{d}_{A'/A} \neq 0$. L'ensemble des $x \in V$ tels que $\mathfrak{o}_x$ se ramifie dans L' s'identifie à l'ensemble des idéaux maximaux de A qui contiennent l'idéal non nul $\mathfrak{d}_{A'/A}$; c'est donc un fermé de V, distinct de V. C.Q.F.D.

Corollaire 4. – *Sous les hypothèses du corollaire* 3, *soit $n = [L' : L]_s$. Alors pour tout $x \in V$, $f^{-1}(x)$ a au plus n éléments, et l'ensemble des $x \in V$ tels que $f^{-1}(x)$ ait n éléments est un ouvert dense.*

Soit L'_s le sous-corps de L' formé des éléments séparables sur L ; alors L'_s est séparable de degré n sur L, et L' purement inséparable sur L'_s. Soit V'_s la normalisée de V dans L'_s ; alors (*loc. cit.*) f se factorise en produit des applications canoniques

$$V' \xrightarrow{f_i} V'_s \longrightarrow V$$

[2] C'est-à-dire un ensemble (K, K)-algébrique irréductible.

(V' s'identifie à la normalisée de V'_s dans L'). Compte tenu du corollaire 3, il suffit de prouver que f_i est une bijection de V' sur V'_s. Pour ceci, on est encore ramené au cas où V est la variété affine définie par une algèbre affine A. Si A'_s est sa fermeture normale dans L'_s, nous voulons donc démontrer que tout idéal premier de A'_s est trace d'un unique idéal premier de A'. Or L' étant une extension normale de L'_s dont le groupe de Galois est réduit à l'unité, il suffit d'appliquer le lemme 3 de **SCC**, exposé 1.

5.3 Forme géométrique du "Main theorem" de Zariski

Le théorème 2 de **SCC**, exposé 12, est essentiellement équivalent (dans le cas de schémas correspondant à des variétés sur K) au cas particulier suivant, de forme plus "globale" :

Théorème 2. – ("Main theorem") *Soit f une application régulière* birationnelle *d'une variété X dans une variété* normale Y, *telle que pour tout $y \in Y$, $f^{-1}(y)$ soit* fini. *Alors f est un isomorphisme de X sur une partie ouverte de Y.*

La référence ci-dessus dit en effet que l'application rationnelle f^{-1} est définie en tous les points de $f(X)$, donc dans un ouvert U contenant $f(X)$. Soit g la restriction de f^{-1} à U ; c'est une application régulière de U dans X, et on a évidemment $fg =$ identité et $gf =$ identité *partout* (puisque ces identités sont vraies dans des ouverts denses, et que gf et fg sont continues), d'où résulte que f est un isomorphisme de X sur U.

Corollaire 1. – *Soit f une application régulière d'une variété X dans une variété* normale Y, *telle que $f(X)$ soit dense dans Y. Les conditions suivantes sont équivalentes :*

a) *X est normale, et $f^{-1}(y)$ est fini pour tout $y \in Y$.*

b) *Le morphisme f est composé d'un isomorphisme de X sur une partie ouverte d'une normalisée Y' de Y dans une extension finie de $L = K(Y)$, et de l'application canonique $Y' \to Y$.*

Evidemment b) $\Rightarrow$ a) ; réciproquement supposons a) vérifiée. Soit $L' = K(X)$ le corps des fonctions rationnelles sur X ; grâce à f on peut considérer L' comme une extension de L. Comme les $f^{-1}(y)$ sont de dimension 0, il s'ensuit que le degré de transcendance de L' sur L est 0 (**SCC**, exposé 8, théorème 2) donc que L' est une extension finie de L (puisque L' est une extension algébrique ayant un nombre fini de générateurs). Soit Y' la normalisée de Y dans L'. Comme X est normale, f se factorise en $X \to Y' \to Y$ (**SCC**, exposé 7, théorème 1) ; or l'application $X \to Y'$ est régulière, birationnelle, et les images réciproques des points de Y' sont finies, donc, Y' étant normale, on peut appliquer le théorème 2 : $X \to Y'$ est un isomorphisme de X sur une partie ouverte de Y'. C.Q.F.D.

Corollaire 2. – *Soit f comme dans le corollaire précédent, et satisfaisant à la condition* a). *Soit n le degré séparable du corps des fonctions rationnelles de X sur celui de Y. Alors pour tout $y \in Y$, il existe au plus n éléments dans $f^{-1}(y)$, et l'ensemble des points de Y tels que $f^{-1}(y)$ ait n points est un ouvert dense.*

En vertu du corollaire 1, on peut supposer que X est un ouvert d'une normalisée Y' de Y. La première assertion résulte alors du corollaire 4 du théorème 1 appliqué à $f : Y' \to Y$. Soit Z le fermé complémentaire de X dans Y' ; son image $f(Z)$ est une partie fermée de Y car Y' est "complet au-dessus de Y" (**SCC**, exposé 6, paragraphe 7, et exposé 7, théorème 1) donc f transforme fermés en fermés (**SCC**, exposé 8, théorème 1 *bis*). Soit d'autre part F l'ensemble des points $y \in Y$ dont l'image réciproque dans Y' contient strictement moins de n points ; c'est une partie fermée de Y distincte de Y (théorème 1, corollaire 4). Alors l'ensemble des $y \in Y$ dont l'image réciproque dans X contient strictement moins de n points est égal à $F \cup f(Z)$; c'est donc un fermé distinct de Y. C.Q.F.D.

Corollaire 3. – *Soit f une application régulière d'une variété normale X dans une variété normale Y, telle que $f(X)$ soit dense dans Y, et que pour tout $y \in Y$, $f^{-1}(y)$ ait un nombre fini de points, indépendant de y. Alors f s'identifie à l'application canonique $Y' \to Y$ de la variété normalisée de Y dans l'extension $K(X)$ de $K(Y)$, et par suite (***SCC***, exposé 7, théorème 1) si Y est complète (resp.* projective*), X est complète (resp.* projective*).*

(N.B. – On dit qu'une variété est *complète* resp. *projective*, si le schéma associé l'est au sens de **SCC**, exposé 5.)

Il suffit d'appliquer le corollaire 1 ; X s'identifie à un ouvert de Y' qui est nécessairement tout Y', en vertu du théorème 1, corollaire 4, puisque autrement il y aurait des points de Y dont l'image réciproque n'aurait pas le "bon" nombre d'éléments.

Remarque. – En passant à la normalisée de X, on voit facilement que la conclusion "X complète si Y complète" du corollaire 3 est valable même si X n'est pas supposée normale. Il est cependant essentiel que Y le soit, même en dimension 1, comme on voit en prenant pour Y une courbe complète ayant un seul point double ordinaire, pour X la normalisée de Y privée d'un des deux points au-dessus du point double.

5.4 Variétés projectives

Nous venons de convenir qu'une variété est dite *projective* (resp. *complète*) si le schéma associé l'est (**SCC**, exposé 5). Une variété projective est complète (*loc. cit.*, proposition 7), mais la réciproque est fausse[3].

[3] D'après un contre-exemple connu de Hironaka.

L'espace projectif $P(V)$. Soit V un espace vectoriel de dimension finie n sur K, $L = K(V)$ le corps des fonctions rationnelles sur V. Le dual V' de V est un sous-espace vectoriel de L ; soit $S(V)$ le schéma projectif qu'il définit (*loc. cit.*), *i.e.* le schéma défini par les algèbres affines $K[V'\,x'^{-1}]$, où $x' \in V'$ $x' \neq 0$. Soit $S_{x'}$ le schéma affine défini par $K[V'\,x'^{-1}]$, $P_{x'}$ la variété affine correspondante, ensemble des homomorphismes de l'algèbre affine envisagée à valeurs dans K. Prenant une base $(X_1, \ldots, X_n)$ dans V' avec $X_1 = x'$, (les X_i sont donc des générateurs algébriquement indépendants de L), $V'\,x'^{-1}$ est l'espace vectoriel ayant pour base 1, $X_2/X_1, \ldots, X_n/X_1$, donc l'algèbre affine qu'il engendre est l'algèbre de polynômes engendrée par les éléments algébriquement indépendants $X_2/X_1, \ldots, X_n/X_1$. Par suite, un élément de $P_{x'}$ s'identifie à un système de $n-1$ éléments de K (valeurs du caractère associé sur les X_i/X_1, $2 \leq i \leq n$) ou plus intrinsèquement, à une forme linéaire sur $V'\,x'^{-1}$ prenant la valeur 1 sur $1 \in V'\,x'^{-1}$. Soit alors $x \in V$ tel que $\langle x, x' \rangle \neq 0$, soit $\overline{x}$ le point de $P_{x'}$ associé à la forme linéaire $X \to \langle x, X \rangle / \langle x, x' \rangle$ sur $V'\,x'^{-1}$; si $H_{x'}$ désigne l'hyperplan de V noyau de x', alors $x \to \overline{x}$ est manifestement une application de $V - H_{x'}$ *sur* $P_{x'}$, et deux éléments de $V - H_{x'}$ ont la même image dans $P_{x'}$ si et seulement s'ils sont proportionnels. Soit L_0 le corps des fonctions rationnelles sur la variété $P(V)$ définie par $S(V)$ *i.e.* le corps engendré par $V'\,x'^{-1}$, (ou encore le sous-corps de $K(X_1, \ldots, X_n)$ formé des fractions rationnelles *homogènes de degré* 0). Par construction, pour tout $x \in V - H_{x'}$, $\overline{x}$ est caractérisé par la condition que pour tout $f = X/x' \subset V'\,x'^{-1} \subset L_0$, $f(\overline{x})$ soit défini et égal à $X(x)/x'(x)$. Il en résulte que si y' est un autre point non nul de V', et si $x \in V - H_{x'} - H_{y'}$, alors les points de $P_{x'}$ et $P_{y'}$ définis par x sont identiques (car si $\overline{x}$ est le premier, on aura pour $f = X/y'$: $f = (X/x')/(y'/x')$, et comme y'/x' est défini et non nul en $\overline{x}$, et X/x' défini en $\overline{x}$, f est défini en $\overline{x}$ et $f(\overline{x}) = (X(x)/x'(x))/(y'(x)/x'(x)) = X(x)/y'(x)$ C.Q.F.D.). Ainsi pour tout x non nul dans V, $\overline{x}$ désigne un point bien déterminé de $P(V)$, et l'application $x \to \overline{x}$ est une application de $V-(0)$ sur $P(V)$, deux points x, y ayant la même image si et seulement s'ils sont proportionnels. Donc, en tant qu'ensemble $P(V)$ s'identifie à "l'espace projectif" défini par V, ensemble des droites vectorielles de V. Quand on considérera cet ensemble comme variété algébrique, il sera entendu qu'il s'agira de la structure qu'on vient de définir.

La vérification des points suivants, qui ne sont pas plus difficiles que ce qui précède, est laissée au lecteur. La structure algébrique induite sur les $P_{x'}$ est aussi celle associée à la structure d'espace affine bien connue sur $P_{x'}$; il en résulte en particulier que l'application $x \to \overline{x}$ de $V - (0)$ dans $P(V)$ est régulière. La topologie de $P(V)$ est la topologie quotient ; en d'autres termes, une partie de $P(V)$ est fermée si et seulement si son image réciproque dans $V - (0)$ l'est ; il en résulte que les parties fermées de $P(V)$ correspondent aussi bijectivement aux cônes fermés non vides de V (les irréductibles correspondant aux cônes irréductibles, la partie vide au cône (0)), ou encore aux idéaux *homogènes* de l'algèbre affine $K[V] = K[X_1, \ldots, X_n]$ de V, distincts de $K[V]$, qui sont intersections d'idéaux homogènes premiers (ces derniers

correspondant aux sous-variétés de $P(V)$ et à la partie vide de $P(V)$). Une variété X est projective si et seulement si elle est isomorphe à une sous-variété (fermée) d'un espace projectif $P(V)$ (en effet, la définition par schémas signifie exactement, après traduction en langage compréhensible, que X est isomorphe à une variété $\overline{f(Y)}$, où Y est une sous-variété d'un espace vectoriel V et f l'application canonique de $V - (0)$ dans $P(V)$). Les applications rationnelles d'un espace projectif dans un autre sont celles qui s'expriment, après introduction de coordonnées projectives, par des polynômes homogènes tous de même degré (et les points où une telle application est définie sont précisément ceux pour lesquels tous ces polynômes ne s'annulent pas simultanément) ; résultat analogue pour les applications rationnelles d'un produit d'espaces projectifs. *Le produit de deux espaces projectifs $P(V)$ et $P(W)$ est une variété projective*, et s'identifie même canoniquement à une sous-variété de $P(V \otimes W)$: il suffit de passer au quotient dans l'application $(x, y) \to x \otimes y$ de $V \times W$ dans $V \otimes W$. Il en résulte que le produit de deux variétés projectives est une variété projective.

Définition des variétés grassmanniennes. Soit toujours V un espace vectoriel de dimension n ; nous allons mettre sur l'ensemble $G_d(V)$ de ses sous-espaces vectoriels E de dimension d une structure de variété projective (pour tout d tel que $1 \leq d \leq n$). Nous pouvons supposer $1 < d < n$. Il est bien connu que pour tout E, le produit extérieur des éléments d'une base de E est bien défini à une multiplication par un scalaire près, et que l'application $f : G_d(V) \to P(\wedge^d V)$ ainsi obtenue est injective. L'image en est d'ailleurs une sous-variété fermée de $P(\wedge^d V)$. Considérons en effet une base $(e_i)_{1 \leq i \leq n}$ de V, soit E_0 l'espace vectoriel sous-tendu par les e_i avec $1 \leq i \leq d$, F l'espace vectoriel sous-tendu par les autres e_j, U l'ouvert affine dans $P(\wedge^d V)$ correspondant aux multivecteurs dont la composante suivant $e_1 \wedge e_2 \wedge \ldots \wedge e_d$ est $\neq 0$; il suffit de montrer que $U \cap f(G_d(V))$ est une sous-variété fermée de l'espace affine U (car les U en question recouvrent $P(\wedge^d V)$). Or les $E \in G_d(V)$ qui correspondent à des points de U sont ceux qui se projettent *sur* E_0 par la projection parallèle à F, cette projection étant donc un isomorphisme de E sur E_0. Soient alors $x_i(E)$ $(1 \leq i \leq d)$ les éléments de E images inverses des e_i $(1 \leq i \leq d)$. L'espace vectoriel E est complètement déterminé quand on connait les $x_i(E)$, donc quand on connait leur projections $y_i(E)$ sur F, et ces projections peuvent être prises arbitrairement : on aura alors $x_i(E) = e_i + y_i(E)$, d'où $f(E) = e_1 \wedge \ldots \wedge e_d + \sum_{1 \leq i \leq d} (-1)^{i+1}\, y_i(E) \wedge e_1 \wedge \ldots \wedge \hat{e}_i \wedge \ldots \wedge e_d + \ldots$.
Il en résulte, identifiant U à l'espace des multivecteurs dans $\wedge^d V$ dont la composante suivant $e_1 \wedge \ldots \wedge e_d$ est 1, que les composantes de $f(E)$ peuvent s'exprimer comme polynômes bien déterminés en les composantes suivant les $e_j \wedge e_1 \wedge \ldots \wedge \hat{e}_i \wedge \ldots \wedge e_d$ (où $1 \leq i \leq d$, $d+1 \leq j \leq n$) et que ces dernières (dont la donnée correspond à la donnée des $y_i(E)$) peuvent être choisies arbitrairement. Ainsi, identifiant U à un produit de deux espaces affines convenables R et S, $f(G_d) \cap U$ s'identifie au graphe d'une

application polynôme de R dans S, et est donc bien une sous-variété fermée (d'ailleurs isomorphe à un espace affine). Nous avons ainsi prouvé que $G_d(V)$ s'identifie à une sous-variété de $P(\wedge^d V)$, (d'ailleurs "rationnelle", *i.e.* birationnellement équivalente à un espace affine) et nous munirons par suite $G_d(V)$ de la structure induite. Nous laissons au lecteur le soin de vérifier que, si $1 \leq d \leq d' \leq n$, l'ensemble des $(F, E) \in G_d(V) \times G_{d'}(V)$ tels que $F \subset E$ est une sous-variété fermée du produit, d'où résulte plus généralement que pour des entiers donnés $0 < d_1 \leq d_2 \leq \ldots \leq d_k < n$ l'ensemble des $(E_1, \ldots, E_k) \in G_{d_1}(V) \times \ldots \times G_{d_k}(V)$ tels que $E_1 \subset E_2 \subset \ldots \subset E_k$ est une sous-variété fermée du produit (il suffit de noter qu'elle est fermée, elle sera automatiquement irréductible et non singulière, puisque le groupe connexe $\mathrm{GL}(V)$ y opère transitivement) ; on l'appelle la *variété des drapeaux de type* $(d_1, \ldots, d_k)$. On appelle simplement *drapeau* dans V un $(1, 2, \ldots, n-1)$ drapeau de V ; ils forment donc une variété projective appelée *variété des drapeaux de* V.

Rappelons enfin qu'une variété affine complète est réduite à un point (**SCC**, exposé 5, numéro 4), et que l'image d'une variété complète par un morphisme est une variété complète (résulte du fait que cette image est fermée – **SCC**, exposé 8, théorème 1 – et qu'un schéma dominé par un schéma complet est complet – trivial sur les définitions –).

5.5 Appendice I. Localités non ramifiées [4] [5]

Soit L/K une extension de type fini d'un corps K ; soient $\mathfrak{o}'$ et $\mathfrak{o}$ des localités de L, $\mathfrak{m}'$ et $\mathfrak{m}$ leurs idéaux maximaux, k' et k les corps résiduels $\mathfrak{o}'/\mathfrak{m}'$ et $\mathfrak{o}/\mathfrak{m}$ respectivement. On suppose que $\mathfrak{o}'$ domine $\mathfrak{o}$; on dit que $\mathfrak{o}'$ est *non ramifiée par rapport à* $\mathfrak{o}$ si les conditions suivantes sont satisfaites :

a) le corps des fractions M' de $\mathfrak{o}'$ est algébrique sur celui, M, de $\mathfrak{o}$;

b) le corps k' est algébrique et séparable sur k ;

c) l'ensemble $\mathfrak{m}$ est un ensemble de générateurs de l'idéal $\mathfrak{m}'$ de $\mathfrak{o}'$.

Dans ces conditions, $\mathfrak{o}'$ domine $\mathfrak{o}$ régulièrement (**SCC**, exposé 11) ; il en résulte que $\mathfrak{o}'$ est anneau local d'un idéal maximal $\mathfrak{M}$ d'un anneau $\mathfrak{O}$ contenant $\mathfrak{o}$ et entier sur $\mathfrak{o}$ (**SCC**, exposé 12, théorème 1). L'anneau $\mathfrak{o}$ est anneau local d'un idéal premier d'une algèbre affine A sur K ; la fermeture intégrale A^* de A dans M' étant un A-module de type fini (**SCC**, exposé 4, théorème 1), la fermeture intégrale $\mathfrak{o}^* = \mathfrak{o}[A^*]$ de $\mathfrak{o}$ est un $\mathfrak{o}$-module de type fini, et il en est de même de $\mathfrak{O}$; il en résulte en particulier que k' est de degré fini sur k. L'anneau $\mathfrak{O}$ n'est en général pas déterminé de manière unique ;

[4] L'hypothèse que le corps K est algébriquement clos n'est pas utilisée dans cet appendice.

[5] Les deux appendices sont de Chevalley.

nous allons montrer que, *sous les hypothèses faites, on peut toujours prendre* $\mathfrak{O}$ *de la forme* $\mathfrak{o}[u]$ *où* u *est un élément de* $\mathfrak{o}'$ *qui est racine d'un polynôme unitaire* F *à coefficients dans* $\mathfrak{o}$ *tel que* $F'(u) \notin \mathfrak{m}'$ (où F' est le polynôme dérivé de F).

Puisque $\mathfrak{m}$ engendre $\mathfrak{m}'$, le transporteur $\mathfrak{a} = \mathfrak{m}\mathfrak{O}$: $\mathfrak{M}$ de $\mathfrak{M}$ dans $\mathfrak{m}\mathfrak{O}$ n'est pas contenu dans $\mathfrak{M}$; on a donc $\mathfrak{a} + \mathfrak{M} = \mathfrak{O}$; soit donc u un élément de $\mathfrak{a}$ tel que la classe $\overline{u}$ de u modulo $\mathfrak{m}' = \mathfrak{M}\mathfrak{o}'$ soit un générateur $\neq 0$ de l'extension k'/k. Posons $\mathfrak{O}_1 = \mathfrak{o}[u]$, $\mathfrak{M}_1 = \mathfrak{M} \cap \mathfrak{O}_1$; soient $\mathfrak{o}_1$ l'anneau local de $\mathfrak{M}_1$ et $\mathfrak{m}_1 = \mathfrak{M}_1\mathfrak{o}_1$. Il est clair que $\mathfrak{o}'$ domine $\mathfrak{o}_1$, est non ramifiée par rapport à $\mathfrak{o}_1$ et que $\mathfrak{o}'/\mathfrak{m}' = \mathfrak{o}_1/\mathfrak{m}_1$; on va montrer que $\mathfrak{o}_1 = \mathfrak{o}'$. Il suffira pour cela de montrer que $\mathfrak{o}' \subset \mathfrak{o}_1$. Tout idéal maximal $\mathfrak{M}' \neq \mathfrak{M}$ de $\mathfrak{O}$ contient $\mathfrak{m}\mathfrak{O}$ et par suite aussi $\mathfrak{a}$, donc u, et engendre par suite l'idéal unité dans $\mathfrak{o}_1[\mathfrak{O}]$ (car $u^{-1} \in \mathfrak{o}_1$ puisque $u \notin \mathfrak{M}$). Comme $\mathfrak{o}_1[\mathfrak{O}]$ est l'anneau des fractions de la partie $\mathfrak{O}_1 - \mathfrak{M}_1$ de $\mathfrak{O}$, on voit que $\mathfrak{o}_1[\mathfrak{O}]$ n'a qu'un idéal maximal, donc est un anneau local ; c'est l'anneau local d'un idéal maximal de $\mathfrak{O}$, qui ne peut être que $\mathfrak{M}$, d'où $\mathfrak{o}_1[\mathfrak{O}] = \mathfrak{o}'$. De plus, on a $\mathfrak{m}' = \mathfrak{m}_1\mathfrak{o}'$ et $\mathfrak{o}'/\mathfrak{m}' = \mathfrak{o}_1/\mathfrak{m}_1$; il en résulte immédiatement que $\mathfrak{o}' = \mathfrak{o}_1 + \mathfrak{m}_1\mathfrak{o}'$. Comme $\mathfrak{o}'$ est un module de type fini sur $\mathfrak{o}_1$ (puisque $\mathfrak{o}' = \mathfrak{o}_1[\mathfrak{O}]$), il résulte de la formule $\mathfrak{o}' = \mathfrak{o}_1 + \mathfrak{m}_1\mathfrak{o}'$ et du lemme de Nakayama que $\mathfrak{o}' = \mathfrak{o}_1$.

Comme k' est algébrique et séparable sur k, il existe un polynôme unitaire G à coefficients dans $\mathfrak{o}$ tel que $G(u) \in \mathfrak{M}_1$, $G'(u) \notin \mathfrak{M}_1$. Puisque $u \in \mathfrak{a}$, on a $uG(u) \in \mathfrak{m}\mathfrak{O}$ et, puisque $\mathfrak{O} \subset \mathfrak{o}_1$, il existe des polynômes A, B à coefficients dans $\mathfrak{o}$ tels que les coefficients de A soient dans $\mathfrak{m}$, que $B(u) \notin \mathfrak{M}_1$ et que $uG(u)\,B(u) = A(u)$; on peut manifestement supposer B unitaire. Soit d le degré du polynôme unitaire $XG(X)\,B(X)$; alors, si $\mathfrak{O} = \mathfrak{o} + \mathfrak{o}\,u + \ldots + \mathfrak{o}\,u^{d-1}$, on a $\mathfrak{O}_1 = \mathfrak{O} + \mathfrak{m}\,\mathfrak{O}_1$; appliquant à nouveau le lemme de Nakayama, on voit que $\mathfrak{O}_1 = \mathfrak{O}$. Ceci montre qu'on peut supposer que A est de degré $< d$; si $F(X) = XG(X)\,B(X) - A(X)$, F possède les propriétés requises.

Soit réciproquement $\mathfrak{o}$ *une localité. Soit* u *un élément d'un sur-corps du corps des fractions de* $\mathfrak{o}$ *qui est racine d'un polynôme unitaire* F *à coefficients dans* $\mathfrak{o}$ *; s'il existe un idéal maximal* $\mathfrak{M}$ *de* $\mathfrak{o}[u]$ *qui ne contient pas* $F'(u)$*, l'anneau local* $\mathfrak{o}'$ *de* $\mathfrak{M}$ *est une localité non ramifiée par rapport à* $\mathfrak{o}$*.* Soit en effet $\overline{G}$ le polynôme minimal par rapport à $k = \mathfrak{o}/\mathfrak{m}$ de la classe $\overline{u}$ de u modulo $\mathfrak{M}$, et soit $\overline{F}$ le polynôme déduit de F par réduction des coefficients modulo $\mathfrak{m}$. Il est clair que $\overline{F}$ est divisible par $\overline{G}$ mais que $\overline{F}'$ ne l'est pas ; soit G un polynôme à coefficients dans $\mathfrak{o}$ qui donne $\overline{G}$ par réduction modulo $\mathfrak{m}$; il résulte alors de ce qu'on vient de dire qu'il y a un polynôme H à coefficients dans $\mathfrak{o}$ tel que $H(u) \not\equiv 0 \pmod{\mathfrak{M}}$ et que $GH - F$ soit à coefficients dans $\mathfrak{m}$; $G(u)$ est donc dans l'idéal $\mathfrak{m}\,\mathfrak{o}'$. Or il est clair que $\mathfrak{M}$ est engendré par $\mathfrak{m}$ et par $G(u)$; on a donc $\mathfrak{m}\,\mathfrak{o}' = \mathfrak{m}'$. Par ailleurs, comme $\overline{F}'(\overline{u}) \neq 0$, on a aussi $\overline{G}'(\overline{u}) \neq 0$ et il en résulte que $\overline{u}$ est séparable sur k. Ceci montre bien que $\mathfrak{o}'$ est non ramifiée par rapport à $\mathfrak{o}$.

Soit maintenant $\mathfrak{o}$ une localité normale ; soit $\mathfrak{O}$ un anneau contenu dans un sur-corps du corps des fractions de $\mathfrak{o}$, contenant $\mathfrak{o}$ et entier sur $\mathfrak{o}$; soient

$\mathfrak{m}$ l'idéal maximal de $\mathfrak{o}$, $\mathfrak{M}_i$ $(1 \leq i \leq h)$ les idéaux maximaux de $\mathfrak{O}$ et $\mathfrak{o}_i$ leurs anneaux locaux. *Pour que $\mathfrak{o}$ ne soit pas ramifiée dans le corps des fractions de $\mathfrak{O}$ au sens de la définition 1, il faut et il suffit qu'aucune des localités $\mathfrak{o}_i$ ne soit ramifiée par rapport à $\mathfrak{o}$.* La condition est en effet nécessaire d'après le théorème 1. Supposons-la satisfaite. Le transporteur de $\mathfrak{M}_1 \cap \ldots \cap \mathfrak{M}_h$ dans $\mathfrak{m}\mathfrak{O}$ n'est alors contenu dans aucun des $\mathfrak{M}_i$ et contient par suite 1, ce qui montre que $\mathfrak{m}\mathfrak{O} = \mathfrak{M}_1 \cap \ldots \cap \mathfrak{M}_h$, donc que $\mathfrak{O}/\mathfrak{m}\mathfrak{O}$ est somme directe des $\mathfrak{O}/\mathfrak{M}_i$ qui sont par hypothèse des extensions séparables de $\mathfrak{o}/\mathfrak{m}$; alors $\mathfrak{O}/\mathfrak{m}\mathfrak{O}$ est une algèbre séparable, ce qui montre que $\mathfrak{o}$ n'est pas ramifiée.

Soient $\mathfrak{o}'$ et $\mathfrak{o}$ des localités telles que $\mathfrak{o}'$ domine $\mathfrak{o}$ et soit non ramifiée par rapport à $\mathfrak{o}$; soient $\mathfrak{p}'$ un idéal premier de $\mathfrak{o}'$ et $\mathfrak{p} = \mathfrak{p}' \cap \mathfrak{o}$; alors $\mathfrak{o}'/\mathfrak{p}'$ est non ramifiée par rapport à $\mathfrak{o}/\mathfrak{p}$, et $\mathfrak{o}'_{\mathfrak{p}'}$ non ramifiée par rapport à $\mathfrak{o}_{\mathfrak{p}}$: cela résulte immédiatement du critère que nous avons établi plus haut.

On notera que la condition c) dans la définition des localités non ramifiées peut aussi se formuler comme suit : c′) l'application naturelle de $\mathfrak{m}/\mathfrak{m}^2 \otimes_k k'$ dans $\mathfrak{m}'/\mathfrak{m}'^2$ est surjective. En effet, il est clair que c) entraîne c′) ; si c′) est satisfaite, soit $\mathfrak{n} = \mathfrak{m}\mathfrak{o}'$; on a $\mathfrak{m}' = \mathfrak{n} + \mathfrak{m}'^2$, d'où $\mathfrak{m}' = \mathfrak{n} + \mathfrak{m}'^n$ pour tout n, et par suite $\mathfrak{m}' = \mathfrak{n}$.

5.6 Appendice II. Une variante du "Main theorem" de Zariski

Nous nous proposons de démontrer le résultat suivant, qui nous sera utile dans la suite :

Proposition 1. – *Soit f un morphisme d'une variété U dans une variété normale V tel que $f(U)$ soit dense dans V. Soit x un point de U qui est un point isolé de l'ensemble $f^{-1}(f(x))$. Alors l'image par f de tout voisinage de x dans U est un voisinage de $f(x)$ dans V.*

En remplaçant U par sa normalisée (dans son corps de fonctions rationnelles lui-même), on se ramène immédiatement au cas où U est normale. Comme $f^{-1}(f(x))$ a une composante irréductible $\{x\}$ de dimension 0, on a $\dim U = \dim f(U)$ d'après **SCC**, exposé 8, théorème 2, d'où $\dim U = \dim V$; le corps $K(U)$ des fonctions rationnelles sur U est donc algébrique sur celui, $K(V)$, des fonctions rationnelles sur V. Soit U' la normalisée de V dans $K(U)$; l'application f se factorise en $f' \circ g$, où f' est l'application canonique $U' \to V$ et g un morphisme birationnel $U \to U'$. Soit $x' = g(x)$; comme x est isolé dans $g^{-1}(x')$, il résulte du théorème principal de Zariski que l'anneau local de x est anneau local d'un idéal maximal d'un anneau entier sur l'anneau local de x', donc est identique à ce dernier. La fonction sur U' à valeurs dans U réciproque de g est donc définie en x', d'où il résulte tout de suite que g induit un isomorphisme d'une sous-variété ouverte convenable de U contenant x sur une sous-variété ouverte de U'.

Il suffira donc de démontrer la proposition dans le cas où U est la normalisée de V dans $K(U)$. Dans ces conditions, l'image par f de toute partie fermée de U est fermée dans V (**SCC**, théorème 1, exposé 7 et théorème 1 *bis*, exposé 8). De plus, si Y, Y' sont des sous-variétés fermées de V telles que $Y \subset Y'$ et X une sous-variété fermée de U telle que $f(X) = Y$, il existe une sous-variété fermée X' de U contenant X et telle que $f(X') = Y'$. Soient en effet $\mathfrak{o}(X)$ et $\mathfrak{o}(Y)$ les anneaux locaux de X et Y respectivement ; $\mathfrak{o}(X)$ est donc l'anneau local d'un idéal maximal $\mathfrak{x}$ de la fermeture entière $\mathfrak{O}$ de $\mathfrak{o}(Y)$ dans $K(U)$. La variété Y' est déterminée par un idéal premier $\mathfrak{y}'$ de $\mathfrak{o}(Y)$; puisque $\mathfrak{o}(Y)$ est un anneau normal, il existe un idéal premier $\mathfrak{x}'$ de $\mathfrak{O}$ contenu dans $\mathfrak{x}$ et tel que $\mathfrak{x}' \cap \mathfrak{o}(Y) = \mathfrak{y}'$ (**SCC**, exposé 1, théorème 4), ce qui démontre notre assertion.

Ceci dit, soit U_1 un voisinage ouvert de x dans U, et soit $A = U - U_1$; on a $f(U_1) = V - B$, où B est l'ensemble des y' tels que $f^{-1}(y') \subset A$; il suffira donc de démontrer que $y = f(x)$ n'est pas adhérent à B. Or, supposons le contraire ; y est alors adhérent à une composante irréductible B_1 de B, dont l'adhérence est une sous-variété fermée Y de V passant par y. Comme $x \in f^{-1}(y)$, il y a une sous-variété fermée X de U passant par x telle que $f(X) = Y$ (voir l'alinéa précédent). Si X_0 est une partie relativement ouverte de X, $f(X_0)$ contient une partie relativement ouverte Y_0 de Y et rencontre par suite B_1 ; l'ensemble $X \cap f^{-1}(B_1)$ est donc dense dans X. Or on a $f^{-1}(B_1) \subset A$ et A est fermé ; on a donc $X \subset A$, d'où contradiction puisque $x \notin A$.

Corollaire. – *Soit f un morphisme d'une variété U dans une variété normale V. On suppose que $f(U)$ est dense dans V et que l'ensemble A des points y de V tels que $f^{-1}(y)$ soit fini est non vide. Alors A est ouvert dense dans V.*

En effet pour y dans A, chaque point x de $f^{-1}(y) = f^{-1}(f(x))$ est isolé dans cet ensemble fini.

6. Les théorèmes de structure fondamentaux pour les groupes algébriques affines [1]

6.1 Espaces de transformations

On appelle *espace de transformation algébrique* le système formé par un groupe algébrique G, un ensemble algébrique E, et une application régulière $G \times E \to E$, notée $(g, x) \to g \cdot x$, satisfaisant les conditions bien connues $e \cdot x = x$ et $g \cdot (g' \cdot x) = (gg') \cdot x$. Si H est un sous-groupe invariant fermé de G qui opère trivialement sur E, alors par passage au quotient G/H opère sur E ; en utilisant les méthodes du n° 8.6, on prouve que l'application correspondante $G/H \times E \to E$ est encore régulière (quand on munit G/H de la structure de groupe algébrique décrite dans le théorème 4 du n° 8.4), de sorte que E devient un espace de transformation algébrique de groupe G/H.

Soit (E, G) un espace de transformation algébrique ; on appelle *orbite* d'un point $x \in E$ l'ensemble des $g \cdot x$ $(g \in G)$.

Lemme 1. – *Une orbite est ouverte dans son adhérence.*

Si f est une application régulière d'un ensemble algébrique G dans un autre E, alors l'intérieur de $f(G)$ dans $\overline{f(G)}$ est dense dans $f(G)$: cela résulte de **SCC**, exposé 7, théorème 3 dans le cas où G et E sont irréductibles, et s'en déduit aisément dans le cas général. Prenons, dans le cas actuel, $f(g) = g \cdot x$; on voit donc que l'intérieur de l'orbite de x dans son adhérence est non vide, or cet intérieur est évidemment invariant sous G, et comme G est transitif dans l'orbite, la conclusion voulue apparaît. Ainsi une orbite est un ensemble algébrique sur lequel G opère transitivement ; c'est donc un espace de transformation algébrique transitif par G, et en particulier tous ses points sont simples (et *a fortiori* normaux) (puisqu'il existe des points simples dans un ensemble algébrique non vide), et toutes ses composantes irréductibles ont même dimension. Si l'orbite n'est pas fermée, alors son complémentaire dans son adhérence est une partie fermée de V, stable par G, de dimension strictement inférieure à celle de l'orbite. Il contient alors une orbite, nécessairement de dimension inférieure à celle de $G \cdot x$, d'où :

Corollaire. – *Une orbite de dimension minimum est fermée (en particulier, il existe des orbites fermées).*

[1] Exposé de A. Grothendieck, le 10.12.1956

Le théorème suivant est l'outil technique essentiel de la théorie de Borel :

Théorème 1. – (A. Borel) *Soit E un espace de transformation algébrique* complet *de groupe G* affine résoluble connexe. *Alors il existe au moins un point de E fixe sous G.*

Démonstration. – Soit H un sous-groupe distingué fermé de G. Alors l'ensemble des points de E fixés par H est une partie fermée de E *stable par* G ; par suite si elle n'est pas vide, c'est un espace de transformation algébrique sous G, et même sous G/H puisque H y opère trivialement, et tout point fixe de ce dernier par G/H est un point fixe de E par G. Considérant alors une suite de composition de G par des sous-groupes distingués connexes fermés à quotients successifs abéliens, et tenant compte qu'un groupe algébrique quotient d'un groupe algébrique affine est affine (*cf.* exposé 3), une récurrence immédiate sur la longueur de cette suite de composition nous ramène au cas où G est *abélien*. D'après le corollaire au lemme précédent, il existe une orbite fermée $X = G \cdot x$; si H est l'ensemble des $g \in G$ tels que $g \cdot x = x$, l'application $g \to g \cdot x$ définit alors une application régulière bijective de G/H sur X. Comme X est complète, il résulte du théorème 2, corollaire 3 (compte tenu que X est normale) que G/H est complète ; or H est un sous-groupe distingué du groupe affine (abélien) G, donc G/H est affine, et par suite est réduit à un point. Donc l'orbite X est réduite à un point, évidemment fixe par G. C.Q.F.D.

6.2 Le théorème de Lie-Kolchin

Théorème 2. – (Lie-Kolchin) *Soit V un espace vectoriel de dimension finie sur K, et soit G un groupe algébrique d'automorphismes de V. Si G est résoluble et connexe, il existe une base de V par rapport à laquelle les éléments de G s'expriment par des matrices triangulaires.*

Il revient au même de dire qu'il existe une suite de composition du G-module V dont les quotients successifs sont de dimension 1, *i.e.* un *drapeau* de V invariant sous G (n° 5.4). Comme G est un groupe résoluble et connexe opérant dans la variété des drapeaux, qui est complète, l'assertion est un cas particulier du théorème 1.

Corollaire 1. – *Un groupe algébrique affine résoluble et connexe admet une suite de composition dont les facteurs sont connexes et de dimension* 1.

Tout d'abord, ce résultat est immédiat pour le groupe $T(n)$ des matrices triangulaires de degré n : en effet, désignant par T_k $(1 \leq k \leq n)$ l'ensemble des matrices triangulaires qui n'ont que des 1 sur la diagonale principale (et en particulier $T_n = \{e\}$), et dont les coefficients a_{ij} sont nuls si $i < j \leq i + k$, et posant $T_0 = T(n)$, on voit qu'on obtient ainsi une suite de composition dont les quotients successifs sont $T_i/T_{i+1} \simeq D(n) = K^{*n}$ si $i = 0$, $T_i/T_{i+1} \simeq K^{n-i}$

pour $1 \leq i < n$. Raffinant la suite de composition précédente, on obtient une suite de composition dont les quotients successifs sont isomorphes à K^* ou K. Si G est affine résoluble et connexe, il est isomorphe à un sous-groupe fermé d'un $T(n)$ d'après le théorème 2 ; prenant la trace sur G d'une suite de composition convenable de $T(n)$, on trouve une suite de composition dont les facteurs L_i admettent des représentations rationnelles fidèles dans K^* ou K, et sont donc de dimension 1. Remplaçant les L_i par leurs composantes neutres, on trouve une suite de composition formée de sous-groupes connexes, à facteurs de dimension 1.

Corollaire 2. – *Soit G un groupe algébrique affine résoluble et connexe. Alors l'ensemble G_u de ses éléments unipotents est un sous-groupe fermé invariant nilpotent, et G/G_u est commutatif.*

Comme G est isomorphe à un sous-groupe fermé d'un groupe $T(n)$, il suffit de remarquer que les valeurs propres d'une matrice triangulaire sont ses éléments diagonaux, et qu'une matrice triangulaire est donc unipotente si et seulement si sa diagonale se réduit à des 1. De plus, les sous-groupes T_i $(1 \leq i \leq n)$ forment une suite centrale pour $T(n)_u$, qui est donc nilpotent ; il en est donc de même de G_u.

Corollaire 3. – *Soit G un groupe algébrique affine résoluble et connexe et soit H un sous-groupe de G formé d'éléments semi-simples. Alors H est commutatif ; son centralisateur et son normalisateur dans G sont identiques.*

L'hypothèse implique que l'homomorphisme de H dans G/G_u induit par l'homomorphisme canonique est injectif ; comme G/G_u est commutatif, il en est de même de H. Soit $g \in G$ normalisant H ; on a donc, pour $h \in H$, $ghg^{-1}h^{-1} \in H$; or on a aussi $ghg^{-1}h^{-1} \in G_u$ en vertu du corollaire 2, d'où $ghg^{-1}h^{-1} = e$, et g centralise H.

Remarque. – Le fait que G soit connexe est évidemment essentiel pour la validité du théorème 2 (prendre G fini !). Cependant, on voit directement, par récurrence sur la longueur d'une suite de composition à quotients commutatifs, et utilisant le fait qu'un caractère rationnel multiplicatif sur un groupe algébrique affine formé d'éléments unipotents est égal à 1, que si G est un groupe algébrique linéaire formé d'éléments *unipotents* et si G est résoluble (on verra en fait que la première hypothèse implique déjà que G est nilpotent), alors il existe une base par rapport à laquelle G soit triangulaire.

6.3 Structure des groupes algébriques affines nilpotents

Théorème 3. – *Soit G un groupe algébrique affine nilpotent. Si G est connexe, G_u et G_s sont des sous-groupes invariants fermés connexes, G_s est dans le centre de G, et G s'identifie au produit direct de G_s et G_u. En tout cas (G*

connexe ou non) deux éléments de G dont l'un au moins est semi-simple, et l'un au moins est dans la composante neutre G_0 de G, commutent.

Supposons d'abord G *connexe* ; en vertu du théorème de Lie-Kolchin, on peut donc supposer que G est un sous-groupe fermé d'un groupe $T(n)$. On sait déjà que G_u est un sous-groupe fermé invariant (corollaire 2 au théorème 2). Prouvons que G_s *est dans le centre de* G *par récurrence sur* $\dim G$, l'assertion étant triviale pour $\dim G = 0$. Supposons donc $\dim G > 0$; alors le centre de G est de dimension > 0, de composante neutre C ; on sait (n° 4.5, théorème 4) que l'on a $C = C_s \times C_u$. Si $C_s \neq \{e\}$, soit f une représentation linéaire de G de noyau C_s (n° 4.2, corollaire au théorème 1), et soit $G' = f(G)$; d'après l'hypothèse de récurrence, G'_s est central dans G', et de plus $f^{-1}(G'_s) = G_s$ puisque $f(G_s) = G'_s$ (n° 4.4, corollaire au théorème 3) et que $G_s = G_s C_s$; il en résulte que G_s est un sous-groupe fermé invariant de G, et comme il est formé d'éléments semi-simples, il est central (théorème 2, corollaire 3). Si $C_u \neq \{e\}$, soit f un homomorphisme rationnel de G ayant pour noyau C_u, et soit G' son image. Alors pour $s \in G_s$, $f(s)$ est semi-simple dans G', donc central par l'hypothèse de récurrence, donc pour $g \in G$ on a $gsg^{-1} = su$ $(u \in C_u)$; comme s et u commutent c'est là la décomposition canonique de gsg^{-1} en ses parties semi-simple et unipotente, et comme gsg^{-1} est évidemment semi-simple, on a $u = e$, d'où $gsg^{-1} = s$. On a prouvé que G_s est l'ensemble des matrices semi-simples du centre de G, ce qui prouve que c'est un sous-groupe fermé (théorème 4 du n° 4.5) évidemment invariant.

L'application $(s, u) \to su$ de $G_s \times G_u$ dans G est donc une représentation rationnelle, évidemment bijective ; pour montrer que c'est un isomorphisme, il suffit de montrer que l'application $g \to g_s$ de G dans G_s est rationnelle. Mais comme G_s est commutatif, on peut trouver une base de l'espace V où opère G, telle que par rapport à cette base, les matrices de G_s soient diagonales (n° 4.4, lemme 3), de sorte que pour $g \in G$, g_s est la partie diagonale de g. Cela implique bien que $g \to g_s$ est rationnelle, donc que G est isomorphe à $G_s \times G_u$, d'où on conclut (puisque G est connexe) que G_s et G_u sont connexes.

Démontrons la deuxième partie du théorème, en distinguant les deux cas possibles.

a) *Prouvons que* G_{0s} *est dans le centre de* G. D'après ce qu'on a vu, G_{0s} est un sous-groupe fermé central connexe de G_0, évidemment invariant par tout automorphisme de G_0, donc invariant dans G. Pour tout $g \in G$, l'automorphisme $\mathrm{int}(g) : s \to gsg^{-1}$ de G_{0s} défini par g est d'ordre fini, puisqu'on a $g^m \in G_0$ pour m convenable ; d'autre part, il résulte de la nilpotence de G qu'il existe une suite de composition de G formée de sous-groupes invariants T_i, tels que $\mathrm{int}(g)$ induise l'identité dans les T_i/T_{i+1}. Prenant les traces des T_i sur G_{0s}, et appliquant la proposition 7 du n° 4.6, on voit que $\mathrm{int}(g)$ est l'identité sur G_{0s}.

b) *Tout élément semi-simple* s *de* G *centralise* G_0. En effet, comme on a $G_0 = G_{0s} \times G_{0u}$, et que s centralise G_{0s} d'après a), il suffit de montrer qu'il

centralise G_{0u}. Pour ceci, reprenant les T_i comme ci-dessus, on applique le lemme 4 du n° 4.6.

Remarque. – La structure des groupes algébriques affines connexes nilpotents est ainsi ramenée au cas d'un groupe *unipotent* connexe. Bien entendu cette structure est loin d'être bien connue (même dans le cas commutatif). Signalons cependant que nous verrons au n° 7.4 qu'un groupe connexe unipotent de dimension 1 est isomorphe à K, d'où il résulte facilement qu'un groupe unipotent connexe admet une suite de composition dont les facteurs sont isomorphes à K. Appliquant un résultat de Rosenlicht (qui implique que la "fibration" d'un groupe algébrique par un sous-groupe fermé *résoluble* est toujours "localement triviale"), et le fait qu'un espace fibré algébrique localement trivial sur K, de groupe K, est trivial (car la base K est un ensemble algébrique *affine*), on trouve qu'un groupe algébrique affine nilpotent connexe unipotent est isomorphe, en tant que variété, à un K^n (et sa loi de composition est donc donnée par des polynômes). La réciproque a été prouvée par Michel Lazard.

6.4 Structure des groupes algébriques affines résolubles et connexes

Théorème 4. – *Soit G un groupe algébrique affine résoluble et connexe. Alors G_u est un sous-groupe invariant fermé connexe nilpotent, les tores maximaux de G sont conjugués par automorphismes intérieurs, et si T est un tel tore, G est le produit semi-direct de G_u par T.*

(Cette dernière assertion signifie, par définition, que l'application $(s, u) \to su$ de $T \times G_u$ dans G est un isomorphisme d'ensembles algébriques.)

Les assertions concernant G_u, sauf la connexité, sont déjà établies (corollaire 2 au théorème 2) ; le fait que G_u est connexe résultera aussitôt de la dernière partie du théorème. Le groupe G/G_u est un groupe affine commutatif (théorème 2, corollaire 2) dont tous les éléments sont semi-simples (car un élément unipotent de G/G_u doit provenir d'un élément de G_u d'après le corollaire du théorème 3 du n° 4.4 ; donc G/G_u est diagonalisable et connexe, c'est donc un tore Q (n° 4.3, corollaire 2 du théorème 2). Nous voulons prouver :

(i) l'extension G de Q par G_u est triviale, *i.e.* il existe un homomorphisme rationnel f de Q dans G dont le composé avec $G \to Q$ soit l'identité.

Alors $T = f(Q)$ est un tore dans G, et le fait que T soit un tore maximal et conjugué à tout autre tore maximal revient alors à dire :

(ii) pour tout tore S de G, il existe un $g \in G$ tel que $gSg^{-1} \subset T$.

Au lieu de (ii), nous prouverons le résultat plus fort :

Lemme 2. – *Soit G un groupe résoluble connexe produit semi-direct du tore T et de G_u, et soit S une partie semi-simple commutative de G. Alors il existe $u \in G_u$ tel que $uSu^{-1} \subset T$.*

Pour démontrer (i), (ii) et le lemme 2, on est ramené au cas où G_u est commutatif, grâce aux deux lemmes suivants, qui se démontrent par une récurrence évidente :

Lemme 3. – *Soit G un groupe algébrique, extension d'un groupe algébrique Q par un groupe algébrique U, et soit $(U_i)_{0\leq i\leq n}$ une suite de composition de U par des sous-groupes invariants dans G. Pour que l'extension de Q par U soit triviale, il suffit que, pour tout i avec $0 \leq i \leq n-1$ et tout sous-groupe L de G tel que $L \cap U = U_i$, $L \cdot U = G$, et tel que la bijection $L/U_i \to Q$ soit un isomorphisme, l'extension L/U_{i+1} de Q par U_i/U_{i+1} soit triviale.*

Lemme 4. – *Soit $G = T \cdot U$ un groupe algébrique produit semi-direct du groupe algébrique T par le sous-groupe distingué U, et soit $(U_i)_{0\leq i\leq n}$ une suite de composition de U par des sous-groupes invariants par T. Soit S une partie de G, V un sous-groupe de G. Pour qu'il existe un $v \in V$ tel que $vSv^{-1} \subset T$, il faut et il suffit que pour tout i avec $0 \leq i \leq n-1$ et tout $v \in V$ tels que $vSv^{-1} \subset T \cdot U_i$, l'image S' de vSv^{-1} dans G/U_{i+1} (identifié au produit semi-direct $T \cdot (U_i/U_{i+1})$), soit conjuguée d'une partie de T à l'aide d'un $v' \in V'$ (où V' est l'image de V dans G/U_{i+1}).*

Nous appliquerons ces lemmes en prenant $U = G_u$, et la suite de composition de G_u formée de G_u et des dérivés successifs de G_u, enfin $V = G$ dans le lemme 4 (bien qu'on pourrait raffiner en prenant, avec Borel, le terme terminal de la suite centrale descendante de G). *Nous supposerons donc G_u commutatif.* Montrons qu'il existe un tore T dans G appliqué *sur* Q, par récurrence sur la dimension n de G, l'assertion étant triviale si $n = 0$. Si Q opère trivialement sur G_u, G est nilpotent et notre assertion résulte du théorème 3. Sinon, il existe un élément de Q opérant non trivialement sur G_u, et cet élément provient d'un élément semi-simple s de G, n'appartenant pas au centre. Donc le centralisateur $Z(s)$ de s est $\neq G$; d'autre part, en vertu de la proposition 6 du n° 4.6, $Z(s)$ est appliqué *sur* $Q = G/G_u$, il en est donc de même de $Z(s)_0$. La dimension de $Z(s)_0$ étant $< n$, l'hypotèse de récurrence s'applique, ce qui prouve l'existence du tore T en question. Comme évidemment $T \cap G_u$ est réduit à $\{e\}$, G s'identifie au produit semi-direct $T \cdot G_u$ en tant que groupe abstrait. Montrons enfin que l'application naturelle $(t, u) \to tu$ de $T \times G_u$ dans G est non seulement régulière, mais un isomorphisme pour les structures d'ensembles algébriques. Or, G étant identifié à un groupe algébrique triangulaire (théorème 2), cela se prouve comme dans le théorème 3. Cela prouve (i).

Pour prouver le lemme 2, on peut supposer que S est un sous-groupe fermé de G, nécessairement diagonalisable ; S est donc l'adhérence de la réunion d'une suite croissante de sous-groupes finis S_n. Soit M_n l'ensemble des $u \in G_u$ tels que $uS_nu^{-1} \subset T$; c'est une partie fermée de G_u, et les M_n forment une suite décroissante de parties fermées de G_u dont l'intersection M est l'ensemble des $u \in G_u$ tels que $uSu^{-1} \subset T$. Pour montrer que M est non vide, il suffit de le montrer pour chacun des M_n ; on est donc ramené au

cas où S est un groupe *fini*. Soit $G' = S \cdot G_u$, $S' = T \cap G'$; alors G' est le produit semi-direct de S par G_u et de S' par G_u, et pour prouver que S et S' sont conjugués par un élément de G_u, il suffit, comme il est bien connu, de montrer que l'on a $H^1(S, G_u) = 0$ (où G_u est considéré comme groupe abélien sur lequel S opère). Or, si la caractéristique est $p > 0$, chaque élément de G_u est d'ordre une puissance de p tandis que G est d'ordre premier à p, d'où la relation voulue, tandis que si la caractéristique est nulle, G_u est isomorphe à K^n et K étant de caractéristique 0, on a encore $H^1(S, G_u) = 0$. C.Q.F.D.

Corollaire. – *Soient G un groupe algébrique affine résoluble et connexe, S une partie de G semi-simple et commutative. Alors le centralisateur de S est connexe, et S est contenue dans un tore maximal T de G.*

La dernière assertion résulte du lemme 2. Supposons donc $S \subset T$; alors le centralisateur de S est identique à $T \cdot G_u^S$, où G_u^S est l'ensemble des éléments de G_u qui commutent à S. Il s'agit de prouver que G_u^S est connexe ; lorsque S est réduit à un seul élément, cela résulte du corollaire de la proposition 5 du n° 4.6 ; le cas où S est fini se démontre facilement par récurrence sur le nombre d'éléments de S ; enfin, le cas général se ramène comme ci-dessus au cas où S est fini.

6.5 Sous-groupes de Borel, théorèmes de conjugaison

Définition 1. – *Soit G un groupe algébrique affine connexe. On appelle sous-groupe de Borel de G tout sous-groupe résoluble connexe maximal de G.*

Bien entendu, tout sous-groupe résoluble connexe de G est contenu dans un sous-groupe de Borel de G (en particulier, il existe des sous-groupes de Borel de G).

Théorème 5. – *Soient G un groupe algébrique affine connexe et B un sous-groupe de Borel de G.*

a) *Les sous-groupes de Borel de G sont conjugués.*

b) *G/B est une variété projective, et pour qu'un sous-groupe fermé H de G contienne un sous-groupe de Borel, il faut et il suffit que G/H soit une variété complète.*

c) *Les tores maximaux T de G sont conjugués dans G ; un tore maximal de B est aussi un tore maximal de G.*

Démonstration. – On peut supposer que G est un sous-groupe fermé de $\mathrm{GL}(V)$. Soit F la variété des drapeaux de V ; comme G opère sur F, il existe donc une orbite fermée $W = G \cdot d$ (corollaire au lemme 1), où d est un drapeau convenable. Considérons le stabilisateur B_1 de d ; c'est un sous-groupe fermé de G, résoluble puisqu'il est isomorphe à un sous-groupe d'un groupe

$T(n)$ (qui est résoluble) ; soit B la composante neutre dans B_1. L'application $g \to g \cdot d$ induit une application régulière de G/B dans W, telle que l'image réciproque d'un point de W ait toujours le même nombre d'éléments (savoir $[B_1 : B]$). Comme W est projective, il en résulte que G/B est aussi projective (corollaire 3 au théorème 2 du n° 5.3).

Soit R un sous-groupe résoluble connexe de G, et soit H un sous-groupe fermé de G tel que la variété G/H soit complète. Alors R, opérant sur G/H, admet un point fixe (théorème 1), ou ce qui revient au même, il existe $g \in G$ tel que $R \cdot g \cdot H = g \cdot H$ *i.e.* $g^{-1} Rg \subset H$. Appliquant ceci au cas où $H = B$ et où R est un sous-groupe de Borel, on voit qu'on doit avoir $g^{-1} Rg = B$, d'où résulte que B est un sous-groupe de Borel, et que les sous-groupes de Borel sont tous conjugués à B ; ceci prouve a).

Prenant $R = B$, on voit ensuite que si G/H est complète, H contient un sous-groupe de Borel de G (savoir $g^{-1}Bg$). La réciproque est évidente, puisque G/B est complète, et qu'une image d'une variété complète par une application régulière est complète ; ceci prouve b).

Soit T un tore maximal de B, et soit T' un tore maximal de G ; comme T' est résoluble et connexe, il est conjugué à un sous-groupe de B, qui est encore un tore maximal de G et *a fortiori* de B, et est donc conjugué à T (théorème 4) ; ceci prouve que T est aussi un tore maximal de G, et en même temps que deux tores maximaux de G sont conjugués, c'est l'assertion c).

Corollaire 1. – *Tout élément g de G centralisant le sous-groupe de Borel B est dans le centre de G.*

En effet, l'application $x \to xgx^{-1}$ de G dans G passe au quotient et définit une application régulière de G/B dans G. Or, G/B étant connexe et complète (théorème 5, b)) et G étant affine, cette application est constante, ce qui signifie que g est dans le centre de G.

Corollaire 2. – *Soient B un sous-groupe de Borel de G et T un tore maximal de G. Les conditions suivantes sont équivalentes :*

a) *G n'a qu'un seul tore maximal ;*

b) *T est dans le centre de G ;*

c) *G est nilpotent ;*

d) *B est nilpotent.*

Si ces conditions sont satisfaites, on a $B = G$.

c) implique b) en vertu du théorème de structure des groupes nilpotents (théorème 3), b) implique a) en vertu de la conjugaison des tores maximaux. Prouvons que a) implique d) : les tores maximaux de B sont des tores maximaux de G, donc B n'a qu'un seul tore maximal, qui est donc invariant dans B donc dans le centre de B (corollaire à la proposition 2 du n° 4.3). Dans ce cas il en résulte que B est isomorphe au produit direct $T \times B_u$ (théorème 4), donc que B est nilpotent. Prouvons enfin que d) implique c), en prouvant que d) implique $G = B$, par récurrence sur dim B. Si dim $B = 0$, *i.e.* $B = \{e\}$,

$G = G/B$ est complète, donc G étant affine connexe on a $G = \{e\}$. Si $\dim B = n > 0$, la composante neutre H du centre de B est de $\dim > 0$ (puisque B est connexe nilpotent) ; or H est dans le centre de G (corollaire 1) donc invariant dans G, B/H est un sous-groupe de Borel de G/H puisque c'est un sous-groupe résoluble connexe tel que $(G/H)/(B/H) = G/B$ soit complète. Comme B/H est nilpotent, il est identique à G/H d'après l'hypothèse de récurrence, d'où $B = G$. C.Q.F.D.

Signalons le cas particulier suivant du corollaire 2 (compte tenu du théorème 3) :

Corollaire 3. – *Pour que l'on ait $T = \{e\}$, il faut et il suffit que G soit nilpotent et identique à sa partie unipotente.*

Corollaire 4. – *Soit T un tore maximal de G. Alors le centralisateur connexe C de T est identique à son normalisateur connexe, et C est son propre normalisateur connexe. De plus, C est un sous-groupe nilpotent de G, et tout sous-groupe de Borel de G contenant T contient C.*

Soit N le normalisateur de T de composante neutre N_0 ; le groupe T est invariant dans le groupe connexe N_0 et il est diagonalisable, donc il est dans le centre de N_0 (corollaire à la proposition 2 du n° 4.3). Ceci prouve l'identité du centralisateur connexe et du normalisateur connexe. Comme T est un tore maximal de C, c'est l'unique tore maximal d'après c) appliqué aux tores de C, compte tenu que T est dans le centre de C. Donc tout $g \in G$ qui normalise C normalise T, la réciproque étant triviale ; les normalisateurs de T et C coïncident, donc aussi leurs composantes neutres, ce qui prouve que $N(T)_0 = C$ coïncide avec le normalisateur connexe $N(C)_0$ de C. Enfin T est un tore maximal de C et il est dans le centre de C, donc C est nilpotent en vertu du corollaire 2.

Corollaire 5. – *Soient G un groupe algébrique affine connexe, B un sous-groupe de Borel de G, R un sous-groupe fermé résoluble et connexe de G. Soit X l'adhérence de RB dans G. Alors X est un sous-ensemble fermé irréductible de G et il existe un élément x de X tel que R soit contenu dans xBx^{-1}.*

Comme R et B sont des ensembles algébriques irréductibles, il en est de même de $R \times B$; comme X est l'adhérence de l'image de $R \times B$ par le morphisme $(r, b) \to rb$ à valeurs dans G, c'est une partie fermée irréductible de G. Soit f l'application canonique de G sur G/B ; la topologie de Zariski de G/B est quotient de celle de G comme on le verra au n° 8.5, et l'on a $XB = X$; si l'on pose $E = f(X)$, c'est une partie fermée irréductible de G/B, donc une variété complète. Le groupe G agit sur G, et X est stable par le sous-groupe résoluble et connexe R de G; on en déduit une action de R sur E. D'après le théorème 1, il existe un point de E fixé par R, de la forme $f(x)$ avec $x \in X$. On a bien $R \subset xBx^{-1}$.

6.6 Théorèmes de densité

Lemme 5. – *Soient G un groupe algébrique connexe, H un sous-groupe fermé connexe de G, N son normalisateur, $e = \dim N/H$, A la réunion des conjugués de H. Alors A est une partie constructible de G de dimension $\leq \dim G - e$, et pour que sa dimension soit égale à $\dim G - e$, il faut et il suffit qu'il existe un $x \in H$ qui ne soit contenu que dans un nombre fini de conjugués de H. Si G/N est une variété complète, A est fermé dans G.*

(L'hypothèse de connexion sur G et H n'a été faite que parce que **SCC** ne traitait que des variétés irréductibles.) Soit X la partie de $G/N \times G$ formée des couples $(\overline{g}, x)$ ($\overline{g}$ désigne la classe de $g \in G$ dans G/N) tels que $x \in gHg^{-1}$ *i.e.* $g^{-1}xg \in H$ (condition qui ne dépend que de $(\overline{g}, x)$). Comme l'ensemble des (g, x) dans $G \times G$ tels que $g^{-1}xg \in H$ est évidemment fermé, X est une partie fermée de $G/N \times G$. De plus, X est irréductible, car c'est l'image de la variété $G \times H$ par l'application régulière déduite par passage au quotient de l'application $(g, h) \to (g, ghg^{-1})$. Considérons la projection $X \to G/N$; c'est évidemment une application régulière surjective, dont les "fibres" sont isomorphes à H, d'où il résulte que X est de dimension égale à $\dim G/N + \dim H = \dim G - \dim N + \dim H = \dim G - e$. Soit f l'application de projection de X dans G ; on a évidemment $A = f(X)$. Soit A_1 l'ensemble des points de A tels que $f^{-1}(x)$ soit fini. Il en résulte que A est constructible et de dimension $\leq \dim X = \dim G - e$, et que sa dimension est égale à $\dim G - e$ si et seulement si A_1 n'est pas vide. Si G/N est complet, on montre que $G/N \times G$ est complet au-dessus de G (**SCC**, exposé 6, paragraphe 7) donc $f(X) = A$ est une partie fermée de G (*loc. cit.*, exposé 8, théorème 1 *bis*). Cela prouve le lemme.

Supposons maintenant $e = 0$, *i.e.* $H = N_0$, et que A_1 soit non vide, *i.e.* A est dense. En vertu d'un théorème de Chevalley (corollaire à la proposition 1 du n° 5.6) compte tenu que G est normal, on trouve que A_1 est ouvert dense, et même le résultat :

Corollaire. – *Les groupes G et H étant comme dans le lemme 5, supposons H identique à son normalisateur connexe, et qu'il existe un $g \in H$ qui ne soit contenu que dans un nombre fini de conjugués de H. Alors l'ensemble U des points $g \in G$ tels que l'ensemble $E(g)$ des conjugués de H contenant g soit fini non vide, est un ouvert dense. De plus*[2]*, il existe un entier $r \geq 1$ tel que pour tout $g \in U$, l'ensemble $E(g)$ ait au plus r éléments, et tel que l'ensemble V des $g \in G$ tels que $E(g)$ ait exactement r éléments soit un ouvert dense dans G.*

Théorème 6. – *Soient G un groupe algébrique affine connexe, T un tore maximal, C son centralisateur connexe, B un sous-groupe de Borel de G.*

a) *La réunion des conjugués de C contient un ouvert dense.*

[2] Utiliser le corollaire 2 du théorème 2 du n° 5.3.

b) *Tout élément de G est conjugué d'un élément de B,* i.e. *est contenu dans un sous-goupe de Borel.*

c) *Tout élément semi-simple de G est conjugué d'un élément de T,* i.e. *est contenu dans un tore maximal.*

d) *L'intersection des tores maximaux de G est identique à la partie semi-simple du centre de G.*

Pour prouver a), appliquons le lemme 5 avec $H = C$; on a $e = 0$ en vertu du corollaire 4 au théorème 5 ; on est ramené à trouver un élément de C qui ne soit contenu que dans un nombre fini de conjugués de C ; nous allons même construire un $x \in T$ tel que tout $g \in G$ tel que $gxg^{-1} \in C$ normalise T donc C (ce qui implique que x n'est contenu que dans *un seul* conjugué de C). Comme T est isomorphe à K^{*n}, il existe une suite croissante de sous-groupes finis cycliques U_m de T dont la réunion est dense (prendre n nombres premiers $q_1, \ldots, q_n$ distincts et distincts de la caractéristique, et pour tout entier m considérer le sous-groupe $\mathbf{Z}/(q_1^m) \times \ldots \times \mathbf{Z}/(q_n^m)$ de K^{*n}). Le normalisateur de T est l'intersection des ensembles N_m formés des $g \in G$ tels que $g\,U_m\,g^{-1} \subset T$, et comme ces ensembles forment une suite décroissante de fermés, N est identique à l'un des N_m, de sorte qu'il suffira de prendre pour x un générateur de U_m (N.B. si on savait que K est de degré de transcendance assez grand sur son corps premier, on aurait pu prendre plus simplement pour x un élément de T engendrant un sous-groupe dense). Cela prouve a).

A fortiori la réunion des conjugués de B est dense (puisque l'un d'eux contient C d'après le corollaire 4 du théorème 5) ; or elle est fermée en vertu du lemme 5, compte tenu que G/B est complet (théorème 5, b)) donc elle est identique à G, d'où b). Soit $s \in G_s$; on vient de voir qu'il est contenu dans un sous-groupe de Borel B, donc (corollaire du théorème 4) dans un tore maximal de B, qui est aussi un tore maximal dans G (théorème 5, c)) ; ceci prouve c). Soit s un élément semi-simple du centre de G ; il est contenu dans un tore maximal comme on vient de voir, donc dans tous en vertu du théorème de conjugaison. L'intersection des tores maximaux est un sous-groupe invariant fermé diagonalisable, donc *central* puisque G est connexe (corollaire de la proposition 2 du n° 4.3), d'où d).

Corollaire 1. – *Soient R un sous-groupe résoluble connexe de G, et x un élément du centralisateur de R ; alors il existe un sous-groupe de Borel B de G contenant R et x.*

Soit B un sous-groupe de Borel de G ; il faut prouver qu'il existe un élément de G/B invariant à la fois par R et par x. Or l'ensemble X des éléments de G/B invariants par x est fermé et non vide puisque G/B est complète et que x est contenu dans un sous-groupe résoluble connexe en vertu du théorème 6, b), de sorte qu'il suffit d'appliquer le théorème 1. Or X est invariant par R, de sorte qu'il suffit d'appliquer le même théorème pour trouver un élément de X invariant par R.

Corollaire 2. – *Soient S un tore de G et x un élément semi-simple de son centralisateur ; alors il existe un tore maximal contenant x et S.*

D'après le corollaire 1, il existe un sous-groupe de Borel contenant x et S, et en vertu du corollaire du théorème 4, il existe dans ce dernier groupe un tore maximal contenant x et S, d'où la conclusion.

Le résultat suivant sera renforcé plus loin (n° 9.3, théorème 1).

Corollaire 3. – *Tout sous-groupe de Borel de G est d'indice fini dans son normalisateur.*

Soient B un sous-groupe de Borel de G, et N son normalisateur ; posons $e = \dim N/B$. La réunion des conjugués de B est égale à G d'après le théorème 6, b) ; elle est de dimension au plus égale à $\dim G - e$ d'après le lemme 5 appliqué à $H = B$. On a donc $e = 0$, d'où le corollaire 3.

6.7 Théorèmes de centralisation et de normalisation

Théorème 7. – *Soit G un groupe algébrique affine connexe.*

a) *Le centralisateur d'un tore S de G est connexe.*

b) *Soit T un tore maximal. Son centralisateur C est connexe et identique à la composante neutre du normalisateur N de T, donc $W = N/C$ est un groupe fini opérant fidèlement par automorphismes dans T.*

c) *C est un groupe nilpotent maximal identique à son normalisateur connexe.*

d) *Soit B un sous-groupe de Borel de G contenant T ; alors $N \cap B = C$.*

Soit g un élément du centralisateur d'un tore S ; d'après le corollaire 1 au théorème 6, il existe un sous-groupe de Borel B de G contenant S et g. Or le centralisateur de S dans B est connexe (corollaire au théorème 4) donc g appartient à un sous-groupe connexe du centralisateur de S dans G, et ce dernier groupe est connexe. Dans le cas où S est un tore maximal T, le corollaire 4 au théorème 5 prouve donc b), ainsi que le fait que C est nilpotent. Soit M un sous-groupe nilpotent contenant C ; prouvons qu'il est égal à C. On peut supposer M fermé ; alors T est contenu dans la partie semi-simple de la composante neutre M_0 de M, donc est dans le centre de M (théorème 3) ; par suite, M est contenu dans le centralisateur C de T, d'où $M = C$; ceci prouve c) compte tenu du corollaire 4 au théorème 5. Enfin d) résulte du corollaire 3 au théorème 2, appliqué au sous-groupe T de B.

Corollaire 1. – *Le centre de G est égal à celui de son sous-groupe de Borel B, et identique au centralisateur de B dans G.*

Compte tenu du corollaire 1 du théorème 5, il suffit de prouver que si g est dans le centre de G, il est dans B. Or g appartient à un sous-groupe de

Borel de G (théorème 6, b)) donc à tous en vertu du théorème de conjugaison (théorème 5, a)).

Corollaire 2. – *Soit $g \in G$. Alors g est contenu dans le centralisateur connexe de sa partie semi-simple g_s. Si $s \in G_s$ et $u \in G_u$ commutent, u appartient au centralisateur connexe de s.*

Démonstration. – Pour la première assertion, on écrit $g = g_s\, g_u$, g_s est contenu dans un tore (théorème 6, c)), donc est dans le centralisateur connexe de g_s ; il reste à prouver la même chose pour g_u, ce qui nous ramène au deuxième énoncé.

Si la caractéristique de K est 0, le groupe algébrique engendré par un élément unipotent u étant connexe (proposition 4 du n° 4.4), u est contenu dans la composante neutre de tout groupe fermé le contenant. On est donc ramené au cas de caractéristique $p > 0$. Il existe un tore maximal T de G contenant s (théorème 6, c)). Supposons d'abord que s normalise T ; l'ensemble des éléments de T qui commutent à u est connexe (proposition 5 du n° 4.6) donc est un tore S ; alors u appartient au centralisateur de S qui est connexe (théorème 7, a)) et contenu dans le centralisateur H de s (puisque $s \in S$), donc u appartient à la composante neutre H_0 de ce dernier groupe. Dans le cas général, comme T est un tore maximal de H_0, ainsi que uTu^{-1}, il existe d'après le théorème de conjugaison appliqué à H_0 un $v \in H_0$ tel que vu normalise T, on est ramené à prouver que $vu \in H_0$. Or $w = vu$ centralise s et normalise T, donc w_s et w_u ont les mêmes propriétés ; on est ramené à prouver que w_s et w_u sont dans H_0. On l'a vu pour w_u ; pour w_s on utilise le fait qu'il existe une puissance q de p telle que $w_s^q \in H_0$ (car, H' désignant le groupe algébrique engendré par H_0 et u, les éléments w, donc w_s et w_u sont dans H', d'autre part H'/H_0 est cyclique d'ordre une puissance de p). Il en résulte que $x_s \in H_0$, car de la structure connue des groupes diagonalisables résulte aisément le fait suivant : si M est un groupe algébrique affine, t un élément semi-simple de M et q une puissance de la caractéristique p, il existe un t' semi-simple *unique* dans M tel que $t'^q = t$.

Remarque. – Contrairement à ce que pourraient faire croire ce dernier corollaire, et le corollaire au théorème 4, il n'est pas vrai en général que le centralisateur d'un élément semi-simple de G soit connexe (ni qu'une partie semi-simple commutative de G soit nécessairement contenue dans un tore), comme on voit par exemple en considérant la matrice diagonale $(-1, -1, +1, +1)$ dans $G = SO(4)$ (ou l'ensemble des matrices diagonales dans $SO(n)$).

7. Sous-groupes de Cartan, éléments réguliers. Groupes algébriques affines de dimension 1[1]

7.1 Sous-groupes de Cartan

La définition qui suit, valable pour tout "groupe abstrait", est due à Chevalley :

Définition 1. – *Soit G un groupe. On appelle sous-groupe de Cartan de G tout sous-groupe nilpotent maximal dont tout sous-groupe d'indice fini est d'indice fini dans son normalisateur.*

Dans le cas où G est un groupe algébrique, un sous-groupe de Cartan C est nécessairement fermé (puisque l'adhérence d'un groupe nilpotent est nilpotent) ; d'autre part, si C est un sous-groupe fermé de G, la condition "tout sous-groupe d'indice fini dans C est d'indice fini dans son normalisateur" équivaut à "C_0 est d'indice fini dans son normalisateur[2]". En effet, la première implique trivialement la seconde. Supposons réciproquement la seconde vérifiée, et soit H un sous-groupe d'indice fini dans C ; alors $\overline{H}$ est compris entre C_0 et C (d'après le théorème 1 du n° 3.1), et admet donc C_0 comme composante neutre ; donc le normalisateur de H, évidemment contenu dans celui de $\overline{H}$, est contenu dans celui de C_0, d'où résulte que $H \cap C_0$ est d'indice fini dans $N(H)$, et *a fortiori* H est d'indice fini dans $N(H)$.

Théorème 1. – *Soient G un groupe algébrique affine connexe, C un sous-groupe de G. Les conditions suivantes sont équivalentes :*

(i) *C est un sous-groupe de Cartan.*

(ii) *C est le centralisateur d'un tore maximal.*

(iii) *C est nilpotent et identique à son normalisateur connexe.*

En particulier, compte tenu du théorème de conjugaison (théorème 5, c) du n° 6.5) :

Corollaire. – *Les sous-groupes de Cartan de G sont connexes et conjugués entre eux.*

Démonstration du théorème 1. – Admettons un instant (iii) $\Rightarrow$ (ii) et prouvons (ii) $\Rightarrow$ (i) et (i) $\Rightarrow$ (iii). Soit C le centralisateur d'un tore maximal ; nous savons que C est nilpotent maximal et identique à son normalisateur

[1] Exposé de A. Grothendieck, le 14.01.1957

[2] Où C_0 désigne la composante neutre de C.

connexe (théorème 7, c) du n° 6.7) ; *a fortiori* il est d'indice fini dans son normalisateur, donc C est un sous-groupe de Cartan d'après ce qui a été dit plus haut. Supposons que C soit un sous-groupe de Cartan ; alors C est nilpotent et C_0 est d'indice fini dans son normalisateur, donc d'après (iii) $\Rightarrow$ (ii), C_0 est le centralisateur d'un tore maximal, donc un sous-groupe de Cartan et par suite nilpotent maximal ; on a donc $C = C_0$, et C est bien le centralisateur d'un tore maximal.

Reste donc à prouver (iii) $\Rightarrow$ (ii). Soit C un sous-groupe nilpotent de G identique à son normalisateur connexe ; prouvons que c'est le centralisateur d'un tore maximal. Soit B un sous-groupe de Borel de G contenant C ; C est un sous-groupe nilpotent de B identique à son normalisateur connexe dans B ; il suffit de prouver qu'il est le centralisateur dans B d'un tore maximal de B (car en vertu du théorème 7, d) du n° 6.7 et du théorème 5, c) du n° 6.5, c'est alors aussi le centralisateur d'un tore maximal de G). On est donc ramené au cas où G est *résoluble*. En vertu du théorème 3 du n° 6.3 et du théorème 4 du n° 6.4, on a $C = S \times C_u$ où $S = C_s$ est l'unique tore maximal de C, et si T désigne un tore maximal de G contenant S, on a $G = T \cdot G_u$ (produit semi-direct). Soit M le centralisateur connexe de S ; alors M contient T et il est donc de la forme $T \cdot M_u$ (théorème 4 du n° 6.4), où évidemment $M_u \supset C_u$; je dis qu'en fait $M_u = C_u$. Pour ceci admettons un instant le :

Lemme 1. – *Soit M un groupe affine nilpotent connexe, et soit N un sous-groupe connexe de M distinct de M. Alors N est distinct de son normalisateur connexe.*

Si l'on avait $M_u \neq C_u$, le normalisateur connexe N de C_u dans M_u serait donc $\neq C_u$, et alors $S \cdot N$ serait un groupe connexe non contenu dans C et normalisant C, contrairement à l'hypothèse sur C. Ainsi $C_u = M_u$; or M_u est évidemment normalisé par T (puisque T commute à S), donc C est normalisé par T et par suite $T \subset C$, d'où $S = T$, donc $C = S$. $C_u = T \cdot M_u$ est bien le centralisateur connexe (= le centralisateur) du tore maximal T.

Reste à démontrer le lemme. On procède par récurrence sur dim M, le cas où dim $M = 0$ étant clair. Soit dim $M = n > 0$; si N ne contient pas la composante neutre H du centre de M, le lemme est clair ; autrement on applique l'hypothèse de récurrence à M/H (qui est de dimension $< n$) et au sous-groupe N/H.

7.2 Eléments réguliers

Définition 2. – *Soit G un groupe. Un élément de G est dit régulier s'il est contenu dans un sous-groupe de Cartan et un seul de G.*

Théorème 2. – *Soient G un groupe algébrique affine connexe, g un élément de G. Les conditions suivantes sur g sont équivalentes :*

(i) *g est régulier* i.e. *(définition 2) g est contenu dans un sous-groupe de Cartan et un seul.*

(i bis) *L'ensemble des sous-groupes de Cartan contenant g est fini non vide.*

(ii) g_s *est contenu dans un seul tore maximal.*

(iii) *Le centralisateur connexe de* g_s *est de dimension minimum.*

(iv) *Le centralisateur connexe de* g_s *est un sous-groupe de Cartan.*

(v) *Le centralisateur connexe de* g_s *est nilpotent.*

Soit T un tore maximal contenant g_s (il en existe, d'après le théorème 6, c) du n° 6.6) et soit C son centralisateur (C est connexe, nilpotent, et c'est un sous-groupe de Cartan, d'après le théorème 1) ; C est contenu dans le centralisateur connexe $Z(g_s)_0$ de g_s. Comme il existe des éléments s de T tels que tout $x \in G$ satisfaisant à $xsx^{-1} \in T$ normalise C (*cf.* démonstration du théorème 6, a) du n° 6.6), et que $C = N(T)_0$, il existe des éléments dans T dont le centralisateur connexe est réduit à C. Donc la dimension minimum envisagée dans (iii) est celle de C, et (iii) équivaut à $Z(g_s)_0 = C$, donc à (iv) et à (v) (car un sous-groupe contenant un sous-groupe de Cartan C est un sous-groupe de Cartan si et seulement s'il est identique à C, ou encore si et seulement s'il est nilpotent !). D'ailleurs, les tores maximaux de G contenant g_s sont évidemment les tores maximaux de $Z(g_s)_0$, donc (ii) signifie que $Z(g_s)_0$ a un seul tore maximal, ce qui équivaut à (v) en vertu du corollaire 2 du théorème 5 du n° 6.5. Ainsi *les conditions* (ii), (iii), (iv) *et* (v) *sont équivalentes ; elles impliquent de plus* (i), car d'une part g appartient à $Z(g_s)_0$ (corollaire 2 du théorème 7 du n° 6.7 démontré tout exprès pour ça) donc à un sous-groupe de Cartan, d'autre part si g appartient à un sous-groupe de Cartan C, C est le centralisateur d'un tore maximal T en vertu du théorème 1, et comme $T = C_s$ on aura $g_s \in T$, donc T et par suite C est uniquement déterminé.

Comme (i) implique (i *bis*) trivialement, il reste à prouver que (i *bis*) implique que $Z(g_s)_0$ n'a qu'un seul tore maximal. Soit C un sous-groupe de Cartan contenant g ; alors $g \in C \subset Z(g_s)_0$, et, comme $Z(g_s)_0$ contient un sous-groupe de Cartan C, les sous-groupes de Cartan de $Z(g_s)_0$ sont des sous-groupes de Cartan de G, ce qui nous ramène au cas où $G = Z(g_s)_0$, *i.e.* au cas où g_s est dans le centre Z de G. Il est immédiat sur la définition 1 que les sous-groupes de Cartan de G sont les images réciproques des sous-groupes de Cartan de G/Z, donc l'image de g dans G/Z est un élément *unipotent* satisfaisant à (i *bis*), ce qui nous ramène à prouver ceci : si G est un groupe algébrique affine connexe ayant un élément unipotent $u = g$ satisfaisant à (i *bis*), G est nilpotent. Comme u est contenu dans un sous-groupe de Borel de G (théorème 6, b) du n° 6.6), et que les sous-groupes de Cartan de B sont des sous-groupes de Cartan de G (théorème 7, d) du n° 6.7) u satisfait à (i *bis*) *dans* B ; prouvons que B est nilpotent, il s'ensuivra que G l'est (corollaire 2 du théorème 5 du n° 6.5). Cela nous ramène au cas où G est résoluble. Soit $C = T \cdot C_u$ un sous-groupe de Cartan de G contenant u ; nous

voulons prouver $C_u = G_u$ (ce qui prouvera que G est nilpotent). Dans le cas contraire, en vertu du lemme 1 appliqué aux groupes nilpotents connexes G_u et C_u, le normalisateur connexe L de C_u dans G_u serait $\neq C_u$, et, comme $L \cap N(C) = C_u$, les vCv^{-1} pour $v \in L$ forment une *infinité* de sous-groupes de Cartan de G contenant u, contrairement à l'hypothèse. C.Q.F.D.

Corollaire 1. – *Pour que g soit régulier, il faut et il suffit que g_s le soit.*

Corollaire 2. – *Soit G un groupe algébrique affine connexe. L'ensemble des éléments réguliers de G est un ensemble ouvert dense dans G.*

Cette assertion résulte aussitôt de l'équivalence de (i) et (i *bis*), de l'existence d'éléments réguliers (visible sur la condition (iii)) et du corollaire au lemme 5 du n° 6.6 appliqué à $H = C$, compte tenu de ce que $N(C)_0 = C$.

Remarque. – Soit m le nombre de sous-groupes de Borel de G contenant un sous-groupe de Cartan C ; on verra plus tard que m est l'ordre du groupe de Weyl $N(C)/C$, mais dès maintenant il résulte facilement du théorème de conjugaison que les sous-groupes de Borel contenant C sont conjugués par des opérations du groupe de Weyl, en particulier il n'y en a qu'un nombre fini. Soit g un élément régulier de G, et soit C l'unique sous-groupe de Cartan le contenant ; alors les sous-groupes de Borel B contenant g sont exactement ceux contenant C (et il y en a donc exactement m). En effet, si B contient g, il contient g_s, donc l'*unique* tore maximal T de G contenant g_s, donc aussi $C = Z(T)$ en vertu du théorème 7, d) du n° 6.7. Dans le cas où G est semi-simple, on peut démontrer la réciproque, du moins si g est semi-simple (condition d'ailleurs nécessaire, dans ce cas, pour que g soit régulier, comme nous verrons plus tard) : si g est contenu dans exactement m sous-groupes de Borel, et est semi-simple, il est régulier. (Résulte facilement du fait qu'un tore maximal est alors l'intersection des sous-groupes de Borel de G qui le contiennent.)

7.3 Théorèmes de conservation

Théorème 3. – a) *Soit f un homomorphisme d'un groupe algébrique affine connexe G sur un autre G'. Alors les sous-groupes de Borel* (resp. les tores maximaux, resp. les sous-groupes de Cartan) *de G' sont les images par f des sous-groupes de Borel* (resp. ...) *de G,*

b) *L'application f transforme élément régulier en élément régulier.*

c) *Soit H un sous-groupe connexe invariant de G. Alors les sous-groupes de Borel* (resp. les tores maximaux) *de H sont les composantes neutres des intersections avec H de certains sous-groupes de Borel* (resp. tores maximaux) *de G.*

La dernière assertion est triviale, car un sous-groupe de Borel (resp. un tore maximal) de H est contenu dans un sous-groupe de Borel (resp. un tore maximal) de G, donc contenu dans la composante neutre de l'intersection de ce dernier avec H, donc identique à cette intersection en vertu de son caractère maximal. Pour la première assertion, il suffit de prouver que f transforme un sous-groupe de Borel (resp. ...) en un sous-groupe de Borel (resp. ...), les théorèmes de conjugaison impliquant alors qu'on obtient ainsi tous les sous-groupes de Borel (resp. ...) de G'.

Soit B un sous-groupe de Borel de G, et posons $B' = f(B)$; on a une application régulière surjective $G/B \to G'/B'$; comme G/B est complète (théorème 5, b) du n° 6.5) il en est de même de G'/B', donc B' contient un sous-groupe de Borel de G' (*loc. cit.*), et étant lui-même résoluble et connexe est un sous-groupe de Borel. Soient T un tore maximal de G, B un sous-groupe de Borel de G contenant T ; posons $T' = f(T)$, $B' = f(B)$. Pour prouver que T' est un tore maximal de G', il suffit de prouver que c'est un tore maximal du sous-groupe de Borel B', ce qui nous ramène au cas où G est résoluble. Mais alors on a $G = T \cdot G_u$ (théorème 4 du n° 6.4) d'où $f(G) = f(T) \cdot f(G_u)$, ce qui prouve que $f(T)$ est un tore maximal du groupe résoluble $G' = f(G)$. Soit enfin C le centralisateur de T dans G, et prouvons que son image C' est le centralisateur de T' dans g' ; utilisant le théorème 7, d) du n° 6.7 on est encore ramené au cas où $G = B$, $G' = B'$, *i.e.* où G est résoluble. Il faut montrer que si g est tel que $f(g)$ centralise $f(T)$, alors on a $f(g) \in f(C)$. L'hypothèse signifie que $gTg^{-1} \subset H$, où $H = f^{-1}(T')_0$; en vertu du théorème de conjugaison appliqué aux deux tores maximaux T, gTg^{-1} de H, il existe $h \in H$ tel que $hTh^{-1} = gTg^{-1}$ *i.e.* tel que $g^{-1}h = x$ normalise T, donc soit dans C (corollaire 3 du théorème 2 du n° 6.2), d'où résulte aussitôt que $f(g) = f(h)\, f(x)^{-1}$ est dans $f(C)$.

Soit g un élément régulier de G ; prouvons que $g' = f(g)$ est régulier. Comme $f(g)_s = f(g)_s$ et qu'un élément est régulier si et seulement si sa partie semi-simple l'est (corollaire 1 du théorème 2), on peut supposer g semi-simple. Soit N le noyau de f ; l'application f se factorise en $G \to G/N_0 \to G'$ (N_0 est la composante neutre de N), ce qui nous ramène à envisager séparément le cas où N est connexe, et celui où N est fini.

a) *N est connexe.* Soit S un tore maximal de G' contenant g' (théorème 6, c) du n° 6.6), soit $H = f^{-1}(S)$; c'est un groupe affine *connexe*, et d'après la première partie du théorème 3, il contient un tore maximal de G s'appliquant sur S, donc par conjugaison tous les tores maximaux de H sont maximaux dans G et s'appliquent sur S. On sait que l'un d'eux contient l'élément semi-simple g (*loc. cit.*) ; or g étant régulier est contenu dans un unique tore maximal T, et comme $S = f(T)$ il n'y a qu'un seul tore maximal de G' contenant g', *i.e.* g' est régulier dans G' (théorème 2).

b) *N est fini.* Alors, G étant connexe, N est nécessairement dans le centre de G, donc les sous-groupes de Cartan de G sont les images réciproques des

sous-groupes de Cartan de G', et la conclusion résulte aussitôt de la définition des éléments réguliers.

7.4 Groupes affines de dimension 1

Théorème 4. – *Soit G un groupe algébrique affine connexe de dimension* 1. *Alors G est isomorphe à K ou à K^*.*

Supposons que G ne soit pas isomorphe à K^*. Alors pour des raisons de dimension, un tore maximal de G est réduit à l'élément neutre, donc (corollaire 3 du théorème 5 du n° 6.5) G est nilpotent et $G = G_u$. Comme le groupe des commutateurs de G est connexe et $\neq G$, il est réduit à 0, donc G est *abélien* unipotent. D'après la démonstration du théorème 2 du n° 6.2, G admet une représentation rationnelle non triviale dans K ou K^*, et comme G est unipotent c'est donc une représentation f de G dans K, de noyau N *fini* puisque G est de dimension 1 et $f \neq 0$. Si la caractéristique est nulle, le groupe fermé engendré par $g \in G$, $g \neq 0$ est isomorphe à K (proposition 4 du n° 4.4), donc G est isomorphe à K. On peut donc supposer la caractéristique $p \neq 0$. Alors le noyau N de f est un p-groupe (*loc. cit.*, compte tenu que $G = G_u$).

Nous allons prouver que G/N est isomorphe à K, puis en conclure que G est isomorphe à K par récurrence sur l'entier n tel que N soit d'ordre p^n, ce qui nous ramène à prouver les deux lemmes suivants :

Lemme 2. – *Soit G un groupe algébrique connexe affine admettant une représentation rationnelle bijective x dans le groupe K. Alors G est isomorphe à K.* (Mais en général x n'est pas un isomorphisme !)

Lemme 3. – *Soit G un groupe algébrique affine connexe abélien unipotent admettant un sous-groupe N d'ordre p tel que G/N soit isomorphe à K. Alors G est isomorphe à K.*

Démonstration du lemme 2. – En vertu du corollaire 4 du théorème 1 du n° 5.2, le corps $K(G)$ des fonctions rationnelles sur G est une extension algébrique finie purement inséparable du corps des fonctions rationnelles sur $G' = K$, qui s'identifie à l'extension transcendante pure $K(x)$ de K engendrée par l'élément x de $K(G)$. Ainsi $K(G)$ est une extension radicielle de $K(x)$, son degré sur $K(x)$ est de la forme p^n ; or il est bien connu que, K étant un corps algébriquement clos, il existe à un isomorphisme près une extension radicielle L et une seule de degré p^n de $K(x)$, savoir $K(x)^{p^{-n}} = K(x^{p^{-n}})$. (Pour le voir, une récurrence immédiate nous ramène au cas où $n = 1$, mais alors $K(x) \subset L \subset K(x)^{p^{-1}}$, et comme $K(x)^{p^{-1}}$ est de degré p sur $K(x)$, car $K(x)$ est de degré p sur $K(x)^p = K(x^p)$, on a nécessairement $L = K(x)^{p^{-1}}$.) Ainsi $x^{p^{-n}}$ est un générateur de $K(G)$ sur K ; or x étant une fonction régulière sur G, il en est de même de $x^{p^{-n}}$ (puisque G est normal), qui est donc

une représentation rationnelle de G dans $G' = K$, bijective et birationnelle. Comme G' est normale, c'est donc en vertu du Main Theorem (théorème 2 du n° 5.3) un isomorphisme de variétés algébriques, donc un isomorphisme de groupes algébriques.

Démonstration du lemme 3. – Soit x un isomorphisme de G/N sur K ; alors $K(G/N)$ s'identifie à $L = K(x)$, et $M = K(G)$ en est une extension galoisienne de groupe de Galois N. De façon générale, si un groupe fini N opère dans une variété G, de telle façon que toute orbite de N soit contenue dans un ouvert affine, il est facile de définir la variété quotient G/N, par la condition que sa topologie soit la topologie quotient, et que les fonctions régulières sur un ouvert soient les fonctions régulières invariantes sous N sur l'ouvert image réciproque. Et on prouve aisément que les fonctions rationnelles sur G/N s'identifient alors aux fonctions rationnelles sur G invariantes par N, de sorte que $K(G)$ est une extension galoisienne de $K(G/N)$, ayant N pour groupe de Galois. Ici N est isomorphe à $\mathbf{Z}/(p) = \mathbf{Z}/p$ une fois choisi un générateur σ de N. En vertu de la théorie de Galois des extensions galoisiennes de degré p ("extensions d'Artin-Schreier"), une telle extension M de L s'obtient en adjoignant à L une racine d'une équation de la forme $X^p - X = u$, où u est un élément de L tel que cette équation soit irréductible, *i.e.* non de la forme $v^p - v$ ($v \in L$). (Ceci résulte de $\mathrm{Tr}_{M/L} 1 = p \cdot 1 = 0$, qui implique en vertu d'un théorème bien connu de Hilbert qu'on peut trouver $f \in M$ telle que $\sigma(f) - f = 1$, et posant alors $u = f^p - f$, on aura $u \in L$.) D'ailleurs, l'extension M ne change pas si on remplace u par $u + u'$, où u' est de la forme $v^p - v$ ($v \in L$). Dans le cas actuel, le groupe N opérant sans points fixes dans G, G/N est non ramifié dans M (corollaire 3 du théorème 1 du n° 5.2). On en conclut facilement qu'on peut choisir u fonction *régulière* sur G/N, soit directement en utilisant le fait que $G/N = K$, et la décomposition canonique des fonctions rationnelles en "éléments simples" ; soit mieux en invoquant la suite exacte générale, donnant le groupe $H^1(X, \mathbf{Z}/p)$ des revêtements non ramifiés (irréductibles ou non) d'une variété normale X, à l'aide du groupe $H^0(X, \mathcal{O})$ des fonctions régulières sur X, du groupe $H^1(X, \mathcal{O})$ ($\mathcal{O}$ désigne le faisceau des anneaux locaux sur X), et de l'opération déduite de l'endomorphisme $f \to f^p - f$ du faisceau $\mathcal{O}$:

$$0 \to \mathbf{Z}/p \to H^0(X, \mathcal{O}) \to H^0(X, \mathcal{O}) \to H^1(X, \mathbf{Z}/p) \to H^1(X, \mathcal{O}) \to H^1(X, \mathcal{O})$$

(cette suite exacte s'établit élémentairement à l'aide de la théorie d'Artin-Schreier, et du critère de non-ramification par le discriminant, donné dans l'exposé 5). Dans le cas actuel, $X = G/N = K$ est une variété *affine*, donc $H^1(X, \mathcal{O}) = 0$ ce qui implique bien qu'on peut prendre $u \in H^0(X, \mathcal{O})$.

Utilisons le fait que G est un groupe ; le diagrammme

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ \downarrow & & \downarrow \\ X \times X & \xrightarrow{h} & X \end{array}$$

(où $X = G/N$, les morphismes horizontaux étant donnés par les lois de groupe) définit un homomorphisme du revêtement produit $G \times G$ de $X \times X$ dans le revêtement image réciproque du revêtement G par h, compatible avec l'homomorphisme $\mathbf{Z}/p \times \mathbf{Z}/p \to \mathbf{Z}/p$ des groupes structuraux. Si D est le noyau de ce dernier homomorphisme, on en conclut un isomorphisme du revêtement $G \times G/D$ de $X \times X$ sur le revêtement $h^{-1}(G)$. Or ces revêtements sont définis respectivement par les fonctions $u(x) + u(y)$ et $u(h(x, y)) = u(x + y)$ sur $X \times X$, comme le montre un calcul immédiat. On a donc :

$$(*) \qquad u(x + y) - u(x) - u(y) = w(x, y)^p - w(x, y)$$

où w une fonction régulière sur $X \times X$. Supposons maintenant que u, qui est un polynôme en x, soit choisi de façon que son degré n soit minimum ; évidemment on a $n \geq 1$, et prouvons $n = 1$. Tout d'abord n n'est pas multiple de p, car si le terme dominant de u était ax^{mp}, ou pourrait remplacer u par $u' = u - ((bx^m)^p - bx^m)$, où $b \in K$ est tel que $b^p = a$, et on aurait $\deg u' < \deg u$. Si on avait $n \neq 1$, le premier membre de $(*)$ serait un polynôme de degré n exactement, tandis que le deuxième membre est de degré multiple de p, ce qui est absurde. On a donc $u = ax + b$, et on peut le remplacer par $u = ax$. Ainsi, $K(G)$ est engendré sur $K(x)$ par une fonction régulière f telle que $f^p - f = ax$, et il en résulte qu'on a en fait $K(G) = K(f)$. Je dis que f est un homomorphisme de groupes, *i.e.* qu'on a $f(g + g') - f(g) - f(g') = 0$ pour $g, g' \in G$. En effet, si le premier membre est noté $F(g, g')$, on aura $F(g, g')^p - F(g, g') = ax(g + g') - ax(g) - ax(g') = 0$ puisque x est un homomorphisme de groupes, et cela prouve que $F(g, g')$ prend ses valeurs dans le groupe à p éléments engendré par $1 \in K$, donc est constante ($G \times G$ étant connexe), donc nulle comme on voit en faisant $g = g' = 0$. Ainsi f est un homomorphisme régulier et birationnel de G dans K, donc un isomorphisme en vertu du Main Theorem.

8. Espaces homogènes de groupes algébriques[1]

8.1 Cohomomorphisme d'une application rationnelle

Soient U et V des variétés, f une fonction (rationnelle) sur U à valeurs dans V ; c'est un morphisme dans V d'une sous-variété ouverte D de U ; pour toute partie A de U, nous poserons $f(A) = f(D \cap A)$. L'ensemble $B = f(U)$ est une partie irréductible de V ; nous désignerons par $\mathfrak{o}$ son anneau local et par $\mathfrak{p}$ l'idéal maximal de $\mathfrak{o}$; $\mathfrak{o}$ est donc l'ensemble de celles des fonctions numériques (*i.e.* à valeurs dans le corps de base K) v sur V qui sont définies en au moins un point de $f(U)$, et $\mathfrak{p}$ est l'ensemble des $v \in \mathfrak{o}$ tels que $v(y) = 0$ pour tout $y \in f(U)$ en lequel v est définie. Soit g une fonction sur V à valeurs dans W, définie en au moins un point de $f(U)$; l'ensemble U_1 des $x \in U$ tels que f soit définie en x et g en $f(x)$ est ouvert non vide, et l'application $x \to g(f(x))$ de U_1 dans W se prolonge d'une manière et d'une seule en une fonction sur U à valeurs dans W ; nous désignerons cette fonction par $g \odot f$, et nous l'appellerons la *fonction composée de g et de f*. Nous exprimerons le fait que g est définie en au moins un point de $f(U)$ en disant que *g est composable avec f*. Il en est toujours ainsi dans le cas où $f(U)$ est dense dans V. Appliquons ce qui précède au cas où $W = K$ (le corps de base). Les fonctions numériques (ou fonctions rationnelles) sur V composables avec f sont celles qui appartiennent à $\mathfrak{o}$; l'application $v \to v \odot f$ de $\mathfrak{o}$ dans le corps F_U des fonctions numériques sur U est un homomorphisme φ qu'on appelle le *cohomomorphisme* de f (pour toute variété U, nous noterons systématiquement F_U le corps des fonctions numériques[2] sur U) ; le noyau de φ est $\mathfrak{p}$. Réciproquement, on montre que, si E est une partie irréductible fermée de V, $\mathfrak{o}$ son anneau local, $\mathfrak{p}$ l'idéal maximal de $\mathfrak{o}$ et φ un homomorphisme $\mathfrak{o} \to F_U$ de noyau $\mathfrak{p}$ (il s'agit toujours d'homomorphismes des structures d'algèbre sur K), il existe une fonction f et une seule sur U à valeurs dans V de cohomomorphisme φ ; $f(U)$ est une partie dense de E. Pour que f soit définie en un point $x \in U$, il faut et il suffit qu'il existe un $y \in E$ tel que φ applique l'anneau local $\mathfrak{o}(y)$ de y (qui est automatiquement contenu dans $\mathfrak{o}$) dans l'anneau local de x ; le point y est alors uniquement déterminé par cette condition et l'on a $f(x) = y$. Si g est une fonction sur V à valeurs dans W, composable avec f, et γ son

[1] Exposé de C. Chevalley, le 28.1.1957

[2] Ce corps est aussi noté $K(U)$ si l'on veut mentionner explicitement le corps de base K (toujours supposé algébriquement clos). C'est ce que l'on a fait précédemment.

cohomomorphisme, l'application $\varphi \circ \gamma$ prolonge le cohomomorphisme de $g \odot f$ et lui est égale si $f(U)$ est dense dans V.

Proposition 1. – *Soit f une fonction sur une variété U à valeurs dans une variété V telle que $f(U)$ soit dense dans V, et soit φ son cohomomorphisme. Soit u une fonction numérique sur U. Les conditions suivantes sont alors équivalentes :*

a) *u est radicielle sur $\varphi(F_V)$;*

b) *il existe un ouvert non vide Ω de U contenu dans les ensembles de définition de u et de f tel que l'on ait $u(x) = u(x')$ toutes les fois que $x, x' \in \Omega$ sont tels que $f(x) = f(x')$.*

Supposons a) satisfaite ; soit q une puissance de l'exposant caractéristique de K telle que $u^q = \varphi(v)$, avec $v \in F_V$. L'ensemble Ω des $x \in U$ tels que f et u soient définies en x et v en $f(x)$ est ouvert non vide ; si x, $x' \in \Omega$ sont tels que $f(x) = f(x')$, on a $u^q(x) = v(f(x)) = u^q(x')$, d'où $u(x) = u(x')$.

Supposons réciproquement b) satisfaite. Soit h la fonction sur U à valeurs dans $V \times K$ telle que $h(x) = (f(x), u(x))$ si f et u sont définies en x, en particulier pour $x \in \Omega$; $h(\Omega)$ est épais et contient une partie relativement ouverte non vide W de son adhérence. La projection de $V \times K$ dans V induit un morphisme f' de W dans V ; il est clair que f' est injectif et que $f'(W)$ est dense dans V. Il existe une partie relativement ouverte W' de W, non vide, telle que, pour tout $z' \in W'$, W' soit normale en z' et V normale en $f'(z')$: remplaçant au besoin W' par une partie ouverte non vide plus petite, on peut supposer que $f'(W')$ est une sous-variété ouverte normale V' de V. Soit φ'_1 le cohomomorphisme de la restriction de f' à W' ; pour tout $y' \in V'$, ${f'}^{-1}(y)$ se compose d'un seul point ; il résulte alors de ce qui a été dit antérieurement (corollaire 2 au théorème 2 du n° 5.3) que $F_{W'}$ est algébrique et radiciel sur $\varphi'_1(F'_{V'})$. En particulier, la projection de $V \times K$ sur K induit sur W' une fonction numérique qui est radicielle sur $\varphi'_1(F_{V'})$. Il existe donc une fonction numérique v sur V et une puissance q de l'exposant caractéristique telles que $u^q(x) = v(f(x))$ pour tout $x \in U$ tel que f et u soient définis en x et $(f(x), u(x)) \in W'$; ces points x formant un ouvert non vide de U, on a $u^q = \varphi(v)$ par continuité. C.Q.F.D.

8.2 Variétés quotients

Définition 1. – *Soient f un morphisme d'une variété U dans une variété V et φ son cohomomorphisme. Supposons les conditions suivantes satisfaites : on a $f(U) = V$; tout élément de F_U radiciel sur $\varphi(F_V)$ appartient à ce corps ; si v est une fonction numérique sur V et si $\varphi(v)$ est définie en un point $x \in U$, alors v est définie en $f(x)$. On dit alors que V est une variété quotient de U par f.*

Théorème 1. – *Soit f un morphisme d'une variété U dans une variété V telle que V soit variété quotient de U par f. Soit g une fonction sur U à valeurs dans une variété W ; supposons qu'il existe un ouvert $\Omega \neq \varnothing$ de U contenu dans l'ensemble de définition de g tel que les conditions x, $x' \in \Omega$, $f(x) = f(x')$ entraînent $g(x) = g(x')$. Alors il existe une fonction*[3] *h et une seule sur V à valeurs dans W telle que $g = h \odot f$; si $x \in U$, h est définie en $f(x)$ si et seulement si g est définie en x.*

Si D est l'ensemble de définition de g, $f(D)$ est épais et dense dans V ; si donc h, h' sont des solutions du problème, elles coïncident sur un ouvert non vide de V, ce qui démontre l'unicité. Pour démontrer l'existence et la dernière assertion, on peut supposer sans restriction de généralité que $g(U)$ est dense dans W. Soient φ et γ les cohomomorphismes de f et g respectivement ; soit $w \in F_W$; si $x, x' \in \Omega$ sont tels que $f(x) = f(x')$ et que w soit défini en $g(x) = g(x')$, on a $(\gamma(w))(x) = (\gamma(w))(x')$; tenant compte de la définition des variétés quotients et de la proposition 1, on voit que $\gamma(w) \in \varphi(F_V)$; il existe donc un isomorphisme η de F_W sur un sous-corps de F_V tel que $\gamma = \varphi \circ \eta$. C'est le cohomomorphisme d'une fonction h sur V à valeurs dans W telle que $g = h \odot f$. Si h est définie en $f(x)$, g l'est en x.

Supposons réciproquement g définie en x, et soit $z = g(x)$; soit w une fonction de l'anneau local $\mathfrak{o}(z)$ de z ; alors $\varphi(\eta(w)) = \gamma(w)$ est définie en x, donc $\eta(w)$ est définie en $f(x)$ par la définition des variétés quotients ; comme $\eta(\mathfrak{o}(z))$ est contenu dans l'anneau local de $f(x)$, h est définie en $f(x)$.

Corollaire. – *Les notations étant celles du théorème* 1*, si g est définie en x, elle est définie en tout point de $f^{-1}(f(x))$ et est constante sur cet ensemble*[4].

Proposition 2. – *Soit f un morphisme d'une variété U dans une variété V tel que V soit variété quotient de U par f. Soit g un morphisme de V dans une variété W, et soit $h = g \circ f$. Pour que W soit variété quotient de U par h, il faut et suffit que W soit variété quotient de V par g.*

Nous laissons au lecteur le soin de faire la démonstration, qui est facile.

Théorème 2. – *Soit f une fonction sur une variété U à valeurs dans une variété V ; supposons que $f(U)$ soit dense dans V et que, φ désignant le cohomomorphisme de f, tout élément de F_U radiciel sur $\varphi(F_V)$ soit dans $\varphi(F_V)$. Il existe alors une sous-variété ouverte U' de U contenue dans le domaine de définition de f et telle que, f' désignant la restriction de f à U', $f'(U')$ soit une sous-variété ouverte V' de V et que V' soit variété quotient de U' par f'.*

---

[3] En particulier, supposons que $g : U \to W$ soit un *morphisme* et que la relation $f(x) = f(x')$ entraîne $g(x) = g(x')$ pour x, x' dans U. Alors il existe un *morphisme* $h : V \to W$ tel que $g = h \circ f$.

[4] De manière plus précise, le domaine de définition U' de g est de la forme $f^{-1}(V')$ où V' est un ouvert non vide de V, le domaine de définition de h est égal à V', et l'on a $g = h \circ f$ sur U'.

Remplaçant U par une sous-variété ouverte, on peut supposer que f est un morphisme. Tenant compte du théorème 4 de l'exposé 8 de **SCC** et de la remarque qui suit la démonstration de ce théorème, on voit qu'il existe une sous-variété ouverte V' de V qui possède la propriété suivante : si $y \in V'$, $x \in U$, $y = f(x)$, et si Y est une sous-variété fermée de V passant par y, il existe une sous-variété fermée X de U passant par x telle que $f(X)$ soit dense dans Y. On peut de plus supposer V' normale et contenue dans $f(U)$. On pose $U' = f^{-1}(V')$. Or on a le lemme suivant :

Lemme 1. – *Soient V une variété, y un point de V en lequel V est normale et v une fonction numérique sur V non définie en y. Il existe alors une sous-variété Y de V passant par y telle que v^{-1} soit définie en au moins un point de Y et prenne la valeur 0 en tout point de Y où elle est définie*[5].

Soit $\mathfrak{o}$ l'anneau local de V en y ; les $a \in \mathfrak{o}$ tels que $av \in \mathfrak{o}$ forment un idéal $\mathfrak{a} \neq \mathfrak{o}$; soit $\mathfrak{p}$ un idéal premier minimal de $\mathfrak{a}$ et soit $\mathfrak{O} = \mathfrak{o}_{\mathfrak{p}}$ son anneau local. Si $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$ sont les idéaux premiers minimaux $\neq \mathfrak{p}$ de $\mathfrak{a}$, il existe un exposant $n > 0$ tel que $\mathfrak{p}^n \cdot \mathfrak{p}_2^n \ldots \mathfrak{p}_r^n \subset \mathfrak{a}$, d'où $\mathfrak{p}^n\,\mathfrak{O} \subset \mathfrak{a}\,\mathfrak{O}$ puisque $\mathfrak{p}_i\,\mathfrak{O} = \mathfrak{O}$ si $i > 1$. Soit donc k le plus petit exposant ≥ 0 tel que $\mathfrak{p}^k\,v \subset \mathfrak{O}$; on a $k > 0$. Soit $v' \in \mathfrak{p}^{k-1}\,v$, $v' \notin \mathfrak{O}$, d'où $\mathfrak{p}\,v' \subset \mathfrak{O}$. Si l'on avait $\mathfrak{p}\,v' \subset \mathfrak{p}\,\mathfrak{O}$, la multiplication par v' donnerait un endomorphisme du $\mathfrak{O}$-module de type fini $\mathfrak{p}\,\mathfrak{O}$; alors v' serait entier sur $\mathfrak{O}$; mais c'est impossible, car, $\mathfrak{o}$ étant normal, il en est de même de $\mathfrak{O}$ et v' n'est pas entier sur $\mathfrak{O}$ puisque $v' \notin \mathfrak{O}$. Donc $\mathfrak{p}\,v'$ contient un élément inversible de $\mathfrak{O}$, et $v'^{-1} \in \mathfrak{O}$. On a $v'^{-1} \in \mathfrak{p}\,\mathfrak{O}$, d'où $\mathfrak{p}\,\mathfrak{O} = v'^{-1}\,\mathfrak{O}$ puisque $\mathfrak{p}\,v' \subset \mathfrak{O}$. On voit alors que vv'^{-k} est un élément inversible de $\mathfrak{O}$, d'où $v^{-1} \in \mathfrak{O}$. Il correspond à $\mathfrak{p}$ une sous-variété Y de V passant par y ; son anneau local est $\mathfrak{O}$; puisque $v^{-1} \in \mathfrak{O}$, v^{-1} est définie en au moins un point de Y ; comme $v^{-1} \in \mathfrak{p}\,\mathfrak{O}$, v^{-1} est nulle en tout point de Y où elle est définie.

Ceci dit, démontrons le théorème 2. Soit $f' : U' \to V'$ la restriction de f, d'où $f'(U') = V'$. Soit y un point de V' et soit v une fonction numérique sur V non définie en y. Soit Y une sous-variété fermée de V passant par y qui possède les propriétés du lemme 1 ; soit x un point quelconque de U' avec $f'(x) = y$. Il passe par x une sous-variété fermée X de U telle que $f(X)$ soit dense dans Y. Soit $u = \varphi(v)$; il existe un ensemble X' ouvert dense dans X tel que u^{-1} soit définie et nulle en tous les points de X' ; cela signifie que u^{-1} appartient à l'idéal maximal de l'anneau local de X, ce qui implique manifestement que u n'est pas définie en x. Ceci établit le théorème 2.

Remarque. – On peut montrer que si $x \in U$ est tel que V soit normale en $f(x)$ et que toute composante de $f^{-1}(f(x))$ passant par x soit de dimension $\dim U - \dim V$, alors on peut prendre U' contenant x ; nous n'utiliserons pas ce résultat plus précis.

[5] Autrement dit, si V est normale, le complémentaire de l'ensemble de définition de $v \in F_V$ est réunion des variétés polaires de v ; l'hypothèse que V est normale est essentielle.

8.3 Existence de variétés quotients

Soit f une application d'une variété U sur un ensemble A. S'il existe sur A une structure de variété qui soit variété quotient de U par f, il n'en existe qu'une, comme il résulte tout de suite du théorème 1 ; on dit alors qu'il existe une variété quotient de U par f. Dans l'énoncé suivant, nous appellerons *partie tubulaire* (pour f) de U toute sous-variété ouverte T de U telle qu'il existe une variété quotient de T par la restriction de f à T.

Proposition 3. – *Soit f une application surjective d'une variété U sur un ensemble A. Supposons que, si x et x' sont des points quelconques de U, il existe toujours une partie tubulaire de U (pour f) contenant x et x'. Il y a alors une variété quotient de U par f.*

Pour toute partie tubulaire T, soit f_T la restriction de f à T, et soit A_T l'ensemble $f(T)$ muni de sa structure de variété quotient de T ; soient φ_T le cohomomorphisme de f_T, et $G_T = \varphi_T(F_{A_T})$. Montrons que les corps G_T sont tous égaux. Soient T et T' des parties tubulaires et $u \in G_T$; si D est l'ensemble de définition de u, $D \cap T \cap T'$ est un ouvert non vide de U, et si x, x' sont des points de cet ensemble tels que $f(x) = f(x')$, on a $u(x) = u(x')$ (corollaire au théorème 1). Il en résulte, en vertu de la proposition 1 et de la définition 1 des variétés quotients, que l'on a $u \in G_{T'}$; on a donc $G_T \subset G_{T'}$, ce qui montre que les corps G_T sont tous égaux. Soit G leur valeur commune, et soit Σ l'ensemble des intersections avec G des localités de F_U qui appartiennent au schéma de U. Si E est une partie irréductible d'une partie tubulaire T, on a, en désignant par $\mathfrak{o}(E)$ et $\mathfrak{o}(f_T(E))$ les anneaux locaux de E et de $f_T(E)$ respectivement, $\varphi_T(\mathfrak{o}(f_T(E))) = \mathfrak{o}(E) \cap G$. En effet, soit v une fonction numérique sur A_T ; si v est définie en au moins un point de $f_T(E)$, $\varphi_T(v)$ est définie en au moins un point de E, et la réciproque est vraie puisque A_T est variété quotient de T par f_T. Les éléments de Σ sont donc des localités de G. Comme U est un espace nœthérien, il peut être couvert par un nombre fini de parties tubulaires, ce qui montre que Σ est réunion finie de schémas affines (on se rappellera que, si E est une partie irréductible de U, $\mathfrak{o}(E) = \mathfrak{o}(E \cap T)$ si E rencontre la partie tubulaire T). Soient $\mathfrak{r} = \mathfrak{o}(E) \cap G$, $\mathfrak{r}' = \mathfrak{o}(E') \cap G$ des éléments de Σ, E et E' étant des parties irréductibles de U ; il y a par hypothèse une partie tubulaire T qui rencontre E et E' ; $\mathfrak{r}$ et $\mathfrak{r}'$ sont donc images par φ_T de localités du schéma de A_T et sont par suite identiques ou non apparentées ; Σ est donc un schéma. Si $y \in A$, les intersections avec G des anneaux locaux des points de $f^{-1}(y)$ sont toutes égales, comme il résulte immédiatement du fait que deux quelconques de ces points sont dans une même partie tubulaire ; si $\mathfrak{o}_y$ est la valeur commune de ces intersections, on vérifie immédiatement que $y \to \mathfrak{o}_y$ est une bijection de A sur l'ensemble des localités de dimension 0 de Σ ; cette bijection définit sur A une structure de variété, qui est évidemment variété quotient de U par f.

8.4 Trace d'une fonction

Théorème 3. – *Soit f une fonction sur une variété U à valeurs dans une variété V ; supposons que $\dim U = \dim V$ et que $f(U)$ soit dense dans V. Il existe alors des sous-variétés ouvertes U', V' de U, V respectivement qui possèdent les propriétés suivantes : U' et V' sont normales ; la restriction f' de f à U' est un morphisme ; on a $V' = f'(U')$; pour tout $y \in V'$, $f'^{-1}(y)$ a toujours le même nombre d'éléments.*

On peut manifestement supposer U et V normales et affines, et que f est un morphisme ; soient P et Q les algèbres affines de U et V respectivement ; si φ est le cohomomorphisme de f, on a $\varphi(Q) \subset P$ puisque f est un morphisme. Comme $\dim U = \dim V$, F_U est algébrique sur le corps des fractions $\varphi(F_V)$ de $Q' = \varphi(Q)$. Comme P est à engendrement fini, il y a un élément $v' \neq 0$ de Q' tel que $P\,[v'^{-1}]$ soit entier sur $Q\,[v'^{-1}]$. Remplaçant U et V par des sous-variétés ouvertes, on peut supposer que P est entier sur Q. La variété U est alors la variété normalisée de V relativement à l'isomorphisme φ de F_V sur un sous-corps de F_U, puisque P est la clôture intégrale de $\varphi(Q)$ dans F_U ; le résultat découle alors d'un résultat établi antérieurement (corollaire 2 au théorème 2 du n° 5.3). C.Q.F.D.

Soit f un morphisme d'une variété normale U dans une variété normale V ; supposons de plus que, pour tout $y \in V$, le nombre n des points de $f^{-1}(y)$ soit fini et toujours le même. Soit φ le cohomomorphisme de f ; supposons d'abord F_U séparable sur $\varphi(F_V)$. Soient y un point de V, $\mathfrak{o}(y)$ son anneau local, $\mathfrak{o}' = \varphi(\mathfrak{o}(y))$, $\mathfrak{O}$ la clôture intégrale de $\mathfrak{o}'$ dans F_U. Si $\mathfrak{p}'$ est l'idéal maximal de $\mathfrak{o}'$, $\mathfrak{p}'\,\mathfrak{O}$ est l'intersection de n idéaux maximaux $\mathfrak{p}_i$ $(1 \leq i \leq n)$ dont les anneaux locaux sont les anneaux locaux des points de $f^{-1}(y)$; $\mathfrak{O}/\mathfrak{p}'\,\mathfrak{O}$ est isomorphe à la somme directe de n corps identiques à K au moyen d'un isomorphisme qui applique tout $t \in \mathfrak{O}$ sur l'élément $(t(x_1), \ldots, t(x_n))$, où les x_i sont les points de $f^{-1}(y)$ (*cf.* théorème 1 du n° 5.2). Il existe des éléments $t_i \in \mathfrak{O}$ tels que $t_i(x_j) = \delta_{ij}$, et ces éléments forment une base de F_U sur $\varphi(F_V)$. Soit alors u une fonction numérique sur U définie en $x_1, \ldots, x_n$; calculant la trace $\operatorname{Tr} u$ de u par rapport à $\varphi(F_V)$ au moyen de la base $(t_1, \ldots, t_n)$, on voit tout de suite que $(\operatorname{Tr} u)(x_i) = \sum_{i=1}^{n} u(x_i)$. On en conclut que, *si u est une fonction régulière sur U, la formule :*

$$v(y) = \sum_{i=1}^{n} u(x_i) \qquad (\text{où } \{x_1, \ldots, x_n\} = f^{-1}(y))$$

définit une fonction régulière v sur V.

Ce résultat doit être modifié lorsque F_U n'est plus séparable sur $\varphi(F_V)$; il existe alors une variété normale U_1, un morphisme f_1 de U dans U_1 et un morphisme f_2 de U_1 dans V tels que, pour tout $x_1 \in U_1$, $f_1^{-1}(x_1)$ se compose d'un seul point, que, pour tout $y \in V$, $f_2^{-1}(y)$ se compose de n points, que

F_U soit radiciel sur l'image de F_{U_1} par le cohomomorphisme φ_1 de f_1 et F_{U_1} séparable sur l'image de F_V par le cohomomorphisme de f_2. Si q est le degré de F_U sur $\varphi_1(F_{U_1})$, et si u est une fonction régulière sur U, la formule $v(y) = \sum_{i=1}^{n} u^q(x_i)$ définit une fonction régulière sur V.

8.5 Application aux groupes : construction des espaces homogènes

Soient G un groupe algébrique connexe et H un sous-groupe fermé[6] de G. Pour tout $t \in H$, le cohomomorphisme de la translation à droite par t est un automorphisme τ_t du corps F_G ; soit R le corps des fonctions invariantes par les τ_t. Les fonctions de R sont appelées les fonctions H-invariantes (sur G).

Proposition 4. – *Si s, s' sont des points de G tels que $sH \neq s'H$, il existe une fonction de R qui est définie en s et s' et y prend des valeurs distinctes.*

Soit H_0 la composante neutre de H ; soient g et h les dimensions de G et H respectivement. Il existe une sous-variété (localement fermée) U de G de dimension $g - h$ passant par e telle que e soit un point isolé de $U \cap H_0$. Pour le prouver, établissons le :

Lemme 2. – *Soient U une variété de dimension m, x un point de U, $T_1, \ldots, T_r$ des sous-variétés de dimensions > 0 de U passant par x ; il existe alors une fonction numérique u sur U, définie en x, y prenant la valeur* 0, *qui n'induit* 0 *sur aucune des T_i.*

Soient $\mathfrak{o}$ l'anneau local de x, $\mathfrak{t}_i$ l'idéal premier de $\mathfrak{o}$ correspondant à T_i ; puisque $\dim T_i > 0$, les $\mathfrak{t}_i$ sont tous distincts de l'idéal maximal $\mathfrak{p}$ de $\mathfrak{o}$. Les $\mathfrak{t}_i$ étant des sous-espaces de la structure d'espace vectoriel de $\mathfrak{p}$ sur K (qui est infini), il existe un $u \in \mathfrak{p}$ qui n'appartient à aucun des $\mathfrak{t}_i$, d'où le lemme 2.

Si U' est une composante irréductible de l'ensemble des zéros de u qui passe par x, U' est de dimension $m - 1$ et, pour chaque i, $U' \cap T_i$ est de dimension $< \dim T_i$. Appliquons ceci à la situation qui nous occupe : on construit inductivement au moyen du lemme 2 une suite $(U_i)_{1 \leq i \leq h}$ de sous-variétés U_i de G passant par e telle que, pour tout i, toute composante irréductible de $U_i \cap H_0$ passant par e soit de dimension $h - i$; $U = U_h$ possède alors la propriété requise. On peut de plus manifestement supposer que U est affine.

L'application $(x, t) \to xt$ est un morphisme de $U \times H_0$ dans G, soit f ; le point (e, e) est isolé dans $f^{-1}(e)$; on a donc $\dim f(U \times H_0) = \dim(U \times H_0) = g - h + h = g$, et $f(U \times H_0)$ est dense dans G. Il existe alors une sous-variété ouverte normale W de $U \times H_0$ et une sous-variété ouverte (donc normale) G' de G telles que, pour tout $z \in G'$, $f'^{-1}(z)$ contienne le même

[6] Le sous-groupe H *n'est pas* supposé connexe, contrairement à G.

nombre n de points, où f' désigne la restriction de f à W (corollaire 4 du théorème 1 du n° 5.2). Soit u une fonction numérique partout définie sur U ; il existe un exposant q, puissance de l'exposant caractéristique de K, tel que la formule $v(z) = \sum_{i=1}^{n} u^q(x_i)$ (où $(x_1, t_1), \ldots, (x_n, t_n)$ sont les points de $f'^{-1}(z)$) définisse une fonction numérique v sur G, partout définie sur G' (*cf.* n° 8.4). *Cette fonction est toujours H_0-invariante.* Soit en effet z un point de G', et soient (x_i, t_i) $(1 \leq i \leq n)$ les points de $f'^{-1}(z)$; l'ensemble A des $t \in H_0$ tels que $(x_i, t_i\, t) \in W$ $(1 \leq i \leq n)$ est manifestement ouvert et non vide dans H_0 ; si $t \in A$, on a $zt \in G'$ et $f'^{-1}(zt)$ contient les points $(x_i, t_i\, t)$, qui sont en nombre n et qui sont par suite tous les points de $f'^{-1}(zt)$; on a donc $v(zt) = v(z)$ si $t \in A$. La fonction v est donc constante sur $zH_0 \cap G'$ (car zA est dense dans zH_0). Soit maintenant t un élément quelconque de H_0, et soit τ_t le cohomomorphisme de la translation à droite par t ; on a donc $v(z) = (\tau_t(v))(z)$ pour tout z tel que $z \in G'$, $zt \in G'$; comme les points z ayant ces deux propriétés forment un ouvert non vide de G, on a $v = \tau_t(v)$.

Ceci étant, soient $z_1, \ldots, z_\nu$ des points de G' tels que les ensembles $z_i\, H$ $(1 \leq i \leq \nu)$ soient tous distincts ; soient (x_{ik}, t_{ik}) $(1 \leq k \leq n)$ les points de $f'^{-1}(z_i)$, d'où $x_{ik} \in z_i\, H_0$; les points x_{ik} $(1 \leq i \leq \nu,\ 1 \leq k \leq n)$ sont donc tous distincts, et, comme U est affine, on peut trouver une fonction numérique u partout définie sur U qui prend en ces points des valeurs arbitrairement données. On en conclut qu'*il existe une fonction numérique v sur G qui est H_0-invariante et qui prend en les z_i des valeurs arbitrairement données.*

Soient maintenant s et s' des points de G tels que $sH \neq s'H$; soient $t_1, \ldots, t_m$ des représentants des classes de H suivant H_0 ; les $st_i\, H_0$, $s't_i\, H_0$ sont donc tous distincts. Les ouverts $G'(st_j)^{-1}$, $G'(s't_j)^{-1}$ se rencontrent[7], et il existe donc un $a \in G$ tel que les ast_j, $as't_j$ soient tous dans G'. Il existe une fonction H_0-invariante v_1 qui prend en tous ces points des valeurs arbitrairement données ; or, pour toute fonction H_0-invariante v_1, il est clair que $\sum_{j=1}^{m} \tau_{t_j}(v_1)$ est une fonction H-invariante ; choisissant convenablement les valeurs de v_1 en les ast_j, $as't_j$, on voit qu'il existe une fonction numérique v_2 sur G, qui est H-invariante, définie en as et as' et telle que $v_2(as) \neq v_2(as')$. Soit σ le cohomomorphisme de la translation à gauche par a ; σ commute donc avec les cohomomorphismes des translations à droite, et $v = \sigma(v_2)$ est H-invariante ; v est définie en s et s' et y prend des valeurs distinctes. Ceci établit la proposition 4.

Théorème 4. – *Soient G un groupe algébrique connexe et H un sous-groupe fermé de G (non nécessairement connexe) ; soit f l'application canonique de G sur l'ensemble G/H. Il existe alors une variété quotient de G par f ; si G/H est muni de cette structure de variété, et que φ désigne le cohomomorphisme de f, alors $\varphi(F_{G/H})$ est le corps R des fonctions H-invariantes sur G.*

[7] Par l'irréductibilité de G.

Il résulte immédiatement de la définition de R que tout élément de F_G qui est radiciel sur R est dans R. Soit X un modèle quelconque de R ; c'est une variété munie d'un isomorphisme φ' de F_X sur R. On peut considérer φ' comme un isomorphisme de F_X sur un sous-corps de F_G ; comme tel, c'est le cohomomorphisme d'une fonction f' sur G à valeurs dans X. Il résulte alors du théorème 2 que l'on peut choisir X de telle manière qu'il existe une sous-variété ouverte G' de G telle que, la restriction de f' à G' étant notée f'', X soit variété quotient de G' par f''. Soient s et s' des points de G' tels que $f''(s) = f''(s')$; il est alors clair que, pour toute fonction $v \in R$ définie en s et en s', on a $v(s) = v(s')$ (car $v = \varphi'(w)$, où w est une fonction numérique sur X qui est définie en $f''(s) = f''(s')$ puisque X est variété quotient de G' par f''). Il en résulte que $sH = s'H$ en vertu de la proposition 4. Soient réciproquement s et s' des points de G' tels que $sH = s'H$: soit $s' = st$ avec $t \in H$. Si v est une fonction de R définie en s', il résulte de la formule $v = \tau_t(v)$ (où τ_t est le cohomomorphisme de la translation à droite par t) que v est définie en s. Il en résulte que toute fonction numérique w sur X qui est définie en $f''(s')$ l'est en $f''(s)$, d'où $f''(s') = f''(s)$. Il y a donc une bijection j de X sur une partie de G/H telle que $j \circ f''$ soit la restriction de f à G' ; autrement dit, G' est une partie tubulaire relativement à f. Il est clair que, pour tout $a \in G$, aG' est encore tubulaire relativement à f. Or, soient s et s' des points quelconques de G ; comme $G's^{-1} \cap G's'^{-1} \neq \varnothing$ (car G est irréductible), il existe un $a \in G$ tel que as et as' soient dans G', de sorte que s et s' sont dans une partie tubulaire pour f. Il résulte alors de la proposition 3 qu'il existe une variété quotient de G par f ; la dernière assertion du théorème 4 résulte immédiatement de notre construction de G/H.

Remarque. – Les notations étant comme ci-dessus, on peut non seulement affirmer que tout élément de F_G radiciel sur R est dans R, mais que F_G est séparable sur R, en vertu du lemme suivant :

Lemme 3. – *Soient F un corps et R le corps des invariants d'un groupe Γ d'automorphismes de F. Alors F est séparable sur R.*

Soient en effet $x_1, \ldots, x_n$ des éléments de R tels que les $x_i^{1/p}$ soient linéairement dépendants sur F (dans une clôture algébrique de ce corps) ; nous voulons montrer qu'ils sont linéairement dépendants sur R. On se ramène tout de suite au cas où $x_1^{1/p}, \ldots, x_{n-1}^{1/p}$ sont linéairement indépendants sur F. Soient $a_1, \ldots, a_{n-1}$ dans F tels que $x_n^{1/p} = \sum_{i=1}^{n-1} a_i\, x_i^{1/p}$. Appliquant un automorphisme γ de Γ (qui se prolonge à $F^{1/p}$), et tenant compte de ce que les $x_i^{1/p}$ $(1 \leq i \leq n-1)$ sont linéairement indépendants sur F et invariants par γ, il vient $\gamma(a_i) = a_i$ $(1 \leq i \leq n-1)$; les a_i sont donc dans R, ce qui démontre le lemme 3.

8.6 Propriétés des espaces homogènes

Proposition 5. – *Soient H', H'' des sous-groupes fermés d'un groupe algébrique G tels que $H'' \subset H'$. Si f est l'application canonique de G/H'' sur G/H', la variété G/H' est variété quotient de G/H'' par f.*

Cela résulte immédiatement de la proposition 2.

Proposition 6. – *Soit G_i $(i = 1, 2)$ un groupe algébrique, et soit H_i un sous-groupe fermé de G_i ; soit f_i l'application canonique de G_i sur G_i/H_i. Soit m un morphisme de G_1 dans G_2 tel que $m(sH_1) \subset m(s)H_2$ pour tout $s \in G_1$; l'application $m^* : G_1/H_1 \to G_2/H_2$ telle que $m^* \circ f_1 = f_2 \circ m$ est un morphisme.*

Comme $f_2 \circ m$ est un morphisme, cela résulte du théorème 1.

La proposition 5 s'applique en particulier aux cas suivants :

a) m est un homomorphisme de G_1 dans G_2 tel que $m(H_1) \subset H_2$;

b) on a $G_1 = G_2$, $H_1 = H_2$ et m est la translation à gauche par un élément de G.

Dans le cas b), on voit que, si s est un élément d'un groupe algébrique G et H un sous-groupe fermé de G, l'application $x \to s \cdot x$ de G/H dans lui-même est un automorphisme de la variété G/H ($s \cdot x$ étant par définition stH si $x = tH$). Il en résulte immédiatement que tous les points de G/H sont simples.

Proposition 7. – *Soit G_i $(i = 1, 2)$ un groupe algébrique et soit H_i un sous-groupe fermé de G_i ; soit f_i l'application canonique $G_i \to G_i/H_i$. Soit $G = G_1 \times G_2$, $H = H_1 \times H_2$, et soit f l'application canonique $G \to G/H$; l'application g de G/H sur $(G_1/H_1) \times (G_2/H_2)$ telle que $g(f(s_1, s_2)) = (f_1(s_1), f_2(s_2))$ est un isomorphisme de variétés.*

Soit R_i le corps des fonctions numériques H_i-invariantes sur G_i, et soit R le corps des fractions de l'anneau intègre[8] $R_1 \otimes R_2$. Comme F_{G_i} est séparable sur R_i, il est algébrique et séparable sur un corps S_i qui est une extension transcendante pure de R_i ; il est alors clair que le corps des fractions S de $S_1 \otimes S_2$ est une extension transcendante pure de R et que le corps des fractions F_G de $F_{G_1} \otimes F_{G_2}$ est algébrique séparable sur S. Donc F_G est séparable sur R, et tout élément de F_G radiciel sur R est dans R.

Soit h l'application $(s_1, s_2) \to (f_1(s_1), f_2(s_2))$ de G sur $(G_1/H_1) \times (G_2/H_2)$; il résulte du théorème 2 qu'il existe une sous-variété ouverte G' de G telle que $h(G')$ soit ouvert dans $(G_1/H_1) \times (G_2/H_2)$ et que, h' désignant la restriction de h à G', $h(G')$ soit variété quotient de G' par h'. Or g est un morphisme (théorème 1) ; $f(G') = g^{-1}(h(G'))$ est donc ouvert

[8] Comme le corps K est algébriquement clos, les corps R_1 et R_2 sont des extensions *régulières* de K (**SCC**, exposé 14, proposition 3) et l'algèbre $R_1 \otimes R_2$ n'a donc pas de diviseurs de 0 d'après *loc. cit.*, théorème 2.

dans G/H et est variété quotient de G' par la restriction de f à G'. Il en résulte immédiatement que g induit un isomorphisme de $f(G')$ sur $h(G')$. Par ailleurs, si $a_i \in G_i$, l'application m de G/H sur lui-même qui transforme $f(s_1, s_2)$ en $f(a_1 s_1, a_2 s_2)$ est un automorphisme, et l'application m' de $(G_1/H_1) \times (G_2/H_2)$ qui transforme $(f_1(s_1), f_2(s_2))$ en $(f_1(a_1 s_1), f_2(a_2 s_2))$ est un automorphisme. Comme $g \circ m = m' \circ g$, on en déduit immédiatement que g est un isomorphisme.

Proposition 8. – *Soit H un sous-groupe fermé d'un groupe algébrique G. L'application $(s, x) \to s \cdot x$ de $G \times (G/H)$ dans G/H est un morphisme.*

Soient f l'application canonique $G \to G/H$ et g l'application $(s, t) \to (s, f(t))$. L'application $(s, t) \to s \cdot f(t) = f(st)$ est un morphisme de $G \times G$ dans G/H et $G \times (G/H)$ est variété quotient de $G \times G$ par g (proposition 7) ; la proposition 8 résulte alors du théorème 1.

Proposition 9. – *Soient G un groupe algébrique et H un sous-groupe invariant fermé de G. La structure de groupe de G/H et sa structure de variété quotient de G définissent alors sur G/H une structure de groupe algébrique.*

On démontre que l'application $(x, y) \to xy$ de $(G/H) \times (G/H)$ dans G/H est un morphisme en opérant comme dans la démonstration de la proposition 7. Soit f l'application canonique $G \to G/H$; $s \to (f(s))^{-1} = f(s^{-1})$ est un morphisme ; il en résulte (théorème 1) que $x \to x^{-1}$ est un morphisme de G/H.

On notera qu'il a été établi que, si H est un sous-groupe invariant fermé d'un groupe algébrique affine G, alors G/H est un groupe affine.

9. Le normalisateur d'un groupe de Borel[1]

9.1 Un lemme de dévissage

Lemme 1. – *Tout automorphisme du groupe additif K (considéré comme groupe algébrique) est de la forme $x \to cx$, c étant un élément $\neq 0$ de K.*

Soit σ un automorphisme. Si θ est l'application identique $K \to K$, $\theta \circ \sigma$ est une fonction numérique partout définie qui n'a qu'un seul zéro, à savoir 0, qui est d'ordre 1 ; une telle fonction est de la forme $c\,\theta$.

Lemme 2. – *Soit G un groupe algébrique résoluble et connexe ; soient G_u l'ensemble des éléments unipotents de G et T un tore maximal de G. Soient A et B des sous-groupes fermés connexes de G_u dont les normalisateurs contiennent T et tels que $A \subset B$. Il existe une suite croissante $(H_i)_{0 \leq i \leq m}$ de sous-groupes fermés connexes de G_u qui possède les propriétés suivantes : $U_0 = \{e\}$; pour $1 \leq i \leq m$, le normalisateur de H_{i-1} contient H_i et T ; il existe un homomorphisme rationnel θ_i de H_i sur le groupe additif K de noyau H_{i-1} qui définit par passage aux quotients un isomorphisme de H_i/H_{i-1} sur K ; on a, pour $s \in H_i$, $t \in T$, $\theta_i(tst^{-1}) = \chi_i(t)\,\theta_i(s)$, χ_i étant un caractère rationnel de T ; H_i est engendré par H_{i-1} et par des éléments du centralisateur de la composante neutre du noyau de χ_i dans T ; on a $H_m = G_u$; A et B figurent parmi les H_i. Si A et B sont invariants dans G, on peut supposer qu'il en est de même de tous les H_i.*

Etablissons d'abord que, si C *est un sous-groupe invariant connexe de G contenu dans G_u et $\neq \{e\}$* (e étant l'élément neutre), C *contient un sous-groupe connexe de dimension* 1 *invariant dans G.* On a déjà vu (n° 6.2, corollaire 1 au théorème 2) qu'il existe une suite $(G_0, \ldots, G_s)$ de sous-groupes invariants connexes de G telle que $G_0 = \{e\}$, $G_{i-1} \subset G_i$ et $\dim G_i/G_{i-1} = 1$ si $1 \leq i \leq s$, $G_s = G_u$. Si $G_1 \subset C$, notre assertion est vraie. Sinon, on procède par récurrence sur $\dim C$. Soit k le plus petit indice tel que $C \subset G_k$; $G_{k-1}\,C$ est connexe, contient G_{k-1} sans lui être égal et est contenu dans G_k, d'où $G_{k-1}\,C = G_k$. Soit $C' = C \cap G_{k-1}$; l'application canonique $G_k \to G_k/G_{k-1}$ induit un épimorphisme de C sur G_k/G_{k-1} de noyau C' ; si C' est fini, C est de dimension 1 ; sinon, la composante neutre C'_0 de C' est de dimension $< \dim C$, mais > 0, et il suffit de lui appliquer l'hypothèse inductive.

Ceci étant, soit H un sous-groupe fermé connexe $\neq G_u$ de G_u dont le normalisateur dans G contient T et sur lequel nous faisons l'hypothèse sui-

[1] Exposé de C. Chevalley, le 4.2.1957

vante : ou bien a) $H \subset A$ et $H \neq A$, ou bien b) $A \subset H \subset B$ et $H \neq B$; ou bien c) $B \subset H$. Soit N un groupe qui est le normalisateur connexe de H dans A dans le cas a), dans B dans le cas b), dans G_u dans le cas c). On a $N \neq H$ en vertu du lemme 1 du n° 7.1. Le normalisateur de N dans G contient T ; NT est un groupe algébrique résoluble connexe contenant H et N comme sous-groupes invariants. Appliquant le résultat établi ci-dessus à NT/H, on voit qu'il existe un sous-groupe fermé connexe invariant H' de NT contenu dans N, contenant H et tel que H'/H soit de dimension 1. On a $H' \subset A$ dans le cas a), $H' \subset B$ dans le cas b), et $H' \subset G_u$ dans tous les cas. Comme H'/H est de dimension 1 et se compose d'éléments unipotents, il est isomorphe à K (théorème 4 du n° 7.4). Il existe donc un homomorphisme rationnel θ de H' sur K de noyau H qui définit par passage aux quotients un isomorphisme de H'/H sur K ; tout autre homomorphisme θ' ayant les mêmes propriétés est de la forme $s \to c\,\theta(s)$ en vertu du lemme 1. Si $t \in T$, $s \to tst^{-1}$ est un automorphisme de H' qui conserve H ; $\theta(tst^{-1})$ est donc de la forme $\chi(t)\,\theta(s)$, $\chi(t) \in K^*$ (le groupe des éléments $\neq 0$ de K). Prenant s tel que $\theta(s) = 1$, on voit que χ est un morphisme de T dans K^* ; c'est évidemment un caractère. Soit Q la composante neutre du noyau du caractère χ de T, et soit C son centralisateur dans le groupe $H'Q$; comme Q est un tore maximal de $H'Q$, C est un groupe de Cartan de $H'Q$ (n° 7.1, théorème 1). Soit π l'homomorphisme canonique de $H'Q$ sur $H'Q/H$; $\pi(C)$ est donc un groupe de Cartan de $H'Q/H$ (théorème 3 du n° 7.3). Or il est clair que $H'Q/H$ est un groupe commutatif, et en particulier nilpotent, d'où $\pi(C) = H'Q/H$, ce qui montre que H' est engendré par H et par des éléments de C. Supposons maintenant de plus que H soit un sous-groupe invariant de G, et qu'il en soit de même de A et B. Le groupe N est alors invariant dans G, et N/H est un sous-groupe invariant de G/H. On peut alors prendre pour H' un sous-groupe invariant de G. Les considérations précédentes permettent de construire inductivement une suite (H_i) ayant les propriétés énoncées.

9.2 Un lemme de géométrie algébrique

Lemme 3. – *Soient G un groupe algébrique, H un sous-groupe fermé connexe de G, f l'application canonique de G sur G/H. Si V est une partie fermée irréductible de G/H, alors $f^{-1}(V)$ est une partie fermée irréductible de G.*

Démonstration. – Posons $C = f^{-1}(V)$ et notons $C_1, \ldots, C_r$ les composantes irréductibles de C. On a

$$C = C \cdot H = \bigcup_i C_i \cdot H\,.$$

Or, pour tout i, l'ensemble $C_i \cdot H$ est l'image par la multiplication $G \times G \to G$ de l'ensemble irréductible $C_i \times H$, donc son adhérence $\overline{C_i \cdot H}$ est irréductible. Comme on a $C_i \subset \overline{C_i \cdot H}$, on en conclut $C_i = C_i \cdot H = \overline{C_i \cdot H}$. Comme la

topologie de Zariski de G/H est quotient de celle de G, il existe des parties fermées $V_1, \ldots, V_r$ de G/H telles que $V = \bigcup_i V_i$ et $C_i = f^{-1}(V_i)$. Comme V est irréductible, il existe un indice i tel que $V_i = V$, d'où $C_i = C$. Ceci prouve que C est irréductible.

9.3 Normalisateur d'un groupe de Borel

Théorème 1. – *Soit B un groupe de Borel d'un groupe algébrique affine connexe G. Alors B est son propre normalisateur dans G.*

Démonstration[2]. – Le normalisateur N de B dans G est un sous-groupe fermé de G. On sait que B est la composante neutre de N (n° 6.6, corollaire 3 du théorème 6). De plus, tout élément du groupe algébrique affine N est produit d'un élément semi-simple de N et d'un élément unipotent de N (n° 4.4, théorème 3). Il suffit donc de prouver que B contient les éléments semi-simples et les éléments unipotents de N.

Lemme 4. – *Soient $g_0 \in N$ et Z un sous-groupe fermé, connexe et résoluble de G. On suppose que l'on a $g_0^{-1}\, z^{-1}\, g_0\, z \in B$ pour tout $z \in Z$. Il existe alors un élément x_0 de G avec les propriétés suivantes :*

a) *le sous-groupe $x_0^{-1}\, Z\, x_0$ de G est contenu dans B ;*

b) *les éléments g_0 et $g_1 = x_0^{-1}\, g_0\, x_0$ appartiennent à la même composante connexe de N.*

Soit X l'adhérence de ZB ; on a évidemment $e \in X$, et comme Z et B sont connexes, et l'application $(z, b) \to zb$ continue, X est connexe. D'après le corollaire 5 au théorème 5 du n° 6.5, il existe $x_0 \in X$ tel que $x_0^{-1}\, Z\, x_0 \subset B$. D'où a).

Pour prouver b), introduisons l'ensemble P des éléments h de G tels que $h^{-1}\, g_0\, h \in N$, et l'ensemble N_1 des éléments de la forme $x^{-1}\, g_0\, x$ avec $x \in X$. Il est clair que P est *fermé*, et comme B est un sous-groupe de N, *on a* $PB = P$. Montrons que Z *est contenu dans* P. Soit $z \in Z$; vu l'hypothèse faite sur g_0 et Z, on a $z^{-1}\, g_0\, z \in g_0\, B$, et comme g_0 appartient à N, on a $g_0\, N \subset N$, d'où $z \in P$. Vu les propriétés de P, on a $X \subset P$, c'est-à-dire $x^{-1}\, g_0\, x \in N$ pour tout $x \in X$. Comme X est connexe, et que l'application $x \to x^{-1}\, g_0\, x$ est continue, N_1 est une partie connexe de N, qui contient évidemment $g_0 = e^{-1}\, g_0\, e$ et $g_1 = x_0^{-1}\, g_0\, x_0$, d'où b).

Le lemme 4 étant démontré, soit g un élément *semi-simple* de N. D'après le théorème 6, c) du n° 6.6, il existe un tore maximal Z de G contenant g ; comme Z est commutatif, on a $g^{-1}\, z^{-1}\, g\, z = e$ pour tout $z \in Z$. D'après le lemme 4, il existe un élément x_0 de G tel que $x_0^{-1}\, Z\, x_0 \subset B$ et que g appartienne à la même composante connexe de N que $x_0^{-1}\, g\, x_0 = g_1$; comme

[2] On remarquera que la démonstration n'utilise par les lemmes 1 à 3.

on a $g \in Z$ et $x_0^{-1} Z x_0 \subset B$, on a $g_1 \in B$, et comme B est la composante neutre de N, on a finalement $g \in B$.

Supposons maintenant que g soit *unipotent*. Soit B' un groupe de Borel de G contenant g (n° 6.6, théorème 6, b)). L'ensemble B'^u des éléments unipotents de B' est un sous-groupe fermé, connexe et nilpotent de G (n° 6.4, théorème 4) et contenant g. Soit $(H_i)_{0 \leq i \leq m}$ la suite centrale descendante de B'^u ; chaque groupe H_i est fermé, connexe et invariant dans B'^u, on a $H_i \supset H_{i+1}$ pour $0 \leq i \leq m-1$, $H_0 = B'^u$ et $H_m = \{e\}$; enfin, on a $(B'^u, H_i) \subset H_{i+1}$ pour $0 \leq i \leq m-1$. Notons C la composante connexe de N contenant g.

Soit i un entier tel que $1 \leq i \leq m$ pour lequel il existe un élément u_i de G avec les propriétés suivantes :

(a)$_i$ *le sous-groupe* $Z_i = u_i^{-1} H_i u_i$ *est contenu dans* B ;

(b)$_i$ *l'élément* $p_i = u_i^{-1} g u_i$ *appartient à* C.

Appliquons le lemme 4 au cas $g_0 = p_i$ et $Z = u_i^{-1} H_{i-1} u_i$. Il est clair que Z est un sous-groupe fermé, connexe et résoluble de G ; pour $z = u_i^{-1} h_{i-1} u_i$ dans Z (avec $h_{i-1} \in H_{i-1}$), le commutateur de p_i et z est de la forme

$$u_i^{-1}(g^{-1} h_{i-1}^{-1} g h_{i-1}) u_i$$

et appartient donc à $u_i^{-1} H_i u_i$, donc à B d'après (a)$_i$. Avec les notations du lemme 4, posons $u_{i-1} = u_i x_0$, et $p_{i-1} = u_{i-1}^{-1} g u_{i-1}$. On a alors $p_{i-1} = x_0^{-1} p_i x_0$. Il résulte aussitôt du lemme 4 que le sous-groupe $Z_{i-1} = u_{i-1}^{-1} H_{i-1} u_{i-1} = x_0^{-1} Z x_0$ est contenu dans B et que p_{i-1} et p_i appartiennent à la même composante connexe de N, d'où $p_{i-1} \in C$.

Pour $i = m$, on a $H_m = \{e\}$ et $g \in C$, et l'on peut démarrer la récurrence descendante avec $u_m = e$. On peut donc construire une suite $(u_0, u_1, \ldots, u_m)$ d'éléments de G satisfaisant aux propriétés (a)$_i$ et (b)$_i$ pour $0 \leq i \leq m$. En particulier, pour $i = 0$, on obtient les relations $u_0^{-1} H_0 u_0 \subset B$ et $u_0^{-1} g u_0 \in C$; on a aussi $g \in B'^u = H_0$, et comme B est la composante neutre de N, on a $C = B$, d'où finalement $g \in B$ puisque C est la composante connexe de g dans N. C.Q.F.D.

Corollaire 1. – *Soit B un groupe de Borel du groupe algébrique affine et connexe G. L'application qui à tout $x \in G/B$ fait correspondre le groupe de stabilité de x est une bijection de G/B sur l'ensemble des groupes de Borel de B.*

Soit f l'application canonique de G sur G/B ; si $x = f(s)$, $s \in G$, le groupe de stabilité de x est sBs^{-1}, qui est un groupe de Borel. Comme tous les groupes de Borel sont conjugués (n° 6.5, théorème 5), l'application en question est surjective ; si $x = f(s)$, $x' = f(s')$ sont tels que $sBs^{-1} = s'Bs'^{-1}$, $s^{-1}s'$ normalise B, donc est dans B, d'où $x = x'$.

Corollaire 2. – *Tout groupe de Borel B d'un groupe algébrique affine et connexe G est un sous-groupe résoluble maximal de G.*

Soit H un sous-groupe résoluble de G contenant B ; soient $\overline{H}$ l'adhérence de H, et $\overline{H}_0$ la composante neutre de $\overline{H}$; $\overline{H}_0$ est résoluble et connexe d'après la remarque du n° 3.4, et contient B, d'où $\overline{H}_0 = B$; $\overline{H}$ étant dans le normalisateur de $\overline{H}_0 = B$, on a $H = B$ d'après le théorème 1.

Corollaire 3. – *Soit T un tore maximal d'un groupe algébrique affine et connexe G ; soient C et N respectivement le centralisateur et le normalisateur de T. Soit B un groupe de Borel contenant T ; les groupes de Borel contenant T sont alors les sBs^{-1}, où $s \in N$; si s, $s' \in N$, on ne peut avoir $sBs^{-1} = s'Bs'^{-1}$ que si $s \equiv s' \pmod{C}$. Le nombre des groupes de Borel contenant T est fini et égal à $[N : C]$.*

Si sBs^{-1} est un groupe de Borel contenant T, sTs^{-1} et T sont des tores maximaux de sBs^{-1}, donc conjugués dans sBs^{-1} (n° 6.5, théorème 5) ; si $sTs^{-1} = b'Tb'^{-1}$, avec $b' \in sBs^{-1}$, alors $b'^{-1}s = s'$ est dans N et $sBs^{-1} = s'Bs'^{-1}$. Soient maintenant s et s' des éléments de N tels que $s'Bs'^{-1} = sBs^{-1}$; $s^{-1}s'$ est alors dans le normalisateur de B, donc dans B (théorème 1) ; de plus $s^{-1}s' \in N$. On a $N \cap B = C$ d'après le théorème 7 du n° 6.7, d'où $s \equiv s' \bmod C$, et N/C est fini d'après *loc. cit.*

Définition 1. – *Les notations étant celles du corollaire 3, le groupe N/C s'appelle le groupe de Weyl de T.*

Tous les tores maximaux de G étant conjugués (n° 6.5, théorème 5), ces tores ont des groupes de Weyl isomorphes. Un groupe abstrait isomorphe aux groupes de Weyl des tores maximaux de G est aussi appelé un *groupe de Weyl* de G.

9.4 Le radical

Définition 2. – *On appelle radical d'un groupe algébrique affine et connexe G la composante neutre de l'intersection des groupes de Borel de G.*

Le radical est manifestement un sous-groupe invariant fermé résoluble de G.

Proposition 1. – *Le radical de G est le plus grand sous-groupe invariant fermé résoluble connexe de G.*

En effet, un sous-groupe invariant connexe et résoluble de G est contenu dans au moins un groupe de Borel, donc dans tous par conjugaison, et par suite aussi dans le radical.

Définition 3. – *On appelle semi-simple un groupe algébrique affine et connexe dont le radical se réduit à l'élément neutre.*

Proposition 2. – *Soit R le radical d'un groupe algébrique affine et connexe G. Le groupe G/R est alors semi-simple et ses sous-groupes de Borel sont les groupes de la forme B/R où B est un sous-groupe de Borel de G.*

Compte tenu du lemme 3, un sous-groupe fermé S de G est connexe si et seulement si S/R est connexe. De plus S est résoluble (resp. invariant) si et seulement si S/R est résoluble (resp. invariant). La proposition 2 résulte aussitôt de là.

9.5 Les groupes à un paramètre d'un tore

Soit T un tore. Nous appellerons *groupe à un paramètre de* T tout homomorphisme rationnel γ du groupe multiplicatif K^* des éléments $\neq 0$ de K dans T ; soit $\Gamma(T)$ l'ensemble des groupes à un paramètre de T. Si $\gamma \in \Gamma(T)$, nous désignerons par $\operatorname{Supp}\gamma$ l'ensemble des $\gamma(x)$, $x \in K^*$. Si γ et γ' sont dans $\Gamma(T)$, il en est de même de l'application $x \to \gamma(x)\ \gamma'(x)$; on a ainsi une loi de composition dans $\Gamma(T)$ relativement à laquelle $\Gamma(T)$ constitue un groupe commutatif comme on le vérifie tout de suite. Ce groupe sera noté suivant les besoins, tantôt additivement, tantôt multiplicativement. Soit aussi $X(T)$ le groupe des caractères de T, *i.e.* des homomorphismes rationnels de T dans K^*. Si $\gamma \in \Gamma(T)$, $\chi \in X(T)$, $\chi \circ \gamma$ est un homomorphisme rationnel de K^* dans lui-même, donc de la forme $x \to x^n$, n étant un entier bien déterminé ; nous poserons $n = \langle \gamma, \chi \rangle$. Considérant $\Gamma(T)$ et $X(T)$ comme des modules sur $\mathbf{Z}$, $(\gamma, \chi) \to \langle \gamma, \chi \rangle$ est évidemment une forme bilinéaire sur $\Gamma(T) \times X(T)$. Montrons qu'elle définit un isomorphisme de l'un quelconque des modules $\Gamma(T)$, $X(T)$ sur le dual de l'autre. On peut se limiter au cas où $T = (K^*)^d$ pour un certain $d > 0$. Le groupe $X(T)$ est alors, comme on l'a vu, le $\mathbf{Z}$-module libre de base les éléments χ_i $(1 \leq i \leq d)$ tels que

$$\chi_i(x_1, \ldots, x_d) = x_i \qquad (1 \leq i \leq d) \quad (\text{où } (x_1, \ldots, x_d) \in (K^*)^d)\,.$$

Par ailleurs, l'application γ_i qui fait correspondre à tout $x \in K^*$ l'élément de $(K^*)^d$ dont la i-ème coordonnée est x et les autres coordonnées valent 1 est un groupe à un paramètre ; on a $\langle \gamma_i, \chi_j \rangle = \delta_{ij}$ $(1 \leq i,\ j \leq d)$. Si γ est un élément quelconque de $\Gamma(T)$, il existe des entiers e_i tels que $\langle \gamma - \sum_{i=1}^{d} e_i\, \gamma_i, \chi_j \rangle = 0$ pour $1 \leq j \leq d$, ce qui entraîne manifestement que $\gamma = \sum_{i=1}^{d} e_i\, \gamma_i$, et démontre notre assertion.

Par extension de l'anneau de base, on déduit de $\Gamma(T)$ un espace vectoriel $\Gamma^{\mathbf{R}}(T)$ de dimension $\dim T$ sur le corps $\mathbf{R}$ des nombres réels.

Proposition 3. – *Soit T un tore; soit U un cône ouvert non vide dans l'espace vectoriel $\Gamma^{\mathbf{R}}(T)$ (muni de sa topologie ordinaire). La réunion des* $\operatorname{Supp}\gamma$ *pour $\gamma \in U \cap \Gamma(T)$ est alors dense dans T.*

On identifie $\Gamma(T)$ à un sous-groupe discret de l'espace vectoriel $\Gamma^{\mathbf{R}}(T)$; tenant compte de la dualité entre $\Gamma(T)$ et $X(T)$, on identifie aussi $X(T)$ à un sous-groupe discret du dual $\Gamma^{\mathbf{R}}(T)'$ de $\Gamma^{\mathbf{R}}(T)$.

Soit E une partie fermée de T, distincte de T, et soit Γ l'ensemble des γ dans $\Gamma(T)$ tels que $\operatorname{Supp}\gamma \subset E$. Nous allons prouver que Γ *est contenu dans la réunion d'un nombre fini d'hyperplans de* $\Gamma^{\mathbf{R}}(T)$. En effet, soit $f \neq 0$ une fonction régulière sur T, nulle sur E. D'après le corollaire 3 du théorème 2 du n° 4.3, f est de la forme $\sum_{i=1}^{r} c_i \cdot \chi_i$ avec $c_1, \ldots, c_r$ dans K^* et des éléments distincts $\chi_1, \ldots, \chi_r$ de $X(T)$. Pour $\gamma \in \Gamma(T)$, et $x \in K^*$, on a

$$f(\gamma(x)) = \sum_{i=1}^{r} c_i \, x^{\langle \gamma, \chi_i \rangle} .$$

Si les entiers $\langle \gamma, \chi_i \rangle$ sont deux à deux distincts, la fonction $f \circ \gamma$ n'est pas nulle, et l'on a $\operatorname{Supp}\gamma \not\subset E$, d'où $\gamma \notin \Gamma$. Autrement dit, Γ est contenu dans la réunion des hyperplans $H_{ij} = \{u \in \Gamma^{\mathbf{R}}(T) \mid \langle u, \chi_i \rangle = \langle u, \chi_j \rangle\}$ pour $1 \leq i < j \leq r$.

Pour démontrer la proposition 3, il suffit de prouver que $U \cap \Gamma(T)$ n'est pas contenu dans la réunion D d'un nombre fini d'hyperplans de $\Gamma^{\mathbf{R}}(T)$. Le sous-espace vectoriel $\Gamma^{\mathbf{Q}}(T)$ engendré par $\Gamma(T)$ sur le corps $\mathbf{Q}$ des nombres rationnels est *dense* dans $\Gamma^{\mathbf{R}}(T)$; il contient donc un point $u \in U \cap \complement D$, et un multiple entier convenable de u appartient à $U \cap \Gamma(T)$, mais non à D (car U est stable par homothéties).

10. Les tores singuliers[1]

10.1 Cinq lemmes

Lemme 1. – *Soient U, V et W des ensembles algébriques, f un morphisme de $U \times V$ dans W, A une partie fermée de V et B une partie fermée de W telle que $f(U \times A) \subset B$; si U est irréductible et si A' est une composante irréductible de A, $f(U \times A')$ est contenu dans une composante irréductible de B.*

Cet ensemble est en effet irréductible comme image continue de l'ensemble irréductible $U \times A'$.

Corollaire. – *Soit G un groupe algébrique connexe qui opère dans un ensemble algébrique V. Si les applications $y \to s \cdot y$ (pour $s \in G$) transforment toutes en elle-même une certaine partie fermée A de V, elles transforment en elle-même toute composante irréductible A' de A.*

En effet, les points $s \cdot y$ ($s \in G$, $y \in A'$) sont contenus dans une même composante irréductible de A (lemme 1) qui, contenant $y = e \cdot y$ pour tout $y \in A'$, est identique à A'.

Lemme 2. – *Soient Q et T des tores et U une variété ; soit, pour chaque $u \in U$, f_u un homomorphisme rationnel de Q dans T. Supposons que, pour tout $z \in Q$, $u \to f_u(z)$ soit un morphisme de U dans T. Alors f_u ne dépend pas de u.*

Soit z un point d'ordre fini m de Q ; $f_u(z)$ est un point d'ordre fini diviseur de m, donc reste dans un ensemble fini ; comme l'ensemble des $f_u(z)$ pour $u \in U$ est irréductible, il se réduit à un point. Soit A l'ensemble des éléments d'ordres finis de Q ; il est dense dans Q. Si $u, u' \in U$, les applications continues f_u, $f_{u'}$, qui coïncident sur A sont égales.

Rappelons que le corps K, muni de sa structure de variété, peut être plongé dans une variété complète D, la droite projective, qui se déduit de K par adjonction d'un point noté ∞, et qui est isomorphe à l'espace projectif associé à l'espace vectoriel K^2.

Lemme 3. – *Toute fonction f sur la droite projective à valeurs dans une variété complète V est partout définie.*

[1] Exposé de C. Chevalley, le 11.2.1957

Si D_0 est l'ensemble de définition de f, $a \to (a, f(a))$ est un morphisme g de D_0 dans $D \times V$; l'adhérence Φ de l'image de D_0 par ce morphisme est une sous-variété fermée de $D \times V$; si p est le morphisme de Φ dans D induit par la projection $D \times V \to D$, $p^{-1}(a)$ est fini pour tout $a \in D$ puisque Φ est de dimension 1 ; de plus, le cohomomorphisme de p est un isomorphisme du corps F_D sur le corps F_Φ, car $p \odot g$ (resp. $g \odot p$) est l'application identique de D (resp. Φ). Comme D est normale, p est un isomorphisme de Φ sur une sous-variété $p(\Phi)$ de D (n° 5.3, théorème 2) ; or Φ, qui est une sous-variété fermée de la variété complète $D \times V$, est complète ; $p(\Phi)$ est donc fermé, d'où $p(\Phi) = D$; le lemme 3 résulte immédiatement de là.

Lemme 4. – *Toute fonction numérique u partout définie sur une variété complète V est constante.*

On peut considérer u comme un morphisme de V dans la droite projective D ; comme V est complète, $u(V)$ est une partie fermée irréductible de D qui ne contient pas le point ∞ et se réduit par suite à un point.

Lemme 5. – *Soient $P(V)$ l'espace projectif associé à un espace vectoriel V de dimension finie et W une sous-variété fermée de dimension $d > 0$ de $P(V)$. Si H est un hyperplan de $P(V)$, $W \cap H$ est non vide, et toute composante irréductible de cet ensemble est de dimension $\geq d - 1$.*

Soit φ l'application canonique de l'ensemble des éléments $\neq 0$ de V sur $P(V)$. Si λ, μ sont des formes linéaires sur V, $\mu \neq 0$, il y a une fonction numérique λ/μ sur $P(V)$ définie en tout point $\varphi(x)$ tel que $\mu(x) \neq 0$ et y prenant la valeur $\lambda(x)(\mu(x))^{-1}$. Prenons pour μ une forme linéaire $\neq 0$ nulle sur $\varphi^{-1}(H)$. Ecartons le cas trivial où $W \subset H$; comme W ne se réduit pas à un point, il existe une forme linéaire λ sur V telle que λ/μ (qui est définie en au moins un point de W) induise une fonction non constante sur W ; il existe un point de W où cette fonction n'est pas définie (lemme 4), d'où $W \cap H \neq \varnothing$. Soit x_0 tel que $\varphi(x_0) \in W \cap H$, et soit ν une forme linéaire sur V telle que $\nu(x_0) \neq 0$; soit W_0 l'ensemble des points de W en lesquels μ/ν est définie. Alors $W_0 \cap H$ est l'image réciproque de 0 par le morphisme de W_0 dans K induit par μ/ν ; les composantes irréductibles de cet ensemble sont donc de dimensions $\geq d - 1$ (**SCC**, exposé 8, théorème 2).

10.2 Les groupes de Borel qui contiennent un tore

Soit G un groupe algébrique affine connexe et soit Q un tore contenu dans G. Soit B_0 un groupe de Borel de G ; les groupes de Borel de G sont donc les stabilisateurs des points de G/B_0 (n° 8.3, corollaire 1 du théorème 1) ; ceux qui contiennent Q sont les stabilisateurs des points de G/B_0 invariants par Q.

Proposition 1. – *Les points de G/B_0 invariants par Q forment un ensemble fermé E. Soit Z le centralisateur de Q dans G ; il est connexe. Si E_1 est une*

composante irréductible de E, les points de E_1 sont transformés transitivement entre eux par les opérations de Z ; leurs stabilisateurs dans Z sont les groupes de Borel de Z ; si C est l'un de ces groupes, on a $\dim E_1 = \dim Z/C$. *Si T est un tore maximal de G contenant Q, E_1 contient un point dont le stabilisateur contient T.*

Il est évident que E est fermé et que les opérations de Z permutent entre eux les points de E. Comme Z est connexe (n° 6.7, théorème 7, a)), les opérations de Z permutent entre eux les points de E_1 (corollaire au lemme 1). Soit f l'application canonique $G \to G/B_0$; alors $U = f^{-1}(E_1)$ est une sous-variété fermée de G (n° 9.2, lemme 3). Si $u \in U$, on a $Q \subset uB_0\,u^{-1}$, d'où $u^{-1}Qu \subset B_0$. Soit B_0^u le groupe des éléments unipotents de B_0 ; alors B_0/B_0^u est un tore ; si h est l'application canonique de B_0 sur B_0/B_0^u, l'application $(u,x) \to h(u^{-1}xu)$ est un morphisme de $U \times Q$ dans B_0/B_0^u ; lui appliquant le lemme 2, on voit qu'il ne dépend pas de u. Il en résulte que le groupe D engendré par B_0^u et $u^{-1}Qu$ ne dépend pas de u ; les $u^{-1}Qu$ en sont des tores maximaux, et sont par suite conjugués les uns des autres dans D (n° 6.5, théorème 5, c)). Soit u_1 un point quelconque de U ; posons $Q_1 = u_1^{-1}Qu_1$. Alors, pour tout $u \in U$, il existe un élément $b(u) \in B_0^u$ tel que $u^{-1}Qu = b(u)Q_1\,(b(u))^{-1}$; de plus, si $x \in Q$, on a $u^{-1}xu \equiv u_1^{-1}xu_1 \pmod{B_0^u}$ et par suite aussi $(ub(u))^{-1}x(ub(u)) \equiv u_1^{-1}xu_1 \pmod{B_0^u}$; comme ces deux éléments appartiennent à Q_1, ils sont égaux, d'où $ub(u) = z(u)u_1$ avec un $z(u) \in Z$. Comme $b(u)$ appartient à B_0, on a $f(ub(u)) = f(u)$, d'où $f(u) = z(u)\cdot x_1$ si $x_1 = f(u_1)$. Comme $f(U) = E_1$, on a $E_1 = Z \cdot x_1$, ce qui montre que les opérations de Z transforment transitivement entre eux les points de E_1.

Si C est un groupe de Borel de Z, les opérations de C laissent invariant un point x au moins de E_1, puisque E_1 est une variété complète et C résoluble et connexe (n° 6.1, théorème 1). Les opérations de Z qui laissent x fixe sont celles de l'intersection de Z avec le stabilisateur de x dans G, qui est un groupe résoluble ; elles forment donc un sous-groupe résoluble de Z qui, contenant C, lui est identique (n° 9.3, corollaire 2 au théorème 1). On en déduit par passage aux quotients un morphisme bijectif de Z/C sur E_1, d'où $\dim E_1 = \dim Z/C$. Tout tore maximal de G contenant Q est contenu dans Z, donc dans au moins un groupe de Borel de Z, ce qui démontre la dernière assertion.

Remarque. – Il faut se garder de croire que les composantes irréductibles de E sont transformées transitivement entre elles par les opérations du normalisateur de Q ; il n'en est pas ainsi, comme on le voit par des exemples simples.

Définition 1. – *Un tore Q de G est dit régulier s'il contient au moins un point régulier de G, semi-régulier s'il n'est contenu que dans un nombre fini de groupes de Borel de G, singulier s'il est contenu dans une infinité de groupes de Borel de G.*

D'après le corollaire 3 du théorème 2 du n° 7.2, tout tore maximal est régulier.

Proposition 2. – *Pour qu'un tore soit semi-régulier, il faut et suffit que son centralisateur soit résoluble.*

Cela résulte immédiatement de la proposition 1.

Corollaire. – *Un tore régulier et, en particulier, un tore maximal est semi-régulier.*

Si un tore Q contient un élément régulier s, son centralisateur (qui est connexe) est contenu dans le centralisateur connexe de s ; comme s est semi-simple, ce dernier groupe est nilpotent, donc résoluble (n° 7.2, théorème 2).

Proposition 3. – *Si Q est un tore semi-régulier contenu dans le tore maximal T, tout groupe de Borel qui contient Q contient T.*

Soit B_0 un groupe de Borel. L'ensemble E des points de G/B_0 invariants par Q est fini. Comme T est commutatif, les opérations de T transforment E en lui-même, donc transforment chaque point de E en lui-même (corollaire au lemme 1).

Proposition 4. – *Pour qu'un tore Q soit semi-régulier* (resp. régulier), *il faut et suffit qu'il existe un groupe à un paramètre γ de T tel que* Supp γ *soit semi-régulier* (resp. régulier).

La condition est évidemment suffisante. L'ensemble Q_0 des points de Q dont les centralisateurs sont égaux à celui de Q contient un ensemble relativement ouvert non vide dans Q. On peut en effet supposer que le groupe G est un groupe algébrique de matrices et que les éléments de Q sont des matrices diagonales ; si $t \in Q$, soient $a_1(t), \ldots, a_n(t)$ les coefficients diagonaux de la matrice t. Le centralisateur de Q se compose des matrices $(b_{ij}) \in G$ telles que $b_{ij} = 0$ pour tout couple (i, j) tel que l'on n'ait pas $a_i(t) = a_j(t)$ pour tout $t \in Q$. Or il existe une partie ouverte non vide Q_0 de Q telle que, si $t \in Q_0$, la relation $a_i(t) = a_j(t)$ entraîne $a_i(t') = a_j(t')$ pour tout $t' \in Q$.

Il existe donc un groupe à un paramètre γ de Q tel que Supp γ rencontre Q_0 (n° 9.5, proposition 3), d'où le résultat.

Nous dirons qu'un groupe à un paramètre d'un tore de G est *régulier* (resp. *semi-régulier*, *singulier*) si le tore Supp γ est régulier (resp. semi-régulier, singulier).

Corollaire. – *Soit T un tore maximal du groupe algébrique affine connexe G. Il existe un groupe à un paramètre régulier* (donc semi-régulier) *de T.*

En effet, un tore maximal est régulier.

10.3 Groupes à un paramètre semi-réguliers

Soient G un groupe algébrique affine connexe et Ω une variété complète sur laquelle opère G. Soient T un tore maximal de G, γ un groupe à un paramètre de T et x un point de Ω ; d'après le lemme 3, le morphisme $\theta \to \gamma(\theta) \cdot x$ de K^* dans Ω se prolonge en un morphisme de la droite projective dans Ω qui applique les points 0 et ∞ sur des points que nous désignerons par $\gamma(0) \cdot x$ et $\gamma(\infty) \cdot x$ respectivement. Il résulte immédiatement de la formule $\gamma(\theta\,\theta') \cdot x = \gamma(\theta) \cdot (\gamma(\theta') \cdot x)$ que les points $\gamma(0) \cdot x$, $\gamma(\infty) \cdot x$ sont invariants par les opérations de $\operatorname{Supp}\gamma$. Ceci dit, supposons que $\Omega = G/B_0$ où B_0 est un groupe de Borel de G. Alors le stabilisateur de $\gamma(0) \cdot x$ est un groupe de Borel contenant $\operatorname{Supp}\gamma$. Réciproquement, si x est un point de Ω invariant par les opérations de $\operatorname{Supp}\gamma$, on a $x = \gamma(0) \cdot x$; les groupes de Borel contenant $\operatorname{Supp}\gamma$ sont donc les stabilisateurs des points $\gamma(0) \cdot x$, où x parcourt les points de Ω ; pour que γ soit semi-régulier, il faut et suffit que l'ensemble des $\gamma(0) \cdot x$ soit fini. Pour étudier cet ensemble, nous allons utiliser une représentation linéaire de G.

Proposition 5. – *Soit H un sous-groupe fermé d'un groupe algébrique affine G. Il existe alors une représentation rationnelle ρ de G et un point $e \neq 0$ de l'espace V de ρ tels que H soit l'ensemble des $s \in G$ tels que $\rho(s)$ transforme l'espace Ke en lui-même*[2].

Soit P l'algèbre des fonctions régulières sur G, et soit $\mathfrak{a}$ l'idéal des fonctions de P nulles sur H. Si $s \in G$, $u \in P$, on désigne par $\sigma(s) \cdot u$ la fonction[3] $t \to u(ts)$. Tout sous-espace de dimension finie de P est contenu dans un sous-espace de dimension finie qui est stable par les opérations $\sigma(s)$ (n° 4.1, lemme 2). Il existe donc un sous-espace P_1 de dimension finie de P, stable par les $\sigma(s)$, qui contient un ensemble de générateurs de $\mathfrak{a}$. Soit $d = \dim(P_1 \cap \mathfrak{a})$; soient V la puissance extérieure d-ième de P_1 et, pour $s \in G$, $\rho(s)$ la puissance extérieure d-ième de la restriction de $\sigma(s)$ à P_1 ; soit e le produit extérieur des éléments d'une base de $P_1 \cap \mathfrak{a}$. Pour qu'un élément s appartienne à H, il faut et suffit que $\sigma(s)$ transforme $\mathfrak{a}$ en lui-même, ou encore transforme $P_1 \cap \mathfrak{a}$ en lui-même, donc que $\rho(s)$ transforme Ke en lui-même.

Remarque. – Prenant P_1 de telle manière que P_1 contienne 1 et un ensemble de générateurs de P, on voit facilement que la représentation ρ construite dans la démonstration précédente est fidèle.

Corollaire. – *Soient G un groupe algébrique affine connexe et B_0 un groupe de Borel de G. Il existe une représentation rationnelle ρ de G, d'espace V et un morphisme bijectif ξ de G/B_0 sur une sous-variété fermée Ω de l'espace projectif $P(V)$ associé à V qui possèdent la propriété suivante : si on désigne,*

[2] Voir aussi le théorème 1 du n° 4.2, dont la démonstration est essentiellement la même que celle de la proposition 5.

[3] Notée $R_s \cdot u$ au n° 4.1.

pour $s \in G$, par $\rho^*(s)$ l'automorphisme de $P(V)$ défini par $\rho(s)$, on a, pour tout $x \in G/B_0$ et tout $s \in G$, $\xi(s \cdot x) = \rho^*(s) \cdot \xi(x)$. On peut de plus supposer que Ω n'est contenu dans aucun hyperplan de $P(V)$.

Appliquons en effet la proposition 5 en prenant $H = B_0$. L'espace engendré par les transformés de e par les opérations de G est stable par G ; on peut donc supposer que c'est V tout entier. Soit φ l'application canonique de l'ensemble des éléments $\neq 0$ de V sur $P(V)$; le groupe de stabilité du point $e^* = \varphi(e)$ est B_0. Le morphisme $s \to \rho^*(s) \cdot e^*$ définit donc par passage aux quotients un morphisme bijectif ξ de G/B_0 dans $P(V)$; comme G/B_0 est complet, $\Omega = \xi(G/B_0)$ est une sous-variété fermée de $P(V)$; il est clair que Ω n'est contenu dans aucun hyperplan de $P(V)$. Si $x = tB_0$, $t \in G$, on a $s \cdot x = stB_0$, $\xi(s \cdot x) = \rho^*(st) \cdot e^* = \rho^*(s) \cdot (\rho^*(t) \cdot e^*) = \rho^*(s) \cdot \xi(x)$.

Les notations étant celles du corollaire précédent, soit de plus T un tore maximal de G. Il existe une base $(e_1, \ldots, e_n)$ de V telle que l'on ait, pour $t \in T$,

$$\rho(t) \cdot e_i = \chi_i(t)\, e_i \qquad (1 \leq i \leq n)\,,$$

les χ_i étant des caractères rationnels de T, qui peuvent être considérés comme des formes linéaires sur le groupe $\Gamma(T)$ des groupes à un paramètre de T. Si $\gamma \in \Gamma(T)$, on a

$$\rho(\gamma(\theta)) \cdot \sum_{i=1}^{n} a_i\, e_i = \sum_{i=1}^{n} a_i\, \theta^{c_i}\, e_i \quad (\theta \in K^*), \text{ avec } c_i = \langle \gamma, \chi_i \rangle\,.$$

Cette formule permet de déterminer explicitement $\gamma(0) \cdot x^*$ si x^* est un point quelconque de $P(V)$. Soit φ l'application canonique de l'ensemble des éléments $\neq 0$ de V sur $P(V)$, et soit $x^* = \varphi(\sum_{i=1}^{n} a_i\, e_i)$; posons $\varepsilon_i(\gamma, x) = 1$ si l'on a $a_i \neq 0$ et $\langle \gamma, \chi_i \rangle \leq \langle \gamma, \chi_j \rangle$ pour tout j tel que $a_j \neq 0$, $\varepsilon_i(\gamma, x) = 0$ dans le cas contraire. On a alors

$$\gamma(0) \cdot x^* = \varphi\,(\sum_{i=1}^{n} a_i\, \varepsilon_i(\gamma, x)\, e_i)\,.$$

On peut de même déterminer $\gamma(\infty) \cdot x^*$: on pose alors $\varepsilon'_i(\gamma, x) = 1$ si $a_i \neq 0$ et $\langle \gamma, \chi_i \rangle \geq \langle \gamma, \chi_j \rangle$ pour tout j tel que $a_j \neq 0$ et $\varepsilon'_i(\gamma, x) = 0$ dans le cas contraire, et on a

$$\gamma(\infty) \cdot x^* = \varphi\,(\sum_{i=1}^{n} a_i\, \varepsilon'_i(\gamma, x)\, e_i)\,.$$

On ne peut avoir $\gamma(0) \cdot x^* = \gamma(\infty) \cdot x^*$ que si les $\langle \gamma, \chi_i \rangle$ pour tous les i tels que $a_i \neq 0$ sont égaux, auquel cas on a $\gamma(\theta) \cdot x^* = x^*$ pour tout $\theta \in K^*$. On déduit de là le résultat suivant :

Proposition 6. – *Soient G un groupe algébrique affine connexe, B_0 un groupe de Borel de G et T un tore maximal de G. Si W est une sous-variété fermée de G/B_0 invariante par T, et si $\dim W > 0$, W contient au moins deux points distincts invariants par T.*

Soit γ un groupe à un paramètre semi-régulier de T (corollaire de la proposition 4). Comme il n'y a qu'un nombre fini de points de G/B_0 invariants par T (n° 9.3, corollaire 3 du théorème 1), ou, ce qui revient au même (proposition 3) par $\operatorname{Supp}\gamma$, il existe un point $x \in W$ tel que l'application $\theta \to \gamma(\theta) \cdot x$ ne soit pas constante. Les points $\gamma(0) \cdot x$ et $\gamma(\infty) \cdot x$ sont alors des points distincts de W invariants par T.

Corollaire. – *Si G est un groupe algébrique affine connexe non résoluble, tout tore maximal de G est contenu dans au moins deux groupes de Borel.*

Revenons maintenant aux notations utilisées plus haut, et cherchons à quelle condition γ est semi-régulier. Soit $\chi(\gamma)$ le plus petit des entiers $\langle \gamma, \chi_i \rangle$, et soit I l'ensemble des i tels que $\chi(\gamma) = \langle \gamma, \chi_i \rangle$. Supposons d'abord que I ne comporte qu'un seul élément i_0. Soit Ω_0 l'ensemble des points de Ω de la forme $\varphi(\sum_{i=1}^{n} a_i e_i)$ avec $a_{i_0} \neq 0$; c'est une partie ouverte non vide de Ω (car Ω n'est contenu dans aucun hyperplan), et on a $\gamma(0) \cdot x^* = \varphi(e_{i_0})$ pour tout $x^* \in \Omega_0$, et $\Omega - \Omega_0$ est stable par $\gamma(0)$. On en conclut que $\varphi(e_{i_0})$ est alors isolé dans l'ensemble des $\gamma(0) \cdot x^*$ ($x^* \in \Omega$), donc que γ est semi-régulier (proposition 1). Supposons au contraire que I contienne deux indices distincts i_0 et i_1 ; si c est un élément quelconque de K, il y a des points x^* de Ω tels que x^* soit de la forme $\varphi(\sum_{i=1}^{n} a_i e_i)$ avec $a_{i_0} \neq 0$, $a_{i_1} \neq 0$, $a_{i_1} \neq c a_{i_0}$: on en conclut immédiatement que l'ensemble des $\gamma(0) \cdot x^*$, $x^* \in \Omega$, est infini, donc que γ est singulier. On a donc le résultat suivant :

Proposition 7. – *Soient G un groupe algébrique affine connexe, B_0 un groupe de Borel de G, d la dimension de G/B_0, T un tore maximal de G, γ un groupe "semi-régulier" à un paramètre de T. Il existe un point x_0 et un seul de G/B_0 qui possède la propriété suivante : l'ensemble U_0 des $x \in G/B_0$ tels que $\gamma(0) \cdot x = x_0$ est dense dans G/B_0. L'ensemble U_0 est alors ouvert ; si $d > 0$, $G/B_0 - U_0$ est un ensemble non vide dont les composantes irréductibles sont de dimension $d - 1$.*

La dernière assertion résulte du lemme 5.

Corollaire. – *Si G/B_0 est de dimension > 1, tout tore maximal de G est contenu dans au moins trois groupes de Borel.*

Observons en effet que, si $t \in T$, t commute avec les éléments de $\operatorname{Supp}\gamma$, d'où il résulte immédiatement que $t \cdot (\gamma(0) \cdot x^*) = \gamma(0) \cdot (t \cdot x)$ pour tout $x \in G/B_0$. Si $x \in U_0$, on a $\gamma(0) \cdot x = x_0$, $x_0 = t \cdot x_0$, d'où $t \cdot x \in U_0$; chaque composante irréductible de $G/B_0 - U_0$ est donc invariante par T (corollaire

au lemme 1) et contient par suite au moins deux points invariants par T (proposition 6), à ajouter à x_0 lui aussi invariant par T.

10.4 Chambres

Les notations étant celles de la proposition 7, désignons par $B(\gamma)$ le stabilisateur de x_0 ; nous avons donc attaché intrinsèquement à tout élément semi-régulier γ de $\Gamma(T)$ un groupe de Borel $B(\gamma)$ contenant T.

Définition 2. – *Soit $\Gamma_{sr}(T)$ l'ensemble des groupes à un paramètre semi-réguliers de T. Pour tout groupe de Borel B contenant T, soit $\mathcal{C}(B)$ l'ensemble des $\gamma \in \Gamma_{sr}(T)$ tels que $B(\gamma) = B$; les ensembles non vides de la forme $\mathcal{C}(B)$ sont appelés les chambres de $\Gamma(T)$; si $\mathcal{C}(B) \neq \varnothing$, $\mathcal{C}(B)$ est appelé la chambre associée à B.*

Nous verrons d'ailleurs que $\mathcal{C}(B) \neq \varnothing$ pour tout groupe de Borel B contenant T.

Proposition 8. – *Soit G un groupe algébrique affine connexe non résoluble, et soit T un tore maximal de G. Il existe alors un tore singulier contenu dans T et de codimension* 1 *dans T.*

Reprenons en effet les notations utilisées plus haut ; soit x^* un point quelconque de Ω et soit W l'adhérence de $T \cdot x^*$. Le sous-espace X de V engendré par $\varphi^{-1}(W)$ est stable par les opérations de $\rho(T)$; il possède donc une base $(e'_1, \ldots, e'_m)$ telle que les sous-espaces Ke'_i soient stables par $\rho(T)$. Supposons que W soit de dimension $\delta > 0$: on peut considérer W comme une sous-variété fermée de l'espace projectif $P(X)$ associé à X ; l'image par φ du sous-espace de X engendré par $e'_2, \ldots, e'_m$ est un hyperplan H de $P(X)$ qui ne contient pas W et qui est invariant par T. Toute composante irréductible A de $H \cap W$ est invariante par T (corollaire au lemme 1) et est de dimension $\delta - 1$ (lemme 5). Si $\delta > 1$, les points de A, qui sont en nombre infini, ne sont pas tous invariants par T, et A contient un point x^* tel que $T \cdot x^*$ soit de dimension > 0 mais $< \delta$. Ce raisonnement montre que G/B_0 *contient un point x^* tel que l'adhérence de $T \cdot x^*$, que nous désignerons maintenant par W, soit de dimension* 1. Soit S_0 la composante neutre du groupe des éléments de T qui laissent x^* fixe ; il existe alors un morphisme de T/S_0 sur $T \cdot x^*$ tel que l'image réciproque de x^* par ce morphisme soit finie ; T/S_0 est donc de dimension 1. Comme T est commutatif, tous les points de $T \cdot x^*$ sont invariants par S_0, ce qui montre que S_0 est singulier.

Corollaire. – *Tout tore singulier contenu dans T est contenu dans un tore singulier contenu dans T et de codimension* 1 *dans T.*

Soient Q un tore singulier contenu dans T et Z son centralisateur dans G : Z n'est donc pas résoluble (proposition 2), et T en est un tore maximal. D'après la proposition 8, il existe un tore S contenu dans T, de codimension

1 dans T et qui est singulier relativement au groupe Z. Le centralisateur de S dans Z est le même que celui de SQ dans Z, puisque Q est dans le centre de Z ; il n'est pas résoluble, d'où[4] $SQ \neq T$; comme S est de codimension 1 dans T et que SQ est un sous-ensemble fermé irréductible de T, distinct de T, il s'ensuit que l'on a $SQ = S$, d'où $Q \subset S$. Par ailleurs le centralisateur de S dans G contient son centralisateur dans Z et n'est par suite pas résoluble, ce qui montre que S est un tore singulier dans G.

Observons maintenant que le groupe de Weyl W de T opère de manière naturelle dans $\Gamma(T)$; si s est un élément du normalisateur N de T et $\gamma \in \Gamma(T)$, l'application $\theta \to s\,\gamma(\theta)s^{-1}$ est encore un groupe à un paramètre de T, que nous désignerons par $s \cdot \gamma$; il est clair que $\gamma \to s \cdot \gamma$ est un automorphisme du groupe $\Gamma(T)$ qui ne dépend que de la classe w de s modulo le centralisateur de T ; aussi poserons nous $w \cdot \gamma = s \cdot \gamma$. L'application qui à tout $w \in W$ fait correspondre l'automorphisme $\gamma \to w \cdot \gamma$ est un homomorphisme de W dans le groupe des automorphismes de $\Gamma(T)$. *Cet homomorphisme est injectif.* En effet, si $w \cdot \gamma = \gamma$, et si s est un représentant de w, s commute avec tous les éléments de $\operatorname{Supp}\gamma$; comme la réunion des $\operatorname{Supp}\gamma$ est dense dans T (n° 9.5, proposition 3), on voit que, si $w \cdot \gamma = \gamma$ pour tout γ, s appartient au centralisateur de T, d'où $w = 1$. Le groupe W opère donc aussi de manière naturelle dans le groupe dual de $\Gamma(T)$, qui s'identifie comme nous l'avons vu au groupe $X(T)$ des caractères rationnels de T ; si χ est un élément de ce groupe et s un représentant de w dans N, on a

$$(w \cdot \chi)(t) = \chi(s^{-1}\,ts) \qquad (t \in T)\,.$$

En étendant le domaine des scalaires au corps $\mathbf{R}$ des nombres réels, on déduit de $\Gamma(T)$ et $X(T)$ des espaces vectoriels $\Gamma^{\mathbf{R}}(T)$, $X^{\mathbf{R}}(T)$ sur $\mathbf{R}$ en dualité l'un avec l'autre, et W opère encore de manière fidèle dans ces espaces vectoriels. Pour simplifier les notations, nous conviendrons d'identifier les éléments de W aux opérations dans $\Gamma(T)$, $X(T)$, $\Gamma^{\mathbf{R}}(T)$, $X^{\mathbf{R}}(T)$ qui leur sont associées.

Ceci étant, si γ est un groupe à un paramètre de T, et si w est une opération du groupe de Weyl, représentée par un élément s du normalisateur de T, les groupes de Borel qui contiennent $\operatorname{Supp} w \cdot \gamma$ sont évidemment les sBs^{-1}, où B parcourt l'ensemble des groupes de Borel qui contiennent $\operatorname{Supp}\gamma$; w transforme donc en lui-même l'ensemble des éléments semi-réguliers. De plus, on a, pour $\theta \in K^*$, $(w \cdot \gamma)(\theta) = s\,\gamma(\theta)\,s^{-1}$, d'où, pour $x \in G/B_0$,

$$((w \cdot \gamma)(0)) \cdot x = s \cdot (\gamma(0) \cdot (s^{-1} \cdot x))\,.$$

Supposons que γ soit semi-régulier et que $\gamma(0) \cdot x = x_0$ pour tout x d'une partie ouverte non vide U de G/B_0 ; on a alors $((w \cdot \gamma)(0)) \cdot x = s \cdot x_0$ pour tout $x \in s \cdot U_0$, et par suite

[4] En effet, le centralisateur dans Z du tore maximal T de Z est nilpotent, donc résoluble, d'après le théorème 1 du n° 7.1.

$$B(w \cdot \gamma) = sB(\gamma)s^{-1} .$$

Comme on sait (n° 9.3, corollaire 3 du théorème 1) que les groupes de Borel contenant T sont permutés entre eux de manière simplement transitive par les opérations du normalisateur de T, on en déduit le résultat suivant :

Proposition 9. – *Pour tout groupe de Borel B contenant le tore maximal T, il existe une chambre $\mathcal{C}(B)$ de $\Gamma(T)$ associée à B ; les opérations du groupe de Weyl dans $\Gamma(T)$ permutent les chambres entre elles de manière simplement transitive.*

Proposition 10. – *Soit $\mathcal{C}$ une chambre de $\Gamma(T)$; il existe un certain nombre de formes linéaires $\lambda_1, \ldots, \lambda_m$ sur $\Gamma(T)$ telles que $\mathcal{C}$ soit l'ensemble des $\gamma \in \Gamma(T)$ tels que $\lambda_i(\gamma) > 0$ $(1 \leq i \leq m)$.*

En effet, on a vu qu'il existe des formes linéaires $\chi_1, \ldots, \chi_n$ sur $\Gamma(T)$ et un indice i_0 tels que $\mathcal{C}$ soit l'ensemble des γ tels que $\chi_{i_0}(\gamma) < \chi_i(\gamma)$ pour tout $i \neq i_0$.

11. Le groupe de Weyl : chambres et réflexions[1]

11.1 Préliminaires géométriques (polyèdres convexes)

Soit E un espace vectoriel de dimension finie sur le corps $\mathbf{Q}$ des nombres rationnels. On considère sur $\mathbf{Q} \times E$ la topologie produit de la topologie usuelle de $\mathbf{Q}$ (noter que la topologie de E est déterminée par sa structure de groupe "abstrait").

Soit $\mathcal{L}$ l'ensemble des formes linéaires non nulles sur E (ou des formes linéaires affines non constantes). Si $L \in \mathcal{L}$, nous noterons respectivement L^0, L^+ et L^- l'ensemble des $x \in E$ tels que $L(x) = 0$, $L(x) > 0$, $L(x) < 0$; en particulier, L^0 est l'hyperplan déterminé par L.

Lemme 1. – *La réunion d'un nombre fini d'hyperplans de E ne contient aucun ouvert non vide de E.*

Lemme 2. – *Soient L_1 et L_2 dans $\mathcal{L}$. S'il existe $x \in L_1^0 \cap L_2^0$ et un voisinage U de x tel que $U \cap L_1^+ \subset L_2^+$, alors on a $L_1^+ = L_2^+$, $L_1^0 = L_2^0$ et $L_1 = aL_2$, avec $a \in \mathbf{Q}$, $a > 0$.*

Les démonstrations s'obtiennent facilement en se ramenant au cas où $\dim E = 1$ ou 2.

Proposition 1. – *Soient $L_1, \ldots, L_k$ dans $\mathcal{L}$ et $D = \bigcap_{1 \le i \le k} L_i^+$. On suppose que D n'est pas vide et que sa représentation comme intersection de demi-espaces est minimale ; autrement dit, si l'on pose $D_j = \bigcap_{i \neq j} L_i^+$, on a $D_j \neq D$ pour $1 \le j \le k$. Alors :*

a) *$F_i = D_i \cap L_i^0$ est non vide et relativement ouvert dans L_i^0 ($1 \le i \le k$).*

b) *Les hyperplans L_i^0 sont déterminées par D. Plus précisément, pour qu'un demi-espace L^+ ($L \in \mathcal{L}$) coïncide avec l'un des L_i^+, il faut et il suffit qu'il existe $x \in L^0$ et un voisinage U de x tel que $U \cap L^+ = U \cap D$.*

c) *La frontière de D est la réunion des adhérences des F_i ($1 \le i \le k$).*

Démonstration. a) On note $\overline{L}_i^+$ l'adhérence $L_i^+ \cup L_i^0$ de L_i^+ ; notation analogue pour $\overline{L}_i^-$. On ne peut avoir $D_i \subset L_i^+$ (car $D_i \neq D$), ni $D_i \subset L_i^-$ (car $D \neq \varnothing$). On peut donc trouver des points $x \in D_i \cap \overline{L}_i^+$ et $y \in D_i \cap \overline{L}_i^-$. Le segment $[x, y]$ (ensemble des points $tx + (1-t)y$, avec $t \in \mathbf{Q}$, $0 \le t \le 1$) est tout entier

[1] Exposé de M. Lazard, le 18.2.1957

dans D_i et rencontre L_i^0 en un point. D'où $F_i \neq \varnothing$, et F_i est évidemment ouvert dans L_i^0.

b) D est ouvert dans E, et il est clair que $F_j \subset \overline{D} - D$ $(1 \leq j \leq k)$. Donc $\overline{D} - D \supset \bigcup_j \overline{F}_j$. Réciproquement, soit $x \in \overline{D} - D$; on a $x \in \overline{L}_j^+$ pour tout j, et $x \in L_{j_0}^0$ pour un indice j_0 (au moins). Prenons $y \in F_{j_0}$; alors x est adhérent au segment semi-ouvert $]x, y]$ (ensemble des points $tx + (1-t)y$, $0 \leq t < 1$) qui est entièrement contenu dans F_{j_0}. Donc $\overline{D} - D \subset \bigcup_j \overline{F}_j$.

c) Si L^+ est l'un des L_i^+, la condition est vérifiée d'après a). Réciproquement, soient $x \in L^0$, U un voisinage de x tel que $U \cap L^+ = U \cap D$. Alors $x \in \overline{D} - D$, et il existe un i tel que $x \in L_i^0$ et $D \subset L_i^+$ d'où $U \cap L^+ \subset L_i^+$. On applique alors le lemme 2, d'où $L^0 = L_i^0$.

Définitions. Une partie D de E sera appelée une *chambre* (de E) si c'est l'intersection non vide d'un nombre fini de demi-espaces ouverts L_i^+. Si l'on suppose que $\{L_i^+\}$ est un système minimal (donc minimum, d'après la proposition 1) de définition de D, les hyperplans L_i^0 seront appelés les *hyperplans limitrophes* de la chambre D. Les parties $F_i = L_i^0 \cap \bigcap_{j \neq i} L_j^+$ seront appelées les *murs* de D.

Chaque mur d'une chambre D est évidemment une chambre dans l'hyperplan limitrophe qui le contient ; on peut donc considérer ses murs relativement à cet hyperplan, etc. On appellera *arête* de D toute face de codimension ≥ 2 (*i.e.* tout mur relatif d'un mur de D ou d'une arête de dimension supérieure).

D'après la proposition 1, c), l'adhérence de D est la réunion de D, de ses murs et de ses arêtes.

Proposition 2. – *Soit $\{D(i)\}$ une famille finie de chambres de E $(1 \leq i \leq r)$. On suppose que les $D(i)$ sont deux à deux disjointes et que la réunion de leurs adhérences est E. Si D et D' sont deux quelconques des chambres $D(i)$, il existe une suite d'indices $i_1, \ldots, i_k$ (entre 1 et r) telle que la suite de chambres $D = D(i_1), \ldots, D(i_k) = D'$ ait la propriété suivante : deux chambres consécutives ont un hyperplan limitrophe commun et leurs murs contenus dans cet hyperplan ont une intersection non vide.*

Démonstration. On se ramènera au cas où $\dim E = 1$. Choisissons un $x \in D$ qui ne soit contenu dans aucun hyperplan limitrophe des chambres $D(i)$, puis un $y \in D'$ qui ne soit contenu dans aucun des hyperplans engendrés par x et les arêtes de codimension 2 de ces chambres $D(i)$ (*cf.* lemme 1). Il suffit alors de prendre les chambres $D = D(i_1), \ldots, D(i_k) = D'$ qui intersectent sur le segment $[x, y]$ des intervalles ouverts non vides, ces chambres étant ordonnées comme les intervalles correspondants. D'après le choix de x et y, les intervalles $D(i_j) \cap [x, y]$ et $D(i_{j+1}) \cap [x, y]$ ont un point frontière commun, qui est contenu dans l'intersection d'un mur de $D(i_j)$ et d'un mur de $D(i_{j+1})$. Il résulte facilement du lemme 2 et de la proposition 1 que ces murs sont portés par le même hyperplan.

11.2 Quelques précisions sur T, $X(T)$, $\Gamma(T)$ et $\Gamma^{\mathbf{Q}}(T)$

Soit T un tore de dimension n, *i.e.* un groupe algébrique isomorphe à $(K^*)^n$. On a étudié au n° 4.3 les relations entre T et son groupe des caractères $X(T) = \mathrm{Hom}(T, K^*)$, où Hom signifie "homomorphismes de groupes algébriques". On a vu que $X(T)$ est isomorphe à $\mathbf{Z}^n$, et que T et $X(T)$ sont en dualité par rapport à K^*, *i.e.* que $T = \mathrm{Hom}(X(T), K^*)$, où Hom signifie "homomorphismes de groupes discrets". On en a déduit, par transposition, $\mathrm{Hom}(T_1, T_2) \simeq \mathrm{Hom}(X(T_2), X(T_1))$, relation valable pour deux tores T_1 et T_2 et leurs duaux $X(T_1)$ et $X(T_2)$.

Par définition, on a $\Gamma(T) = \mathrm{Hom}(K^*, T)$. Comme $X(K^*) \simeq \mathbf{Z}$ (canoniquement), on a $\Gamma(T) \simeq \mathrm{Hom}(X(T), \mathbf{Z})$, ainsi qu'on l'a vu au n° 9.5. Ainsi T et $\Gamma(T)$ peuvent être considérés chacun comme le bidual de l'autre, la dualité étant prise par rapport à K^* puis à $\mathbf{Z}$, ou vice versa. Si l'on a deux tores T_1 et T_2, $\mathrm{Hom}(T_1, T_2)$ s'identifie, par bitransposition, à $\mathrm{Hom}(\Gamma(T_1), \Gamma(T_2))$. On peut dire que $T \to \Gamma(T)$ est un foncteur covariant additif qui applique la catégorie additive des tores sur la catégorie additive des groupes abéliens libres de type fini ; on a de même le foncteur réciproque : $\Gamma(T) \to T$. Il en résulte que le groupe des automorphismes algébriques $\mathrm{Aut}(T)$ s'identifie au groupe des automorphismes de groupe discret $\mathrm{Aut}(\Gamma(T))$. C'est ainsi que nous ferons opérer le groupe de Weyl d'un tore maximal T sur le groupe $\Gamma(T)$.

Une décomposition de T en produit direct de deux sous-tores entraîne une décomposition de $\Gamma(T)$ en somme directe de deux sous-groupes, et réciproquement. Pour qu'un sous-groupe $H \subset \Gamma(T)$ soit facteur direct, il faut et il suffit que le quotient $\Gamma(T)/H$ soit sans torsion ; un tel H est dit *primitif*. Le sous-tore de T qui lui correspond est Q, égal à l'adhérence de $\bigcup_{\gamma \in H} \mathrm{Supp}\,\gamma$. Réciproquement, à tout sous-tore Q de T correspond un sous-groupe primitif H de $\Gamma(T)$: $\gamma \in H$ équivaut à $\mathrm{Supp}\,\gamma \subset Q$; on dira que Q et H sont associés. Soient $H_1, \ldots, H_k$ des sous-groupes primitifs de $\Gamma(T)$, $Q_1, \ldots, Q_k$ les sous-tores associés ; alors $\bigcap_i H_i$ est associé à la composante neutre de $\bigcap_i Q_i$.

Au lieu de considérer, comme dans l'exposé 9, l'espace vectoriel $\Gamma^{\mathbf{R}}(T) = \mathbf{R} \otimes_{\mathbf{Z}} \Gamma(T)$ sur $\mathbf{R}$, nous introduisons l'espace vectoriel sur $\mathbf{Q}$: $\Gamma^{\mathbf{Q}}(T) = \mathbf{Q} \otimes_{\mathbf{Z}} \Gamma(T)$, et nous identifions $\Gamma(T)$ à un sous-groupe de $\Gamma^{\mathbf{Q}}(T)$. Tout $x \in \Gamma^{\mathbf{Q}}(T)$ peut s'écrire sous la forme $(1/n)y$, avec $y \in \Gamma(T)$ et n entier > 0. Soient H un sous-groupe de $\Gamma(T)$, $H^{\mathbf{Q}}$ le sous-espace vectoriel de $\Gamma^{\mathbf{Q}}(T)$ engendré par H ; alors $H = \Gamma(T) \cap H^{\mathbf{Q}}$ si et seulement si H est primitif. Comme tout sous-espace de $\Gamma^{\mathbf{Q}}(T)$ est engendré par son intersection avec $\Gamma(T)$, on voit qu'il existe une correspondance biunivoque entre sous-tores de T et sous-espaces de $\Gamma^{\mathbf{Q}}(T)$.

Enfin nous pouvons identifier le groupe $\mathrm{Aut}(\Gamma(T))$ à un sous-groupe de $\mathrm{Aut}(\Gamma^{\mathbf{Q}}(T))$. C'est ainsi que nous ferons opérer sur $\Gamma^{\mathbf{Q}}(T)$ le groupe de Weyl d'un tore maximal T.

11.3 La décomposition en chambres de $\Gamma^{\mathbf{Q}}(T)$

On considère un tore maximal T d'un groupe algébrique affine connexe non résoluble G.

Définition 1. – *Soient H un sous-espace vectoriel de $\Gamma^{\mathbf{Q}}(T)$ et Q le sous-tore de T associé à H. Nous dirons que H est semi-régulier (*resp. *régulier, singulier) si Q est semi-régulier (*resp. *régulier, singulier). Si $x \in \Gamma^{\mathbf{Q}}(T)$, nous dirons que x est semi-régulier (resp. etc.) si le sous-espace $\mathbf{Q}x$ qu'il engendre est semi-régulier (resp. etc.).*

Lorsque $x = \gamma \in \Gamma(T)$, cette définition coïncide avec la précédente (fin du n° 10.2). En effet, $\mathrm{Supp}\,\gamma$ est le sous-tore associé au sous-espace $\mathbf{Q}x$ de $\Gamma^{\mathbf{Q}}(T)$.

Lemme 3. – *Si un sous-espace vectoriel H de $\Gamma^{\mathbf{Q}}(T)$ est semi-régulier, l'ensemble des éléments semi-réguliers de H est dense dans H.*

Le lecteur trouvera la démonstration (d'ailleurs facile) développée à propos de la proposition 3 du n° 9.5 et de la proposition 4 du n° 10.2.

Définition 2. – *Soit $\mathcal{C}(B)$ la chambre de Weyl[2] associée au groupe de Borel $B \supset T$ dans $\Gamma(T)$. Nous appellerons chambre de Weyl associée à B dans $\Gamma^{\mathbf{Q}}(T)$ l'ensemble $\mathcal{C}^{\mathbf{Q}}(B)$ des $x \in \Gamma^{\mathbf{Q}}(T)$ tels qu'il existe un entier $n > 0$ avec $nx \in \mathcal{C}(B)$.*

Comme tout élément semi-régulier de $\Gamma(T)$ est dans une chambre de Weyl, la réunion des chambres de Weyl $\mathcal{C}^{\mathbf{Q}}(B)$ est l'ensemble des éléments semi-réguliers de $\Gamma^{\mathbf{Q}}(T)$.

Théorème 1. – *A tout groupe de Borel $B \supset T$ correspond une chambre de Weyl $\mathcal{C}^{\mathbf{Q}}(B)$ et une seule. On a $\mathcal{C}^{\mathbf{Q}}(B) \cap \Gamma(T) = \mathcal{C}(B)$, et $\mathcal{C}^{\mathbf{Q}}(B)$ est une chambre dans $\Gamma^{\mathbf{Q}}(T)$ au sens du n° 11.1. Les hyperplans limitrophes des chambres $\mathcal{C}^{\mathbf{Q}}(B)$ sont les hyperplans singuliers de $\Gamma^{\mathbf{Q}}(T)$; ils sont associés aux sous-tores singuliers de codimension 1 de T. Tout sous-espace singulier de $\Gamma^{\mathbf{Q}}(T)$ est contenu dans l'un de ces hyperplans limitrophes, dont la réunion est l'ensemble des éléments singuliers de $\Gamma^{\mathbf{Q}}(T)$.*

Démonstration. D'après les propositions 9 et 10 du n° 10.4, à tout groupe de Borel $B \supset T$ est associée une chambre de Weyl et une seule $\mathcal{C}(B)$ dans $\Gamma(T)$, et celle-ci est définie comme l'ensemble des points où un nombre fini de

[2] Voir la définition 2 du n° 10.4.

formes linéaires sont strictement positives. Il en résulte que $\mathcal{C}^{\mathbf{Q}}(B)$ est défini par le même système d'inégalités strictes, et que $\mathcal{C}(B) = \mathcal{C}^{\mathbf{Q}}(B) \cap \Gamma(T)$.

Soit $\{L_i(\gamma) > 0\}$ un système minimal d'inégalités définissant une chambre de Weyl $\mathcal{C}(B)$ et la chambre étendue $\mathcal{C}^{\mathbf{Q}}(B)$. Si l'on se reporte au critère de semi-régularité pour les éléments de $\Gamma(T)$ (précédant la proposition 7 du n° 10.3), on voit que tout point frontière de $\mathcal{C}^{\mathbf{Q}}(B)$ est singulier. Tout hyperplan limitrophe d'une chambre contient un mur, donc un ensemble relativement ouvert non vide d'éléments singuliers. D'après le lemme 3, cet hyperplan est singulier.

La réunion des chambres de Weyl $\mathcal{C}^{\mathbf{Q}}(B)$ et de leurs hyperplans limitrophes est fermée dans $\Gamma^{\mathbf{Q}}(T)$. L'ensemble ouvert complémentaire est vide ; sinon il contiendrait un élément semi-régulier[3] qui serait contenu dans l'une des chambres. Enfin tout sous-espace singulier est contenu dans l'un des hyperplans singuliers, d'après le corollaire de la proposition 8 du n° 10.4.

La décomposition de $\Gamma^{\mathbf{Q}}(T)$ peut être résumée ainsi : soient, comme au n° 11.1, $\{L_i^0\}$ les hyperplans singuliers, L_i^+ et L_i^- les deux demi-espaces ouverts séparés par L_i^0. Alors les chambres de Weyl sont les parties non vides de la forme $\bigcap_i L_i^{\varepsilon(i)}$, où chaque $\varepsilon(i)$ est l'un des signes + ou −. Il résulte alors de la proposition 1 que les murs des chambres de Weyl sont les parties non vides de la forme $L_i^0 \cap \bigcap_{j \neq i} L_j^{\varepsilon(j)}$, où chaque $\varepsilon(j)$ est l'un des signes + ou −. L'énoncé suivant en résulte.

Corollaire. – *Si deux chambres de Weyl distinctes $\mathcal{C}^{\mathbf{Q}}(B)$ et $\mathcal{C}^{\mathbf{Q}}(B')$ sont telles que les réunions respectives de leurs murs aient une intersection non vide, ces deux chambres ont exactement un mur commun et sont situées de part et d'autre de l'hyperplan limitrophe commun. Chaque mur est commun à deux chambres.*

Lemme 4. – *Soit H un sous-espace vectoriel de $\Gamma^{\mathbf{Q}}(T)$, Q le sous-tore de T associé. Pour qu'un automorphisme de T induise l'identité sur Q, il faut et il suffit que l'automorphisme associé de $\Gamma^{\mathbf{Q}}(T)$ induise l'identité sur H.*

Résultat évident, si l'on se rappelle que pour $\gamma \in \Gamma(T)$ et un automorphisme σ de T, $\sigma\gamma$ est défini par $(\sigma\gamma)(\theta) = \sigma(\gamma(\theta))$ et que la réunion des Supp γ pour $\gamma \in H \cap \Gamma(T)$ est dense dans Q.

Théorème 2. – *Soient H un hyperplan singulier de $\Gamma^{\mathbf{Q}}(T)$, Q le tore singulier de codimension 1 associé. Il existe une opération et une seule w du groupe de Weyl W qui est distincte de 1 (élément neutre de W) et induit l'identité sur H (resp. sur Q) ; cette opération est involutive, et sera dite la réflexion par rapport à H (ou à Q). L'espace vectoriel $\Gamma^{\mathbf{Q}}(T)$ est somme directe de l'hyperplan H et de la droite "orthogonale" H_1 ; on a $w(x)+x = 0$*

[3] Car l'ensemble des éléments semi-réguliers de $\Gamma^{\mathbf{Q}}(T)$ est dense dans $\Gamma^{\mathbf{Q}}(T)$ d'après le lemme 3.

pour tout $x \in H_1$. Le tore T est produit (non nécessairement direct) de Q et du sous-tore "orthogonal" Q_1 de dimension 1, associé à H_1 ; on a $w(t)t = e$ pour tout $t \in Q_1$, donc $w(t)t \in Q$ pour tout $t \in T$. Le groupe de Weyl est engendré par les réflexions par rapport aux hyperplans limitrophes d'une chambre de Weyl donnée.

Démonstration. Les opérations de W sur T sont induites par les automorphismes intérieurs de G associés aux éléments du normalisateur N de T. Pour que $w : t \to sts^{-1}$ soit l'identité sur un tore $Q \subset T$, il faut et il suffit que $s \in Z(Q)$, centralisateur de Q. Suivant que Q est ou non semi-régulier, $Z(Q)$ est ou non résoluble (n° 10.2, proposition 2), et le normalisateur de T dans $Z(Q)$ (*i.e.* $Z(Q) \cap N$) est confondu ou non avec son centralisateur (n° 10.3, proposition 6). De là résulte l'existence d'au moins un élément de W distinct de 1 et induisant l'identité sur un tore singulier Q de codimension 1, *i.e.* sur l'hyperplan singulier H associé. Soient $\mathcal{C}_1$ et $\mathcal{C}_2$ deux chambres ayant un mur commun M dans H. On a $w\,\mathcal{C}_1 = \mathcal{C}_1$ ou $w\,\mathcal{C}_1 = \mathcal{C}_2$ car on a $wM = M$ et $\mathcal{C}_1, \mathcal{C}_2$ sont les seules chambres ayant M comme mur (corollaire du théorème 1). Mais $w\,\mathcal{C}_1 = \mathcal{C}_1$ impliquerait $w = 1$, puisque W opère d'une manière simplement transitive sur les chambres. Donc $w\,\mathcal{C}_1 = \mathcal{C}_2$. Si w' est un autre élément $\neq 1$ de W conservant ponctuellement H, on a $(ww')\,\mathcal{C}_1 = \mathcal{C}_1$, donc $ww' = 1$; en particulier : $w^2 = 1$ et $w = w'$. L'espace vectoriel $\Gamma^{\mathbf{Q}}(T)$ est alors somme directe de H et de H_1, noyau de $1 + w$. Comme H est un hyperplan, H_1 est de dimension 1. Si Q_1 est le sous-tore de T associé à H_1, Q_1 est de dimension 1, $Q \cap Q_1$ est fini (car $H \cap H_1 = 0$) donc QQ_1 est un tore contenu dans T, contenant strictement Q, donc égal à T. Si $\gamma \in H_1 \cap \Gamma(T)$, on a $w(\gamma) = -\gamma$, autrement dit $w(\gamma(\theta)) = (\gamma(\theta))^{-1}$ pour $\theta \in K^*$, *i.e.* $w(t) = t^{-1}$ pour $t \in Q_1$.

Soient $\mathcal{C}$ une chambre de Weyl, $H_1, \ldots, H_s$ ses hyperplans limitrophes, $w_1, \ldots, w_s$ les réflexions correspondantes, $W_0 \subset W$ le sous-groupe qu'elles engendrent. Pour établir que W_0 est égal à W, il suffit de prouver que W_0 opère transitivement sur les chambres. Or soient $w \in W_0$, $\mathcal{C}' = w\,\mathcal{C}$, H' un hyperplan limitrophe de $\mathcal{C}'$; alors $w^{-1}H'$ est un hyperplan limitrophe de $\mathcal{C}$, soit H_i ; de plus, $ww_i\,w^{-1}$ est la réflexion par rapport à H' et $ww_i\,\mathcal{C}$ est la chambre symétrique de $\mathcal{C}'$ par rapport à H'. Il résulte alors de la proposition 2 et du théorème 1 que W_0 opère transitivement sur les chambres.

11.4 Où l'on retrouve les schémas de Dynkin

Prenons sur $\Gamma^{\mathbf{Q}}(T)$ une forme quadratique définie positive, invariante par W. Les réflexions par rapport aux hyperplans limitrophes sont alors des réflexions au sens usuel. Notons $\langle x, y \rangle$ le produit scalaire dans $\Gamma^{\mathbf{Q}}(T)$.

Soient $\mathcal{C}$ une chambre de Weyl, $H_1, \ldots, H_s$ ses hyperplans limitrophes. Associons à chaque H_i un vecteur v_i bien déterminé par les conditions suivantes : $v_i \in \Gamma(T)$ est un générateur de $\Gamma(T) \cap H_i'$, où H_i' désigne la droite

de $\Gamma^{\mathbf{Q}}(T)$ orthogonale à H_i, et $\langle v_i, x\rangle > 0$ pour tout $x \in \mathcal{C}$. La réflexion w_i par rapport à H_i s'écrit alors :

$$w_i \ : x \to x - 2\,\frac{\langle v_i, x\rangle}{\langle v_i, v_i\rangle}\, v_i\,.$$

En effet, $w_i(x) - x \in H_i'$ et $w_i(x) + x \in H_i$. Comme W conserve $\Gamma(T)$, il en résulte que : $-2\,\frac{\langle v_i,x\rangle}{\langle v_i,v_i\rangle}\, v_i \in \Gamma(T)$ pour tout $x \in \Gamma(T)$, donc que $-2\,\frac{\langle v_i,x\rangle}{\langle v_i,v_i\rangle}$ est entier pour tout $x \in \Gamma(T)$. En particulier, $a_{ij} = -2\,\frac{\langle v_i,v_j\rangle}{\langle v_i,v_i\rangle} \in \mathbf{Z}$ pour tout couple i, j.

Proposition 3. – *Pour $i \neq j$, on a $a_{ij} \geq 0$.*

Démonstration. En effet, $w_i(v_j)$ est orthogonal à l'hyperplan limitrophe $w_i H_j$, donc $\langle w_i(v_j), x\rangle = \langle v_j + a_{ij} v_i, x\rangle$ garde un signe constant pour $x \in \mathcal{C}$.

On ne peut avoir $\langle v_j + a_{ij} v_i, x\rangle < 0$ pour $x \in \mathcal{C}$, car on a $\langle v_i, x\rangle > 0$, $\langle v_j, x\rangle > 0$ pour $x \in \mathcal{C}$ et a_{ij} devrait être strictement négatif. Mais alors, pour $x \in \Gamma^{\mathbf{Q}}(T)$, les inégalités :

$$\langle (-a_{ij})v_i - v_j, x\rangle > 0 \ \ ; \ \langle v_k, x\rangle > 0 \quad \text{pour} \quad k \neq i$$

impliqueraient $\langle v_i, x\rangle > 0$. D'après la proposition 1, l'hyperplan H_i ne serait pas limitrophe. On a donc $\langle v_j + a_{ij} v_i, x\rangle > 0$ pour $x \in \mathcal{C}$.

Si $a_{ij} < 0$, les inégalités :

$$\langle v_j + a_{ij} v_i, x\rangle > 0 \ \ ; \ \langle v_k, x\rangle > 0 \quad \text{pour} \quad k \neq j$$

impliqueraient $\langle v_j, x\rangle > 0$. Pour la même raison, H_j ne serait pas limitrophe. Ainsi $a_{ij} \geq 0$. C.Q.F.D.

Montrons enfin que les s vecteurs v_i sont linéairement indépendants. Une relation non triviale de dépendance linéaire $\sum\limits_i n_i v_i = 0$ ($n_i \in \mathbf{Q}$) peut s'écrire $\sum\limits_\alpha n_\alpha v_\alpha = \sum\limits_\beta n_\beta v_\beta$, avec des n_α et $n_\beta > 0$, α et β parcourant des ensembles d'indices disjoints. Mais alors on a $\langle v_\alpha, v_\beta\rangle \leq 0$ pour chaque paire α, β, d'après la proposition 3, d'où

$$0 \leq \langle \sum_\alpha n_\alpha v_\alpha, \sum_\alpha n_\alpha v_\alpha\rangle = \langle \sum_\alpha n_\alpha v_\alpha, \sum_\beta n_\beta v_\beta\rangle = \sum_{\alpha,\beta} n_\alpha n_\beta \langle v_\alpha, v_\beta\rangle \leq 0\,.$$

Donc, $\sum\limits_\alpha n_\alpha v_\alpha = 0$. Mais, pour $x \in \mathcal{C}$, on a $\langle \sum\limits_\alpha n_\alpha v_\alpha, x\rangle = \sum\limits_\alpha n_\alpha \langle v_\alpha, x\rangle > 0$, d'où contradiction.

En conclusion, nous avons obtenu une famille de vecteurs linéairement indépendants v_i, tels que $-2\,\frac{\langle v_i,v_j\rangle}{\langle v_i,v_i\rangle}$ soit un entier ≥ 0 pour $i \neq j$. Une telle famille se décompose en sous-familles deux à deux orthogonales, où chaque

sous-famille est isomorphe (à un facteur constant près si l'on veut normer la métrique) au système des racines simples d'une algèbre de Lie simple (en caractéristique 0). Le lecteur trouvera la classification de ces familles de vecteurs dans l'exposé 13 du Séminaire "Sophus Lie" (E.N.S. 1954/55).

12. Racines[1]

12.1 Groupes de Weyl d'ordre 2

Dans tout ce n°, G désignera un groupe algébrique affine connexe dont le groupe de Weyl est d'ordre 2.

Lemme 1. – a) *Si B est un groupe de Borel de G, la variété $\Omega = G/B$ est isomorphe à une droite projective.*

b) *Il existe un épimorphisme rationnel de G sur le groupe projectif à 2 variables* $\mathrm{PL}(2, K)$ *dont le noyau est l'intersection des groupes de Borel.*

Démonstration. Ω n'est pas réduit à un point, puisque G n'est pas résoluble ; on a $\dim \Omega \leq 1$ puisque le groupe de Weyl est d'ordre 2 (n° 10.3, corollaire de la proposition 7) ; donc Ω est une courbe. Soit T un tore maximal de G. Il laisse invariants précisément deux points de Ω (n° 9.3, corollaire 3 du théorème 1), et il existe donc un tore de dimension 1, $Q \subset T$, qui n'opère pas trivialement sur Ω. Si $x_1 \in \Omega$ n'est pas invariant par Q (donc aussi non invariant par T), l'ensemble Qx_1 des points sx_1 ($s \in Q$) est épais et non réduit à un point, donc ouvert dans la courbe Ω. Le corps $K(\Omega)$ des fonctions rationnelles sur Ω coïncide avec celui des fonctions sur Qx_1, qui est un sous-corps du corps des fonctions rationnelles sur Q. D'après le théorème de Lüroth (v.d. Waerden, *Moderne Algebra*, 2ème éd., §63) le corps des fonctions rationnelles sur Ω est donc une extension transcendante pure de K. Comme Ω est une courbe complète et sans singularités, il en résulte que Ω est une droite projective.

Notons x_0 et x_∞ les deux points de Ω invariants par T, et ζ la fonction rationnelle sur Ω, bien déterminée par les conditions d'avoir un seul zéro simple en x_0, un seul pôle simple en x_∞, et d'être égale à 1 en x_1 (qui a été choisi non invariant par T, donc distinct de x_0 et x_∞). Pour $g \in G$, $x \in \Omega$, posons $(g\zeta)(x) = \zeta(g^{-1}x)$. Alors g définit un automorphisme de la droite projective Ω, donc la fonction $g\zeta$ est de la forme $(a\zeta + b)(c\zeta + d)^{-1}$, avec $a, b, c, d \in K$. Plus précisément, si l'on note $(\alpha, \beta, \gamma, \delta)$ le "birapport" des 4 quantités $\alpha, \beta, \gamma, \delta \in \overline{K}$ ($\overline{K} = K \cup \{\infty\}$), *i.e.* la quantité $(\alpha - \gamma)(\beta - \delta)(\alpha - \delta)^{-1}(\beta - \gamma)^{-1}$, on a

$$g\zeta = (\zeta, \zeta(gx_1), \zeta(gx_0), \zeta(gx_\infty)),$$

[1] Exposé de M. Lazard, le 11.3.1957

d'après l'invariance du "birapport" par les transformations homographiques. Comme $g \to \zeta(gx)$ est une fonction rationnelle sur G pour tout $x \in \Omega$, l'homomorphisme $g \to (\zeta \to g\zeta)$ est un homomorphisme rationnel de G dans $\mathrm{PL}(2, K)$.

Soient B_0 et B_∞ les deux groupes de Borel de G contenant T, qui sont les stabilisateurs respectifs de x_0 et de x_∞. Pour $s \in B_\infty$, on a : $s\zeta = a(s)\zeta + b(s)$. L'application $s \to a(s)$ est un homomorphisme rationnel de B_∞ dans K^* dont le noyau contient B_∞^u (partie unipotente de B_∞) mais non T. En effet, on a $b(t) = 0$ pour tout $t \in T$, et T n'opère pas trivialement sur Ω. La restriction de a à T est donc un épimorphisme de T sur K^*. De même, la restriction de b à B_∞^u est un épimorphisme de B_∞^u sur le groupe additif K. En effet, cette restriction est un homomorphisme, et si ce n'était par un épimorphisme $b(B_\infty^u)$ serait un sous-groupe fermé connexe de K distinct de K, donc réduit à 0, et $B_\infty = B_\infty^u T$ laisserait x_0 invariant, ce qui est impossible.

Pour tout $\alpha \in K^*$, $\beta \in K$, on peut donc trouver $t \in T$ et $s \in B_\infty^u$ tels que $a(t) = \alpha$, $b(s) = \beta$, d'où $(ts)\zeta = \alpha\zeta + \beta$. Autrement dit, les opérations de B_∞ sur Ω sont tous les automorphismes algébriques qui laissent invariant x_∞. Le même raisonnement s'applique à B_0 et x_0. Comme tout automorphisme de Ω est le produit de deux automorphismes laissant fixe respectivement x_0 et x_∞, les opérations de G sur Ω sont tous les automorphismes rationnels de Ω ; autrement dit, $G \to \mathrm{PL}(2, K)$ est un épimorphisme rationnel.

Lemme 2. – *Soient R le radical de G, R' l'intersection de ses groupes de Borel, T un tore maximal contenu dans un groupe de Borel B, et B^u, R^u, R'^u les parties unipotentes de B, R, R' respectivement. Alors :*

a) *$R^u = R'^u$ est un sous-groupe fermé invariant de B^u. Le quotient B^u/R^u est isomorphe au groupe additif K.*

b) *Soit f un épimorphisme de B^u sur K qui, par passage au quotient, définit un isomorphisme de B^u/R^u sur K. Pour tout $t \in T$, $s \in B^u$, on a $f(tst^{-1}) = \alpha(t)f(s)$, où α est un caractère rationnel de T indépendant du choix de f dont le noyau est $T \cap R' \neq T$.*

Démonstration. Reprenons les notations de la démonstration précédente avec $B = B_\infty$. Le radical R est par définition (n° 9.4, définition 2) la composante neutre de R'. Comme $R' \subset B$, $R'^u = B^u \cap R'$ est un sous-groupe invariant fermé de G et R^u est sa composante neutre. Le quotient R'^u/R^u est donc un p-groupe fini[2].

Nous avons introduit un épimorphisme b de B^u sur K dont le noyau est R'^u. Il en résulte que B^u/R'^u est un groupe connexe unipotent de dimension 1, donc isomorphe à K (n° 7.4, théorème 4) ; il en est de même de B^u/R^u, extension de B^u/R'^u par le groupe fini R'^u/R^u. Rappelons que tout endomorphisme algébrique du groupe additif K est de la forme $k \to P(k)$, où

[2] Où p est l'exposant caractéristique de K. Lorsque K est de caractéristique 0, on a $p = 1$ et $R_u = R'_u$, et la démonstration se simplifie, les p-polynômes étant de la forme cX avec $c \in K$.

$P(X)$ est un p-polynôme (*i.e.* un polynôme de la forme $\Sigma_i\, c_i\, X^{p^i}$, $c_i \in K$). Tout automorphisme de K est de la forme $k \to ck$, avec $c \in K^*$ (n° 9.1, lemme 1). Si f est un épimorphisme comme dans l'énoncé, f est donc défini à un facteur constant non nul près. De plus, l'épimorphisme b de B^u sur K de noyau R'^u peut s'écrire $P \circ f$, où $P(X)$ est un p-polynôme non nul.

L'automorphisme intérieur associé à un élément $t \in T$ laisse globalement invariants B^u et R^u. Donc $s \to f(tst^{-1})$ définit un isomorphisme de B^u/R^u sur K, d'où $f(tst^{-1}) = \alpha(t)f(s)$, $\alpha(t) \in K^*$ et α est évidemment un caractère rationnel de T indépendant du choix de f.

D'autre part, nous avons avec la définition précédente de l'homomorphisme a : $b(tst^{-1}) = a(t^{-1})b(s)$ pour $t \in T$, $s \in B^u$. Si $b(s) = \Sigma_i\, c_i\, f(s)^{p^i}$, nous avons : $b(tst^{-1}) = \Sigma_i\, c_i\, \alpha(t)^{p^i}\, f(s)^{p^i} = \Sigma_i\, c_i\, a(t^{-1})\, f(s)^{p^i}$. Il en résulte que $c_i = 0$ sauf pour une valeur j de l'indice i. Par conséquent f et b annulent les mêmes éléments de B^u, *i.e.* $R'^u = R^u$. D'autre part $\alpha(t)^{p^j} = a(t^{-1})$; donc le noyau de α coïncide avec celui de la restriction de a à T, *i.e.* $T \cap R'$.

Remarque. Nous avons considéré l'espace homogène $\Omega = G/B$; mais nous aurions pu considérer l'image de Ω par une application rationnelle bijective sans rien changer aux démonstrations.

12.2 Racines d'un groupe algébrique

Soient G un groupe algébrique affine connexe, T un tore maximal. Les *racines* de G associées à T sont des caractères de T dont les noyaux connexes sont les tores singuliers de codimension 1, ou encore des formes linéaires sur $\Gamma(T)$ orthogonales aux hyperplans limitrophes des chambres de Weyl. A chaque hyperplan limitrophe correspondent deux racines opposées.

Explicitons d'abord un résultat contenu dans la proposition 1 du n° 10.2.

Lemme 3. – *Soient G un groupe algébrique affine connexe, T un tore maximal, Q un sous-tore de T, Z le centralisateur de Q dans G. Alors les groupes de Borel de Z contenant T sont les intersections avec Z des groupes de Borel de G contenant T.*

En particulier, si Q est semi-régulier, son centralisateur Z est résoluble (n° 10.2, proposition 2), donc il est contenu dans tout groupe de Borel de G contenant T.

Soit maintenant Q un tore singulier de codimension 1. Nous avons vu (n° 11.3, théorème 2) que le groupe de Weyl du centralisateur Z de Q est d'ordre 2 ; les éléments du normalisateur de T dans Z induisent (par automorphismes intérieurs) l'identité ou la réflexion par rapport à Q. Les groupes de Borel de G contenant T découpent sur Z l'ou ou l'autre de ses deux groupes de Borel contenant T. Les résultats du n° précédent justifient la définition suivante :

Définition 1. – *Soient G un groupe algébrique affine connexe non résoluble, T un tore maximal, $Q \subset T$ un tore singulier de codimension 1, $B \supset T$ un groupe de Borel, B^u sa partie unipotente, Z le centralisateur de Q, R le radical de Z. Si l'on identifie $(B^u \cap Z)/(B^u \cap R)$ au groupe additif K, l'automorphisme de $(B^u \cap Z)/(B^u \cap R)$ défini par restriction et passage au quotient à partir de l'automorphisme intérieur de G associé à un élément $t \in T$ s'identifie à la multiplication par $\alpha(t) \in K^*$. Le caractère α de T sera appelé la racine associée à T, Q et B (ou encore à T, Q et au groupe de Borel $A = B \cap Z$ de Z).*

Comme Q est dans le centre de Z, il est contenu dans le noyau de α ; par ailleurs, on a vu que α n'est pas une constante ; comme Q est de codimension 1, c'est la composante neutre dans le noyau de α.

Proposition 1. – *Soient, avec les notations précédentes, τ un élément du normalisateur de T dans G, w_τ l'élément du groupe de Weyl défini par τ, α la racine associée à T, Q, A. Alors la racine $w_\tau\alpha$ associée à T, $\tau Q\tau^{-1}$, $\tau A\tau^{-1}$ est la fonction $t \to (w_\tau\alpha)(t) = \alpha(\tau^{-1}t\tau)$.*

Démonstration. Si $f : A^u \to K$ définit un isomorphisme de $A^u/A^u \cap R$ sur K, la fonction $s \to f(\tau^{-1}s\tau)$ définit un isomorphisme de

$$\tau A^u\tau^{-1}/(\tau A^u\tau^{-1}) \cap (\tau R\tau^{-1})$$

sur K. On obtient alors, pour $t \in T$ et $s \in \tau A^u\tau^{-1}$:

$$f(\tau^{-1}(tst^{-1})\tau) = f((\tau^{-1}t\tau)(\tau^{-1}s\tau)(\tau^{-1}t^{-1}\tau)) = \alpha(\tau^{-1}t\tau)f(\tau^{-1}s\tau)\,.$$

Corollaire. – *Les racines associées aux deux groupes de Borel de Z contenant T sont inverses l'une de l'autre.*

Démonstration. Supposons que τ appartienne à Z et au normalisateur de T, mais non à son centralisateur. Alors $\tau A\tau^{-1}$ est le groupe de Borel de Z distinct de A qui contient T. Comme $\tau^{-1}t\tau t \in Q$ pour $t \in T$ (n° 11.3, théorème 2) et que Q est contenu dans le noyau de α, on obtient $w_\tau\alpha = \alpha^{-1}$.

Proposition 2. – *Avec les notations de la définition 1, la racine α considérée comme forme linéaire sur $\Gamma(T)$ est négative sur la chambre de Weyl associée à B.*

Démonstration. Soit x_∞ le point de $\Omega = G/B$ invariant par B. Considérons $Zx_\infty = \Omega'$. Nous savons que Ω' est une sous-variété fermée de Ω (n° 10.2, proposition 1) ; le groupe Z y opère transitivement, et, comme le stabilisateur de x_∞ dans Z est $A = Z \cap B$, qui est un groupe de Borel de Z, nous avons une application rationnelle bijective de Z/A sur Ω'. Nous pouvons alors appliquer les lemmes 1 et 2, compte tenu de la remarque qui les suit.

Ω' est donc une droite projective et contient un point $x_0 \neq x_\infty$ invariant par T. Si ζ est une fonction rationnelle sur Ω' qui a un seul pôle simple

en x_∞ et un seul zéro simple en x_0, nous avons pour $t \in T$ et $x \in \Omega'$, $\zeta(tx) = a(t^{-1})\zeta(x)$, avec $a(t^{-1}) = \alpha(t)^{p^j}$ pour un entier $j \geq 0$ (d'après la fin de la démonstration du lemme 2).

Soit $\gamma \in \Gamma(T)$. Alors, pour $x \in \Omega'$ et $\theta \in K^*$, on a $\zeta(\gamma(\theta)x) = \alpha(\gamma(\theta))^{p^j}\zeta(x) = \theta^{p^j\langle\alpha,\gamma\rangle}\zeta(x)$. Il en résulte que :

$$\begin{cases} \gamma(0)x = x_\infty & \text{pour} \quad \langle\alpha,\gamma\rangle < 0 \text{ et } x \in \Omega' - x_0 \\ \gamma(0)x = x_0 & \text{pour} \quad \langle\alpha,\gamma\rangle > 0 \text{ et } x \in \Omega' - x_\infty \\ \gamma(0)x = x & \text{pour} \quad \langle\alpha,\gamma\rangle = 0 \text{ et } x \in \Omega' . \end{cases}$$

Or si γ est dans la chambre associée à B, l'ensemble U des $x \in \Omega$ tels que $\gamma(0)x = x_\infty$ est un ouvert non vide de Ω. Comme $x_\infty \in \Omega' \cap U$, $\Omega' \cap U$ est un ouvert non vide de Ω', et il résulte du calcul précédent que $\langle\alpha,\gamma\rangle < 0$.

Corollaire 1. – *Soient $B \supset T$ un groupe de Borel de G, $A \supset T$ un groupe de Borel du centralisateur Z d'un tore singulier $Q \subset T$ de codimension* 1*, α la racine associée à T, Q, A ; soient A^u la partie unipotente de A, τ un élément du normalisateur de T dans G. Pour que $\tau A^u \tau^{-1} \subset B$, il faut et il suffit que la fonction $w_\tau\alpha$ soit négative sur la chambre associée à B.*

Démonstration. $\tau A^u\tau^{-1} \subset B$ équivaut à $\tau A\tau^{-1} \subset B$ (puisque $A = A^uT$, $\tau T\tau^{-1} = T$ et $B \supset T$), ou encore à $\tau A\tau^{-1} = B \cap \tau Z\tau^{-1}$.

Soit A' le second groupe de Borel de Z contenant T. Alors $\tau A\tau^{-1}$ et $\tau A'\tau^{-1}$ sont les deux groupes de Borel de $\tau Z\tau^{-1}$ contenant T. D'après la proposition 1 et son corollaire, les racines associées à T, $\tau Q\tau^{-1}$, $\tau A\tau^{-1}$ (resp. $\tau A'\tau^{-1}$) sont $w_\tau\alpha$ (resp. $-w_\tau\alpha$ en notation additive). La proposition 2 permet de déterminer quel est le groupe de Borel de $\tau Z\tau^{-1}$ qui est contenu dans B, ce qui établit le corollaire 1.

Corollaire 2. – *Pour chaque tore singulier $Q \subset T$ de codimension* 1*, considérons la partition suivante de l'ensemble des groupes de Borel de G contenant T : deux groupes de Borel appartiennent à la même classe si et seulement s'ils ont même intersection avec le centralisateur de Q. Alors, si α est une des deux racines associées à Q, la partition des chambres de Weyl définie par Q est celle définie dans $\Gamma^{\mathbf{Q}}(T)$ par les deux demi-espaces complémentaires de l'hyperplan orthogonal à α. Deux tores singuliers de codimension* 1*, $Q \neq Q'$, définissent deux partitions distinctes.*

Démonstration. La première partie de ce corollaire n'est qu'une formulation affaiblie – à tous points de vue – de la proposition 2, compte tenu du corollaire à la proposition 1. La seconde partie résulte de ce qu'un hyperplan limitrophe d'une chambre dans $\Gamma^{\mathbf{Q}}(T)$ est la frontière de l'adhérence de la réunion des chambres contenues dans un même demi-espace limité par cet hyperplan.

12.3 Réunion et intersection des groupes de Borel contenant un tore maximal

Lemme 4. – *Soit G un groupe algébrique affine connexe. Tous sous-groupe fermé H de G contenant un groupe de Borel B est son propre normalisateur dans G.*

Démonstration. On n'utilise que les deux propriétés suivantes d'un groupe de Borel B :

a) B est son propre normalisateur dans G (n° 9.3, théorème 1) ;

b) si B et xBx^{-1} sont tous deux contenus dans un sous-groupe fermé H de G ($x \in G$), il existe $y \in H$ tel que $xBx^{-1} = yBy^{-1}$ (n° 6.5, théorème 5 ; on peut prendre y dans la composante neutre de H).

Soient alors $H \supset B$ un sous-groupe fermé de G, et $x \in G$, tel que $xHx^{-1} = H$. Alors $xBx^{-1} \subset H$; il existe $y \in H$ tel que $xBx^{-1} = yBy^{-1}$; donc $y^{-1}x$ normalise B, d'où $y^{-1}x \in B$, et finalement $x \in H$.

Proposition 3. – *Soient G un groupe algébrique affine connexe, T un tore maximal. La réunion des groupes de Borel de G contenant T engendre G.*

Démonstration. Soit H le sous-groupe engendré par ces groupes de Borel. Comme ils sont en nombre fini et connexes, H est fermé et connexe (n° 3.3, théorème 2). Le normalisateur N de T est contenu dans le normalisateur de H, donc $H \supset N$ (lemme 4).

Considérons l'espace homogène G/H. Si $xH \in G/H$ est invariant par T, on a $TxH \subset xH$, d'où $x^{-1}Tx \subset H$. Comme T et $x^{-1}Tx$ sont deux tores maximaux de H, il existe donc $h \in H$ tel que $x^{-1}Tx = h^{-1}Th$; on a $xh^{-1} \in N$, d'où $x \in H$. Cela signifie que T ne laisse invariant qu'un seul point de G/H.

Il en résulte que G/H est un point, *i.e.* $G = H$. En effet, on peut appliquer à H la proposition 5 du n° 10.3, et faire opérer G sur un espace projectif P de telle sorte que H soit le stabilisateur d'un point $u \in P$. Comme G/H est une variété complète (n° 6.5, théorème 5) et que l'orbite de u est l'image de G/H par un morphisme bijectif, on voit comme pour la proposition 6 du n° 10.3 que G/H est réduite à un point si elle ne contient pas au moins deux points distincts invariants par T.

Théorème 1. – *Soient G un groupe algébrique affine connexe, T un tore maximal, S l'intersection des groupes de Borel de G contenant T, S_0 la composante neutre de S, S_0^u la partie unipotente de S_0. Alors S_0^u est un sous-groupe invariant contenu dans le radical de G.*

Démonstration. La proposition 1 du n° 9.4 montre que le sous-groupe résoluble connexe S_0^u est contenu dans le radical de G s'il est invariant. D'après la proposition 3 ci-dessus, il suffit de montrer que le normalisateur

H de S_0^u contient tout groupe de Borel B contenant T. Nous savons déjà que $H \supset S \supset T$. Comme $B = B^u T$, il suffit de montrer que $H \supset B^u$. Or d'après le lemme 2 du n° 9.1 (appliqué à B) B^u est engendré par ses intersections avec les centralisateurs des sous-tores de codimension ≤ 1 de T. Les centralisateurs des sous-tores semi-réguliers sont contenus dans S (*cf.* lemme 3). Tout revient donc à démontrer que, *si B^u est la partie unipotente d'un groupe de Borel B contenant T, Q un tore singulier de codimension* 1 *dans T, Z le centralisateur de Q dans G, on a $Z \cap B^u \subset H$, c'est-à-dire que $Z \cap B^u$ normalise S_0^u.*

Soit S' l'intersection de tous les groupes de Borel $B_i \supset T$ tels que $B_i \cap Z = B \cap Z$. Notons S'_0 la composante neutre de S' et Σ la partie unipotente de S'_0. Nous avons les inclusions : $S_0^u \subset \Sigma \subset B^u$. De plus, $B \cap Z = S' \cap Z = S'_0 \cap Z$, puisque $B \cap Z$ est connexe ; donc $B^u \cap Z = \Sigma \cap Z$. Il s'agit donc de démontrer que $\Sigma \cap Z$ normalise S_0^u. Cela est évident si $\Sigma = S_0^u$. Sinon nous pouvons appliquer le lemme 2 du n° 9.1, et introduire un sous-groupe fermé connexe Σ' vérifiant les propriétés suivantes : on a les inclusions

$$S_0^u \subset \Sigma' \subset \Sigma \subset B^u \ ;$$

S_0^u est un sous-groupe invariant de Σ' (*i.e.* $\Sigma' \subset H$) ; Σ'/S_0^u est isomorphe à K, et Σ' est engendré par S_0^u et des éléments du centralisateur Z' d'un tore $Q' \subset T$ de codimension ≤ 1 (*i.e.* $\Sigma' = S_0^u(\Sigma' \cap Z')$).

Le tore Q' est nécessairement singulier ; sinon son centralisateur Z' serait contenu dans S_0, d'où $\Sigma' \cap Z' \subset S_0^u$, $\Sigma' = S_0^u$ contrairement à l'hypothèse. Soit R le radical de Z', R^u la partie unipotente de R. D'après le lemme 3, on a $S \cap Z' \supset R$, d'où $S_0 \supset R$ et $S_0^u \supset R^u$. Nous avons donc les inclusions

$$R^u \subset S_0^u \subset \Sigma' \subset \Sigma \subset B^u \,,$$

et $R \subset Z'$ d'où

$$R^u \subset S_0^u \cap Z' \subset \Sigma' \cap Z' \subset \Sigma \cap Z' \subset B^u \cap Z' \,.$$

Comme $\Sigma'/S_0^u = S_0^u(\Sigma' \cap Z')/S_0^u$ est isomorphe à K et (comme groupe discret) à $(\Sigma' \cap Z')/(S_0^u \cap Z')$, ce dernier groupe est infini.

Donc $\dim(\Sigma' \cap Z') > \dim R^u$. Comme d'autre part $(B^u \cap Z')/R^u$ est isomorphe à K (lemme 2), nous avons $\dim(\Sigma' \cap Z') = \dim(B^u \cap Z')$; d'où

$$\Sigma' \cap Z' = \Sigma \cap Z' = B^u \cap Z' \,.$$

Comme $S'_0 = T\Sigma$, nous avons $S'_0 \cap Z' = T(\Sigma \cap Z') = T(B^u \cap Z') = B \cap Z'$. *A fortiori* $S' \cap Z' = B \cap Z'$. D'après le corollaire 2 à la proposition 2 et la définition de S' à partir de Q et de B, la relation $S' \cap Z' = B \cap Z'$ implique $Q = Q'$ et $Z = Z'$. Nous avons donc $B^u \cap Z \subset \Sigma' \subset H$, ce qui achève la démonstration.

Corollaire.[3] – *Soient $Q \subset T$ un tore de G et Z le centralisateur de Q. Alors tout élément unipotent du radical de Z est contenu dans le radical de G.*

En effet, nous avons vu que le radical de Z est contenu dans S_0.

12.4 Application aux groupes semi-simples

Théorème 2. – *Soient G un groupe algébrique* semi-simple*, T un tore maximal de G. Alors :*

a) *les groupes de Cartan de G sont ses tores maximaux ;*

b) *tout tore semi-régulier est régulier et son centralisateur est un tore maximal ;*

c) *si Q est un tore singulier de codimension* 1 *dans T, le radical du centralisateur de Q est Q ;*

d) *G est engendré par les centralisateurs des tores singuliers de codimension* 1 *contenus dans T ;*

e) *l'intersection des tores singuliers de codimension* 1 *contenus dans T est un groupe fini contenu dans le centre de G.*

Démonstration. D'après le corollaire précédent, le radical du centralisateur d'un tore est un groupe résoluble connexe sans élément unipotent distinct de e, donc un tore. Si $Q \subset T$ est semi-régulier, son centralisateur (qui est résoluble) est donc égal à T. Cela établit a) puisque les groupes de Cartan sont les centralisateurs des tores maximaux (n° 7.1, théorème 1). Si $x \in Q$ (semi-régulier) est choisi tel que son centralisateur coïncide avec celui de Q, le centralisateur de x est T, donc x et Q sont réguliers ; d'où b).

Si Q est singulier de codimension 1, le radical R de son centralisateur Z est un tore contenant Q. Si $R \neq Q$, R serait un tore maximal T ; Z serait donc contenu dans le normalisateur de T, ce qui est impossible puisque la composante neutre de ce normalisateur est T ; d'où c).

Soit H le sous-groupe de G engendré par les centralisateurs Z_i des tores singuliers de codimension 1 de T. Pour montrer que H est égal à G, il suffit d'après la proposition 3 d'établir que l'on a $B \subset H$ pour tout groupe de Borel $B \supset T$, et même, puisque $T \subset Z_i$, que $B^u \subset H$. Or B^u est engendré par ses intersections avec les centralisateurs des sous-tores de codimension ≤ 1 de T (n° 9.1, lemme 2). D'après b) seules interviennent les intersections de B^u avec les centralisateurs des tores singuliers ; d'où d).

[3] Dans la terminologie actuelle, on appelle *groupe réductif* un groupe algébrique affine connexe G dont le radical R ne contient aucun élément unipotent distinct de e (donc R est un tore). Le corollaire exprime que, dans un groupe réductif G, le centralisateur Z d'un tore Q est un groupe réductif (appelé *sous-groupe de Levi* de G).

L'intersection des tores singuliers de codimension 1 contenus dans T est un sous-groupe central de G, d'après d). Ce sous-groupe est fini car la composante neutre du centre de G est contenue dans le radical, *i.e.* le centre de G est un sous-groupe fini car G est semi-simple ; d'où e).

13. Groupes semi-simples : structure de B et de G/B[1]

13.1 Propriétés de certains groupes nilpotents à opérateurs

Dans tout ce numéro, nous étudierons des groupes discrets à opérateurs (*cf.* Bourbaki, Algèbre, chapitre I, §4) ; le domaine d'opérateurs T fixé une fois pour toutes n'interviendra pas explicitement. Par contre, pour abréger les énoncés, nous conviendrons de dire "sous-groupe" au lieu de "sous-groupe stable", "suite de Jordan-Hölder" au lieu de "suite de Jordan-Hölder en tant que groupe à opérateurs", etc... Nous dirons qu'un groupe B est *produit d'une famille de sous-groupes* $(P_i)_{1\leq i\leq n}$ si tout élément de B s'écrit d'une manière et d'une seule sous la forme $\prod_{i=1}^{n} p_i$, $p_i \in P_i$ $(1 \leq i \leq n)$.

Lemme 1. – *Soit B un groupe nilpotent.*

a) *La suite centrale descendante de B : $B = B_1 \supset \ldots \supset B_i \supset B_{i+1} \supset \ldots \supset B_{c+1} = \{e\}$ est une suite de sous-groupes invariants dont la longueur est la classe c de B.*

b) *Soit $C \neq B$ un sous-groupe de B ; alors il existe un sous-groupe D de B qui contient strictement C comme sous-groupe distingué.*[2]

c) *Si B est simple (*i.e. *ne contient pas de sous-groupe distingué propre), il est commutatif et ne contient pas de sous-groupe propre.*

d) *Si B possède une suite de Jordan-Hölder, tout sous-groupe de B figure dans une suite de Jordan-Hölder.*

Démonstration. a) Toutes ces propriétés sont bien connues pour les groupes sans opérateurs. Rappelons que B_{i+1} est engendré par les commutateurs $xyx^{-1}y^{-1}$ avec $x \in B$, $y \in B_i$. Comme la suite centrale descendante est complètement invariante (*i.e.* $f(B_i) \subset B_i$ pour tout endomorphisme f de B), c'est bien une suite de sous-groupes (stables).

b) Soient $C \neq B$ un sous-groupe de B et i le plus grand indice tel que $B_i \not\subset C$. Alors $D = B_i C$ contient strictement C, et C est invariant dans D (passer au quotient modulo B_{i+1}).

[1] Exposé de M. Lazard, le 25.3.1957

[2] Autrement dit, C est distinct de son normalisateur dans B.

c) Si B est simple, il est commutatif (sinon B_2 serait un sous-groupe invariant propre), et tout sous-groupe est invariant.

d) Soit $\{e\} = H_0 \subset H_1 \subset \ldots \subset H_n = B$ une suite de Jordan-Hölder de B. D'après c) on ne peut intercaler entre H_i et H_{i+1} aucun sous-groupe distinct de H_i et de H_{i+1}. Il résulte alors facilement du théorème de Schreier-Zassenhaus (Bourbaki, *loc. cit.*) que, si $C_0 \subset C_1 \subset \ldots \subset C_h$ est une suite de composition, c'est-à-dire une suite strictement croissante de sous-groupes de B telle que C_i soit invariant dans C_{i+1} $(0 \leq i \leq h-1)$, on a $h \leq n$. Partant d'un sous-groupe C quelconque, on déduit de b) et du résultat précédent qu'on peut construire une suite de composition où figure C ; il suffit alors de raffiner cette dernière en une suite de Jordan-Hölder.

Définition 1. – *Un groupe B sera dit vérifier les conditions* (C) *si :*

C1) *B est nilpotent.*

C2) *B admet une suite de Jordan-Hölder (H_i) ; notations*[3] *: $H_0 = \{e\}$, $H_{i-1} \subset H_i$ pour $1 \leq i \leq n$, $H_n = B$.*

C3) *La suite de Jordan-Hölder (H_i) est clivée par une famille de sous-groupes $(P_i)_{1 \leq i \leq n}$; autrement dit, pour $1 \leq i \leq n$, on a $P_i \cap H_{i-1} = \{e\}$, $P_i H_{i-1} = H_i$.*

C4) *Les quotients H_i/H_{i-1} sont deux à deux non isomorphes.*

Proposition 1. – *Soient B un groupe vérifiant les conditions* (C), *$(P_i)_{1 \leq i \leq n}$ une famille de sous-groupes clivant une suite de Jordan-Hölder (H_i). Alors :*

a) *Toute suite de Jordan-Hölder de B est clivée par les mêmes sous-groupes (P_i), rangés éventuellement dans un ordre différent.*

b) *Tout sous-groupe et tout quotient de B vérifient les conditions* (C).

c) *Tout sous-groupe de B est produit des sous-groupes P_i qu'il contient ; plus précisément, si $P_{\alpha(1)}, \ldots, P_{\alpha(h)}$ sont tous les sous-groupes distincts P_i contenus dans un sous-groupe C de B, rangés dans un ordre quelconque, tout élément $x \in C$ s'écrit d'une manière et d'une seule sous la forme $x = y_1 y_2 \ldots y_h$ avec $y_i \in P_{\alpha(i)}$.*

d) *Les sous-groupes P_i sont tous les sous-groupes simples*[4] *de B.*

Démonstration. a) Soit $(K_i)_{0 \leq i \leq n}$ une suite de Jordan-Hölder de B. Nous savons que ses quotients K_i/K_{i-1} sont isomorphes aux quotients H_j/H_{j-1} de la suite (H_j), rangés dans un ordre convenable. Pour tout indice α $(1 \leq \alpha \leq n)$, soit $i(\alpha)$ le plus petit indice i tel que $P_\alpha \subset K_i$. Comme P_α est isomorphe à $H_\alpha/H_{\alpha-1}$, P_α n'a pas de sous-groupe propre (lemme 1, c)) ; donc $P_\alpha \cap K_{i(\alpha)-1} = (e)$. Comme $K_{i(\alpha)}/K_{i(\alpha)-1}$ n'a pas de sous-groupe propre, on a $P_\alpha K_{i(\alpha)-1} = K_{i(\alpha)}$. Il en résulte que P_α est isomorphe à $K_{i(\alpha)}/K_{i(\alpha)-1}$; comme les P_α sont deux à deux non isomorphes, l'application $\alpha \to i(\alpha)$ est

[3] Et bien sûr, H_{i-1} est invariant dans H_i pour $1 \leq i \leq n$.

[4] Ils sont donc commutatifs d'après le lemme 1, c).

injective, donc bijective puisqu'elle applique l'intervalle fini $[1, n]$ dans lui-même. Autrement dit les P_i clivent la suite (K_i).

b) Il est clair que les conditions (C) sont vérifiées pour tout sous-groupe H_j figurant dans la suite (H_i). De même, si H_j est invariant dans B, le groupe B/H_j vérifie les conditions (C). Il suffit alors d'appliquer le lemme 1, d).

c) Si $x \in H_i$ (avec les notations de la définition 1), on démontre sans peine (par récurrence sur i) que $x = y_1 y_2 \dots y_i$, avec des $y_j \in P_j$ bien déterminés par x ; H_i est donc le produit des P_j pour $1 \leq j \leq i$, *i.e.* le produit des P_j qu'il contient. Cette propriété est vraie pour tout sous-groupe C, car C figure dans une suite de Jordan-Hölder clivée par les P_i. Pour montrer que l'ordre des facteurs P_i peut être choisi arbitrairement, nous pouvons supposer $C = B$. Soient alors $(P_i)_{1 \leq i \leq n}$ les sous-groupes P_i *rangés dans un ordre quelconque.* La propriété cherchée est évidente si B est commutatif. Sinon, raisonnons par récurrence sur la classe c de B. Soit $I \subset [1, n]$ l'ensemble de tous les indices i tels que $P_i \subset B_c$ (dernier sous-groupe non réduit à l'élément neutre de la suite centrale descendante de B). Si nous passons au quotient modulo B_c, l'hypothèse de récurrence nous montre que les produits $y_1 \dots y_n$ avec $y_i \in P_i$ et $y_i = e$ pour $i \in I$ constituent un système de représentants de B mod. B_c. Comme B_c est dans le centre de B et que $B_c = \prod_{i \in I} P_i$, il en résulte que $(y_1, \dots, y_n) \to y_1 \dots y_n$ $(y_i \in P_i)$ est une bijection de $P_1 \times \dots \times P_n$ sur B.

d) est une conséquence immédiate de c).

Définition 2. – *Soient B un groupe vérifiant les conditions* (C), *$(P_i)_{1 \leq i \leq n}$ l'ensemble de ses sous-groupes simples. Si I est une partie de l'intervalle d'entiers $[1, n]$, nous dirons que I est saturée si le sous-groupe engendré par les $(P_i)_{i \in I}$ ne contient pas d'autre sous-groupe simple ; ce sous-groupe, produit des $(P_i)_{i \in I}$, sera noté B_I. Si I est une partie quelconque de $[1, n]$, la plus petite partie saturée contenant I sera dite engendrée par I.* (L'intersection d'une famille de parties saturées est évidemment saturée.)

Proposition 2. – *Soient B un groupe vérifiant les conditions* (C), *$(P_i)_{1 \leq i \leq n}$ l'ensemble de ses sous-groupes simples.*

a) *Si $\{I, I'\}$ est une partition de $[1, n]$ en deux parties saturées, B est produit de B_I et de $B_{I'}$.*

b) *Si I et I' sont deux parties saturées de $[1, n]$ telles que B_I et $B_{I'}$ soient conjugués dans B, alors $I = I'$.*

c) *Pour qu'une partie $I \subset [1, n]$ soit saturée, il faut et il suffit qu'elle vérifie la condition suivante : pour tout couple $i, j \in I$, la plus petite partie saturée contenant i et j est contenue dans I.*

Démonstration. a) est une conséquence immédiate de la proposition 1, c).

b) Démonstration par récurrence sur la classe c de B (la proposition est évidente si $c = 1$). Considérons les deux sous-groupes $B_I \cap B_c$ et $B_{I'} \cap B_c$ que nous pouvons écrire respectivement B_{I_1} et $B_{I'_1}$, I_1 et I'_1 étant des parties de $[1, n]$. Alors B_{I_1} et $B_{I'_1}$ sont conjugués dans B. Comme ils sont centraux,

on a évidemment $I_1 = I'_1$. Considérons maintenant le quotient B/B_c, et appliquons l'hypothèse de récurrence aux images de B_I et de $B_{I'}$: nous en déduisons que $I - I_1 = I' - I'_1$ (différences ensemblistes) ; d'où $I = I'$. (Ce résultat ne signifie évidemment pas que tout sous-groupe est invariant, mais que, si C est un sous-groupe de B et $x \in B$, xCx^{-1} n'est un sous-groupe (stable par T !) que s'il est égal à C.)[5]

c) Il suffit de prouver la suffisance de la condition énoncée. Supposons les (P_i) ordonnés comme dans la définition 1, ce qui équivaut à supposer les parties $[1, i]$, saturées pour $1 \leq i \leq n$. Raisonnons par récurrence sur le nombre d'éléments de I. Soient α le plus grand élément de I et $I' = I - \{\alpha\}$. Alors, si $i, j \in I'$, le sous-groupe engendré par P_i et P_j ne contient pas P_α, et l'hypothèse de récurrence s'applique donc à I', qui est saturée. Pour montrer que I est saturée, il faut montrer que $P_\alpha B_{I'}$ est un sous-groupe. Il suffit donc de montrer que $P_i P_\alpha \subset P_\alpha P_{I'}$ pour tout $i \in I'$; or c'est un cas particulier de l'hypothèse.

Signalons pour conclure un résultat qui servira peut-être : tout sous-groupe propre maximal est invariant, et le quotient est abélien. On en déduit qu'il existe une famille minima de P_i qui engendre B : elle est constituée par tous les P_i qui ne sont pas contenus dans le groupe dérivé B_2 de B.

13.2 Structure du groupe B^u

Dans ce numéro, nous notons *G un groupe algébrique semi-simple, T un tore maximal, B un groupe de Borel contenant T, B^u la partie unipotente de B.*

Théorème 1. – a) *Si l'on fait opérer par automorphismes intérieurs les éléments de T sur B^u, le groupe à opérateurs B^u vérifie les conditions* (C) *de la définition* 1.

b) *Soit $\mathcal{B}$ l'ensemble des racines α associées à T qui sont négatives sur la chambre de Weyl associée à B. Les sous-groupes stables minimaux de B^u sont les intersections $(P_\alpha)_{\alpha \in \mathcal{B}}$ de B^u avec les centralisateurs Z_α des tores singuliers $Q_\alpha \subset T$ de codimension* 1 *(correspondant respectivement aux racines α).*

c) *Chacun des groupes P_α est isomorphe à K comme groupe algébrique. Si P_α est identifié à K par l'isomorphisme $\tau_\alpha : K \to P_\alpha$, on a $t\tau_\alpha(\xi)t^{-1} = \tau_\alpha(\alpha(t)\xi)$ pour $\alpha \in \mathcal{B}$, $\xi \in K$, $t \in T$.*

d) *Tous sous-groupe de B^u normalisé par T est fermé. C'est le produit des P_α qu'il contient.*

[5] Le point de cette remarque est le suivant : si C est un sous-groupe stable par T dans B, et x un élément de B, on ne peut garantir que xCx^{-1} est stable par T si x n'est pas lui-même invariant par T.

Démonstration. Appliquons le lemme 2 du n° 9.1 (en y remplaçant G par B). Nous en déduisons l'existence d'une suite de composition $(H_i)_{0\leq i\leq n}$ de B^u, où les sous-groupes H_i sont tous normalisés par T. Pour tout i $(1 \leq i \leq n)$ H_i/H_{i-1} est isomorphe à K ; le groupe H_i est engendré par H_{i-1} et par des éléments du centralisateur Z_i d'un tore $Q_i \subset T$ de codimension ≤ 1.

Les tores Q_i sont des tores singulier de codimension 1. Sinon, d'après le théorème 2, b) du n° 12.4, l'un des Z_i serait égal à T et l'on aurait $Z_i \cap B^u = \{e\}$, d'où $H_{i-1} = H_i$.

D'après le lemme 2 du n° 12.1, le lemme 3 du n° 12.2 et le corollaire au théorème 1 du n° 12.3, nous savons que $B^u \cap Z_i = P_i$ est isomorphe à K. Si $\tau_i : K \to P_i$ est un isomorphisme de K sur P_i, nous avons, pour $\xi \in K$ et $t \in T$, $t\tau_i(\xi)t^{-1} = \tau_i(\alpha_i(t)\xi)$, où α_i est la racine associée à T, Q_i et B (n° 12.2, définition 1). Comme α_i n'est pas nulle, $\alpha_i(t)$ prend toutes les valeurs de K^*, et P_i est simple en tant que sous-groupe à opérateurs. On en déduit $P_i \cap H_{i-1} = \{e\}$, puisque $P_i \not\subset H_{i-1}$; on a aussi $P_i \subset H_i$, puisque $P_i \cap H_i \neq \{e\}$.

Le groupe B^u est nilpotent (puisqu'il est unipotent et connexe) et admet, en tant que groupe à opérateurs, une suite de Jordan-Hölder clivée par les P_i. Reste à montrer que les P_i sont deux à deux non isomorphes en tant que groupes à opérateurs. Or P_i est isomorphe à P_j si et seulement si $\alpha_i = \alpha_j$ (rappelons que α_i est indépendant du choix de τ_i) ; mais si $\alpha_i = \alpha_j$, leurs noyaux connexes Q_i et Q_j coïncident, donc $P_i = P_j$.

Nous avons donc démontré a) ; au passage, nous avons établi que l'intersection P_α de B^u avec le centralisateur Z_α d'un tore singulier Q_α de codimension 1 dans T est un sous-groupe stable simple de B^u. La proposition 1 établit les autres assertions du théorème 1 (noter que les P_α sont fermés, ainsi que les sous-groupes engendrés par certains d'entre eux).

Nous allons maintenant étudier certains sous-groupes stables de B^u.

Proposition 3. – *Soient, avec les notations précédentes, σ un élément du normalisateur de T, w l'opération du groupe de Weyl W définie par σ. Posons* $B'^u_w = B^u \cap \sigma B^u \sigma^{-1}$.

Alors B'^u_w est un sous-groupe de B^u normalisé par T. Si $\alpha \in \mathcal{B}$ est une racine négative sur $\mathcal{C}(B)$, les conditions suivantes sont équivalentes :

a) $P_\alpha \subset B'^u_w$;

b) $w^{-1}\alpha \in \mathcal{B}$;

c) *α est négative sur la chambre de Weyl $w\mathcal{C}(B)$;*

d) *l'hyperplan de $\Gamma^{\mathbf{Q}}(T)$ orthogonal à α ne sépare pas les chambres associées aux groupes de Borel B et $wB = \sigma B \sigma^{-1}$.*

Enfin, si $w, w' \in W$, $B'^u_w = B'^u_{w'}$ équivaut à $w = w'$.

Démonstration. Comme B^u et wB^u sont normalisés par T, il en est de même de leur intersection B'^u_w. Il résulte alors du théorème 1, d), que B'^u_w est le

produit des P_α qu'il contient. Pour $\alpha \in \mathcal{B}$, la relation $P_\alpha \subset {B'}_w^u$ équivaut à $P_\alpha \subset \sigma B^u \sigma^{-1}$ ou encore à $\sigma^{-1} P_\alpha \sigma \subset B^u$. D'après le corollaire 1 de la proposition 2 du n° 12.2, cette relation équivaut à $w^{-1}\alpha \in \mathcal{B}$. Soit $\gamma \in \mathcal{C}(B)$; alors $w^{-1}\alpha \in \mathcal{B}$ équivaut à $\langle w^{-1}\alpha, \gamma\rangle < 0$. Or $\langle w^{-1}\alpha, \gamma\rangle = \langle \alpha, w\gamma\rangle$. Enfin α est négatif sur $\mathcal{C}(B)$ et $w\mathcal{C}(B) = \mathcal{C}(wB)$ si et seulement si l'hyperplan orthogonal ne sépare pas ces chambres de Weyl. Cela démontre l'équivalence de a), b), c) et d).

Soient $w, w' \in W$, ${B'}_w^u = {B'}_{w'}^u$. Alors, si nous appliquons d), nous voyons que les chambres $\mathcal{C}(wB)$ et $\mathcal{C}(w'B)$ ne sont séparées par aucun hyperplan limitrophe dans $\Gamma^{\mathbf{Q}}(T)$. D'après la caractérisation des chambres de Weyl (n° 11.3, théorème 1), cela signifie $\mathcal{C}(wB) = \mathcal{C}(w'B)$, *i.e.* $w = w'$.

Lemme 2. – a) *Si $\gamma \in \Gamma^{\mathbf{Q}}(T)$ parcourt la chambre de Weyl associée à un groupe de Borel $B \supset T$, $(-\gamma)$ parcourt la chambre de Weyl associée à un groupe de Borel $\widetilde{B} \supset T$. La relation entre B et $\widetilde{B}$ est symétrique ; ces deux groupes de Borel, ainsi que les chambres associées, seront dits opposés. Toute racine β prend les signes opposés sur $\mathcal{C}(B)$ et $\mathcal{C}(\widetilde{B})$.*

b) *Les intersections respectives de B et $\widetilde{B}$ avec le centralisateur Z d'un tore singulier $Q \subset T$ de codimension* 1 *sont les deux groupes de Borel de Z contenant T.*

c) *Il existe un élément et un seul $w_B \in W$, tel que $w_B B = \widetilde{B}$. On a $w_B^2 = 1$ (élément neutre). Si $B' = wB$ est un groupe de Borel contenant T ($w \in W$), on a $w_{B'} = w w_B w^{-1}$.*

Démonstration. a) résulte du théorème 1 du n° 11.3. Les chambres $\mathcal{C}(B)$ et $\mathcal{C}(\tilde{B})$ sont situées de part et d'autre de tout hyperplan de $\Gamma^{\mathbf{Q}}(T)$ qui ne les rencontre pas, donc en particulier de tout hyperplan limitrophe d'une chambre (hyperplan orthogonal à une racine).

b) résulte du corollaire de la proposition 1 et de la proposition 2 du n° 12.2.

c) L'existence et l'unicité de w_B résulte de ce que W opère d'une manière simplement transitive sur les groupes de Borel contenant T (ou sur les chambres associées). Comme $w \in W$ définit un automorphisme de $\Gamma^{\mathbf{Q}}(T)$, les chambres $w\mathcal{C}(B)$ et $w\mathcal{C}(\widetilde{B})$ sont opposées ; autrement dit, $\widetilde{wB} = (ww_B)B = (ww_Bw^{-1})(wB)$. La relation $w_B^2 = 1$ résulte de $B = \widetilde{w_B B} = w_B^2 B$.

Proposition 4. – *Avec les notations précédentes, posons pour $w \in W$, $B_w^u = {B'}_{ww_B}^u$. Alors B^u est produit de ses deux sous-groupes B_w^u et ${B'}_w^u$. On a $B_{w_B}^u = B^u$ et ${B'}_{w_B}^u = \{e\}$.*

Démonstration. D'après la proposition 2, a) et le théorème 1, il suffit de prouver que, pour tout $\alpha \in \mathcal{B}$, on a une et une seule des relations $P_\alpha \subset B_w^u$ et $P_\alpha \subset {B'}_w^u$; cela résulte de la proposition 3, c) et du lemme 2. La dernière partie résulte de ce que (si 1 désigne l'élément neutre de W) on a ${B'}_1^u = B^u$, $B_1^u = \{e\}$.

On peut prouver facilement (*cf.* le corollaire 2 de la proposition 2 du n° 12.2) que tout sous-groupe P_α ($\alpha \in \mathcal{B}$) est l'intersection d'une famille de

sous-groupes B_w^u. Mais il peut exister des sous-groupes de B^u normalisés par T qui ne sont pas de cette forme.

13.3 Racines fondamentales

Définition 3. – *Soit G un groupe algébrique semi-simple, et soit T un tore maximal de G. Nous appellerons racines fondamentales par rapport au groupe de Borel $B \supset T$ les racines associées à T et B dont les hyperplans orthogonaux dans $\Gamma^{\mathbf{Q}}(T)$ sont limitrophes de la chambre $\mathcal{C}(B)$. L'ensemble des racines fondamentales par rapport à B sera noté $\mathcal{B}^*$ ($\subset \mathcal{B}$, ensemble des racines négatives sur $\mathcal{C}(B)$).*

Théorème 2. – *Si ℓ est le rang du groupe algébrique semi-simple G,* i.e. *la dimension d'un tore maximal de G, il y a exactement ℓ racines fondamentales par rapport à un groupe de Borel B. Considérées comme formes linéaires sur $\Gamma^{\mathbf{Q}}(T)$, elles sont linéairement indépendantes.*

Démonstration. Les propriétés énoncées ne dépendent pas de la manière dont on a normé les racines ; autrement dit, ce sont des propriétés des hyperplans limitrophes de $\mathcal{C}(B)$. L'indépendance linéaire des $\alpha \in \mathcal{B}^*$ a été démontrée au n° 11.4. Pour que leur nombre soit égal à ℓ, il faut et il suffit que l'intersection H des hyperplans limitrophes de $\mathcal{C}(B)$ se réduise à (0). Or le groupe de Weyl est engendré par les réflexions par rapport à ces hyperplans (n° 11.3, théorème 2). Le sous-espace H est donc l'intersection de tous les hyperplans limitrophes des chambres de Weyl dans $\Gamma^{\mathbf{Q}}(T)$. Il est donc de la forme $\Gamma^{\mathbf{Q}}(Q)$, où Q est la composante neutre de l'intersection des tores singuliers de codimension 1 de T. D'après le théorème 2, e) du n° 12.4, on a $H = (0)$.

Proposition 5. – a) *Toute racine est transformée par au moins un élément de W d'une racine fondamentale par rapport à B.*

b) *Le groupe semi-simple G est engendré par les centralisateurs Z_α des tores singuliers $Q_\alpha \subset T$ de codimension* 1 *lorsque α parcourt $\mathcal{B}^*$.*

Démonstration. a) Soient β une racine, H l'hyperplan orthogonal à β dans $\Gamma^{\mathbf{Q}}(T)$, B' un groupe de Borel tel que H soit limitrophe de la chambre $\mathcal{C}(B')$. Si $w \in W$ est tel que $wB' = B$, $w\beta$ est fondamentale par rapport à B ou à $\widetilde{B}$; dans ce dernier cas, $(w_B w)\beta$ est fondamentale par rapport à B.

b) Il résulte de a) que tout centralisateur d'un tore singulier de codimension 1 de T est transformé de l'un des Z_α par un élément de W. Or ces centralisateurs engendrent G (n° 12.4, théorème 2, d)). Il suffit donc de prouver que le sous-groupe engendré par les Z_α ($\alpha \in \mathcal{B}^*$) contient le normalisateur N de T. Or W est engendré par les réflexions par rapport aux hyperplans limitrophes de $\mathcal{C}(B)$, et l'intersection $Z_\alpha \cap N$ se compose de deux classes modulo T : T lui-même et la classe dont les éléments définissent la réflexion par rapport

à Q_α. Le sous-groupe engendré par les Z_α contient un système de générateurs de N, donc N lui-même.

Lemme 3. – *Soient G un groupe algébrique affine connexe (non nécessairement semi-simple) dont le groupe de Weyl est d'ordre 2, T un tore maximal, B et B_0 deux groupes de Borel (avec $T \subset B$), Ω l'espace homogène G/B_0. Alors, si l'on fait opérer B sur Ω, Ω se décompose en deux orbites ; chacune d'elles contient exactement un point invariant par T. Cet énoncé reste valable si l'on y remplace Ω par son image par un morphisme bijectif.*

Démonstration. On n'a fait qu'énoncer, sous une forme plus géométrique, des résultats établis au cours de la démonstration du lemme 1 du n° 12.1.

Corollaire. – *Avec les notations du lemme 3, si σ est un élément du normalisateur de T non contenu dans son centralisateur, $\{B, B\sigma B\}$ est une partition de G.*

Démonstration. Si l'on fait $B_0 = B$, les points de Ω invariants par T sont les images de B et de σB ; les images réciproques de leurs orbites par B sont B et $B\sigma B$.

Proposition 6. – *Soient G un groupe algébrique semi-simple, $B \supset T$ un groupe de Borel et un tore maximal, B_w^u, ${B'}_w^u$, etc... comme précédemment. Alors :*

a) *Pour que B_w^u se réduise à l'un des P_α, il faut et il suffit que l'on ait $\alpha \in \mathcal{B}^*$ et que w soit la réflexion par rapport à l'hyperplan orthogonal à α. Nous poserons dans ce cas $C_\alpha = {B'}_w^u$ ($\alpha \in \mathcal{B}^*$).*

b) *C_α est un sous-groupe invariant de B^u. Son normalisateur contient le centralisateur Z_α de Q_α.*

c) *On a $Z_\alpha B = BZ_\alpha$.*

Démonstration. a) Soit $w \in W$. La détermination des $P_\beta \subset B_w^u$ se ramène à la recherche des hyperplans limitrophes de chambres dans $\Gamma^{\mathbf{Q}}(T)$ qui sépare $\mathcal{C}(B)$ et $\mathcal{C}(wB)$, d'après la proposition 3, d) et la proposition 4. L'énoncé est alors une conséquence facile du théorème 1 du n° 11.3 (et des développements qui précèdent son corollaire). Il en résulte en effet que deux chambres sont séparées par un seul hyperplan limitrophe si et seulement si elles ont un mur commun dans cet hyperplan limitrophe, *i.e.* si elles sont transformées l'une en l'autre par la réflexion par rapport à cet hyperplan.

b) Il résulte du théorème 1, d) que C_α est un sous-groupe stable maximal de B^u. Il est donc distingué (lemme 1, b)). Soit σ_α un élément de Z_α appartenant au normalisateur de T mais non à T ($\alpha \in \mathcal{B}^*$). Alors la réflexion $w \in W$ associée à α est définie par l'automorphisme intérieur associé à σ_α. Cet automorphisme permute B^u et wB^u. Il conserve donc leur intersection ${B'}_w^u = C_\alpha$; *i.e.* σ_α normalise C_α. Posons $A_\alpha = B \cap Z_\alpha$, donc A_α est un groupe de Borel de Z_α ; sa partie unipotente est P_α, et $A_\alpha = P_\alpha T$. Le groupe C_α est

normalisé par T et par P_α (puisque $P_\alpha \subset B^u$), donc par A_α. Mais (corollaire du lemme 3), on a $Z_\alpha = A_\alpha \cup A_\alpha \sigma_\alpha A_\alpha$. Donc Z_α normalise C_α.

c) On a : $B = TB^u = TP_\alpha C_\alpha = C_\alpha P_\alpha T$. Donc :

$$Z_\alpha B = Z_\alpha T P_\alpha C_\alpha = Z_\alpha C_\alpha = C_\alpha Z_\alpha = C_\alpha P_\alpha T Z_\alpha = B Z_\alpha \,.$$

13.4 Structure de l'espace homogène G/B

Théorème 3. – *Soient G un groupe algébrique affine connexe, B un groupe de Borel contenant un tore maximal T, Ω une variété algébrique sur laquelle G opère algébriquement et transitivement, de telle sorte que le stabilisateur d'un point soit un groupe de Borel. Alors, si l'on fait opérer B sur Ω, Ω se décompose en un nombre fini d'orbites ; chacune d'elles contient exactement un point invariant par T.*

Démonstration. Si G n'est pas semi-simple, le radical R de G opère trivialement sur Ω, car il est contenu dans l'intersection des groupes de Borel. Nous pouvons donc faire opérer sur Ω le groupe semi-simple G/R, et remplacer B par son image qui est un groupe de Borel de G/R. Nous nous ramenons ainsi au cas où G est semi-simple, ce que nous supposerons désormais.

Soient $(\sigma_w)_{w\in W}$ une famille de représentants des classes mod. T du normalisateur N de T, et e_B le point de Ω invariant par B. Alors les points de Ω invariants par T sont les points $\sigma_w e_B$ ($w \in W$), qui correspondent aux groupes de Borel de G contenant T.

Montrons d'abord que l'on a $B\sigma_w e_B \cap B\sigma_{w'} e_B = \varnothing$ pour $w \neq w'$. Le stabilisateur de $\sigma_w e_B$ dans G est $wB = \sigma_w B \sigma_w^{-1}$; son stabilisateur dans B est $B \cap wB = B'^u_w T$. Si $B\sigma_w e_B$ et $B\sigma_{w'} e_B$ avaient une intersection non vide, ils coïncideraient (comme orbites par B d'un même point) ; les sous-groupes $B'^u_w T$ et $B'^u_{w'} T$ seraient conjugués dans B (comme stabilisateurs de deux points d'une même orbite), ainsi que leurs parties unipotentes B'^u_w et $B'^u_{w'}$. D'après la proposition 2, b), on aurait $B'^u_w = B'^u_{w'}$, d'où $w = w'$ d'après la proposition 3.

Démontrons maintenant que, si l'on pose $\Omega' = \bigcup_{w\in W} B\sigma_w e_B$, on a $\Omega' = \Omega$. Il suffit de prouver que l'on a $G\Omega' \subset \Omega'$, ou, d'après la proposition 5, b), que l'on a $Z_\alpha \Omega' \subset \Omega'$ pour $\alpha \in \mathcal{B}^*$.

Considérons $Z_\alpha \sigma_w e_B \subset \Omega$. Le stabilisateur de $\sigma_w e_B$ dans Z_α est $A_\alpha = Z_\alpha \cap wB$, *i.e.* un groupe de Borel de Z_α. Désignons par σ_α un élément de $N \cap (Z_\alpha - T)$. Le corollaire du lemme 3 montre que $Z_\alpha = A_\alpha \cup A_\alpha \sigma_\alpha A_\alpha$, d'où $Z_\alpha \sigma_w e_B = \sigma_w e_B \cup A_\alpha \sigma_\alpha \sigma_w e_B$. Comme $Z_\alpha B = B Z_\alpha$ (proposition 6, c)), on a : $Z_\alpha B \sigma_w e_B = B Z_\alpha \sigma_w e_B = B\sigma_w e_B \cup B\sigma_\alpha \sigma_w e_B$. Or $\sigma_\alpha \sigma_w e_B = \sigma_{w'} e_B$, avec $w' \in W$. Donc $Z_\alpha B \sigma_w e_B = B\sigma_w e_B \cup B\sigma_{w'} e_B \subset \Omega'$, d'où $Z_\alpha \Omega' \subset \Omega'$, ce qui achève la démonstration.

Corollaire 1. – ("décomposition de Bruhat") *Supposons G semi-simple. Alors les ensembles $B^u_w\sigma_w B = B\sigma_w B$, où $w \in W$, définissent une partition de G. Pour chaque $w \in W$, l'application $(b, b') \to b\sigma_w b'$ de $B^u_w \times B$ dans $B\sigma_w B$ est bijective.*

Démonstration. Prenons $\Omega = G/B$. Les ensembles $B\sigma_w B$ constituent une partition de G, image réciproque de la partition de Ω en orbites suivant B. Comme le stabilisateur de $\sigma_w e_B$ dans B est ${B'}^u_w T$, et que B est produit de B^u_w et de ${B'}^u_w T$, l'application $b \to b\sigma_w e_B$ de B^u_w dans $B\sigma_w e_B$ est bijective. En remontant à G, on en déduit que tout point de $B\sigma_w B = B^u_w\sigma_w B$ s'écrit d'une manière et d'une seule sous la forme $b\sigma_w b'$ indiquée.

Corollaire 2. – *Supposons toujours G semi-simple. Alors la dimension de l'orbite $B\sigma_w e_B$ est égale à la dimension de B^u_w. L'orbite de $w_B e_B$ est ouverte dans Ω. La somme des dimensions des orbites $B\sigma_w e_B$ et $B\sigma_w\sigma_{w_B} e_B$ est égale à n, dimension commune de Ω et de B^u (pour tout $w \in W$). Les orbites par B de dimension $n-1$ sont les ensembles $B\sigma_\alpha\sigma_{w_B} e_B$; avec les notations de la proposition 6, l'application $C_\alpha \to B\sigma_\alpha\sigma_{w_B} e_B$ est bijective, pour $\alpha \in \mathcal{B}^*$. Si G est de rang ℓ, sa dimension est $2n+\ell$; $\widetilde{B}B$ est une partie ouverte de G, et l'application $(b, t, b') \to btb'$ de $\widetilde{B}^u \times T \times B^u$ dans $\widetilde{B}B$ est bijective.*

Démonstration. Toute orbite par B est une partie épaisse, et, plus précisément, une partie irréductible ouverte dans son adhérence (n° 6.1, lemme 1). La réunion des adhérences des orbites $B\sigma_w e_B$ est Ω ; comme Ω est irréductible, l'une de ces adhérences est Ω, et par conséquent l'une des orbites $B\sigma_w e$ est un ouvert de Ω. Une seule orbite a cette propriété, car deux ouverts de Ω ont une intersection non vide. Nous avons vu que l'application de B^u_w sur $B\sigma_w e_B$ est bijective ; la dimension de $B\sigma_w e_B$ est donc égale à celle de B^u_w, d'où $\dim B\sigma_w e_B \leq n$. L'égalité ne peut avoir lieu que si $B^u_w = B^u$, *i.e.* si $w = w_B$ d'après la proposition 4. La somme des dimensions de B^u_w et de $B^u_{ww_B}$ est égale à n, puisque B^u est produit de B^u_w et de ${B'}^u_w = B^u_{ww_B}$. Pour que $\dim B^u_w = n-1$, il faut et il suffit que $\dim B^u_{ww_B} = 1$, *i.e.* que ww_B soit une réflexion w_α définie par σ_α ($\alpha \in \mathcal{B}^*$) (proposition 6, a)). Les orbites $B\sigma_\alpha\sigma_{w_B} e_B$ ($\alpha \in \mathcal{B}^*$) sont donc les seules de dimension $n-1$; rappelons qu'on a posé $C_\alpha = {B'}^u_{w_\alpha} = B^u_{w_\alpha w_B}$. Prenons $\Omega = G/B$. Si G est de rang ℓ, $B = B^u T$ est de dimension $n+\ell$, et $\dim G = \dim B + \dim G/B = 2n+\ell$. L'image réciproque de l'ouvert $B\sigma_{w_B} e_B$ dans G est l'ouvert $B\sigma_{w_B} B = \sigma_{w_B}(\sigma^{-1}_{w_B} B\sigma_{w_B})B = \sigma_{w_B}\widetilde{B}B$. L'application $(b, b') \to b\sigma_{w_B} b'$ de $B^u \times B$ dans $B\sigma_{w_B} B$ est bijective ; le petit calcul précédent montre qu'il en est de même de l'application $(b, b') \to bb'$ de $\widetilde{B}^u \times B$ dans $\widetilde{B}B$, ou encore de l'application $(b, t, b') \to btb'$ de $\widetilde{B}^u \times T \times B^u$ dans $\widetilde{B}B$.

Proposition 7. – *Reprenons les notations du théorème 3, en supposant G semi-simple. Soit $\gamma \in \mathcal{C}(B)$ un sous-groupe à un paramètre de T. Alors, si $x \in B\sigma_w e_B$, on a $\gamma(\infty)x = \sigma_w e_B$.*

Démonstration. L'élément x peut s'écrire $x = b\sigma_w e_B$, avec $b \in B^u$, et, pour $t \in T$, on a $tx = tb\sigma_w e_B = (tbt^{-1})t\sigma_w e_B = (tbt^{-1})\sigma_w e_B$. Nous allons remplacer B^u par un espace vectoriel K^n de la manière suivante. Ordonnons l'ensemble $\mathcal{B}$ des racines α négatives sur $\mathcal{C}(B)$ ($\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$). Alors, avec les notations du théorème 1, l'application $\varphi : K^n \to B^u$ définie par $\varphi(\xi_1, \ldots, \xi_n) = \tau_{\alpha_1}(\xi_1) \ldots \tau_{\alpha_n}(\xi_n)$ est bijective (proposition 1, c)). Le morphisme ψ de $K^* \times K^n$ dans K^n défini par

$$\begin{aligned} \psi(\theta, (\xi_1, \ldots, \xi_n)) &= (\alpha_1(\gamma(\theta))\xi_1, \ldots, \alpha_n(\gamma(\theta))\xi_n) \\ &= (\theta^{\langle \alpha_1, \gamma \rangle}\xi_1, \ldots, \theta^{\langle \alpha_n, \gamma \rangle}\xi_n) \end{aligned}$$

se prolonge en un morphisme de $\overline{K}^* \times K^n$ dans K^n ($\overline{K}^* = K^* \cup \{\infty\}$), en posant $\psi(\infty, (\xi_1, \ldots, \xi_n)) = (0, \ldots, 0)$; en effet, tous les entiers $\langle \alpha_i, \gamma \rangle$ sont strictement négatifs. Le morphisme composé $\varphi \circ \psi$ se prolonge de même. Or (théorème 1), on a $\gamma(\theta)\varphi(\Theta)\gamma(\theta)^{-1} = (\varphi \circ \psi)(\theta, \Theta)$, pour $\Theta = (\xi_1, \ldots, \xi_n) \in K^n$ et $\theta \in K^*$. Donc, si $b = \varphi(\Theta)$, on a $\gamma(\theta)x = \gamma(\theta)b\sigma_w e_B = (\varphi \circ \psi)(\theta, \Theta)\sigma_w e_B$. D'où $\gamma(\infty)x = \sigma_w e_B$.

14. Groupes finis engendrés par des réflexions[1]

14.1 Réflexions

Soit V un espace vectoriel de dimension finie $n > 0$ sur le corps des nombres *réels*. Si S est une transformation linéaire *involutive* de V, c'est-à-dire si $S^2 = 1$, nous poserons $E_+ = (S+1)/2$, $E_- = (1-S)/2$; on a alors

$$(1) \qquad E_+ + E_- = 1 \qquad E_+E_- = E_-E_+ = 0 \qquad S = E_+ - E_-$$

et par suite E_+ et E_- sont les projecteurs associés à une décomposition de V en somme directe de sous-espaces V_+ et V_- ; on a alors

$$(2) \qquad S(x_+ + x_-) = x_+ - x_-$$

pour $x_\pm \in E_\pm$. Les éléments de $E_\pm$ sont caractérisés par la condition $S(x) = \pm x$. Inversement, si V est somme directe des sous-espaces V_+ et V_-, la formule (2) définit un opérateur involutif.

De plus, si l'on a donné un produit scalaire $(x \mid y)$ sur V, pour que l'opérateur S défini par la formule (2) soit orthogonal, il faut et il suffit que l'on ait

$$(x_+ + x_- \mid x_+ + x_-) = (x_+ - x_- \mid x_+ - x_-)$$

soit $(x_+ \mid x_-) = 0$ pour $x_\pm \in V_\pm$; ceci signifie que les sous-espaces V_+ et V_- de V sont orthogonaux.

Nous appellerons *réflexion un opérateur linéaire S dans V, involutif et dont l'ensemble des points fixes est un hyperplan.*

Si l'on s'est donné un produit scalaire $(x \mid y)$ défini positif sur V, pour tout $a \in V$ non nul, il existe une réflexion S_a et une seule qui soit une transformation orthogonale et applique a sur $-a$. En effet, soit H_a l'hyperplan orthogonal à a ; on devra avoir $V_+ = H_a$ et $V_- = \mathbf{R}\cdot a$ et la réflexion cherchée sera de la forme $1 - 2E$, E étant le projecteur de V sur la droite $\mathbf{R}\cdot a$ nul sur H_a. Or si $Ex = \lambda a$, on doit avoir $x - \lambda a \in H_a$, *i.e.* $(x - \lambda a \mid a) = 0$, d'où en résolvant par rapport à λ, la formule

$$(3) \qquad S_a(x) = x - 2\,\frac{(x \mid a)}{(a \mid a)} \cdot a\,.$$

Il est clair que la formule (3) définit une réflexion répondant à la question. S_a est la seule transformation orthogonale $\neq 1$ qui induise l'identité sur H_a.

[1] Exposé de P. Cartier, le 1.4.1957

14.2 Systèmes de racines

L'espace vectoriel V restera fixé jusqu'à la fin de cet exposé.

Nous appellerons *système de racines*[2] un ensemble *fini* Δ contenu dans V vérifiant les conditions suivantes :

1) *L'espace vectoriel V est engendré par Δ.*

2) *Si $a \in \Delta$, on a $-a \in \Delta$, mais aucun autre vecteur proportionnel à a ne peut appartenir à Δ.*

3) *Pour tout $a \in \Delta$, il existe une réflexion S_a appliquant a sur $-a$ et telle que $S_a\Delta = \Delta$.*

Il résulte immédiatement de ces conditions que $0 \notin \Delta$ et que le groupe G d'opérateurs dans V engendré par les réflexions S_a est fini. De plus, on définit sur le dual V^* de V un produit scalaire défini positif par la formule :

$$(f \mid g) = \sum_{a \in \Delta} f(a)g(a)\,. \tag{4}$$

Par dualité, on définit donc aussi un produit scalaire $(x \mid y)$ défini positif sur V, qui sera invariant par tout opérateur linéaire dans V conservant l'ensemble Δ. En particulier, S_a est la réflexion orthogonale changeant a en $-a$, et c'est donc l'unique transformation linéaire dans V changeant a en $-a$ et conservant Δ. On en déduit $gS_ag^{-1} = S_{g\cdot a}$ pour toute transformation linéaire g conservant Δ. On note H_a l'hyperplan orthogonal à $a \in \Delta$.

Les éléments de Δ seront appelés *racines* ; on posera

$$u(a,b) = -2(a \mid b)/(a \mid a)$$

pour tout couple de racines a, b ; on a donc :

$$u(a,a) = -2 \tag{5}$$

$$S_a b = b + u(a,b)a\,. \tag{6}$$

14.3 Racines fondamentales

Comme l'ensemble Δ est fini, il existe $x_0 \in V$ tel que l'on ait $(x_0 \mid a) \neq 0$ pour toute racine a ; nous noterons Σ l'ensemble des racines a telles que $(x_0 \mid a) > 0$. Les ensembles Σ et $-\Sigma$ forment donc une partition de Δ. Nous munirons V de la relation d'ordre (partielle) compatible avec sa structure

[2] L'usage actuel est de réserver le nom de "systèmes de racines" aux systèmes qui satisfont à la restriction "$u(a,b)$ entier pour tous les couples de racines a, b" (*cf.* remarque 2 du n° 14.7).

d'espace vectoriel réel pour laquelle les éléments positifs sont les combinaisons linéaires à coefficients ≥ 0 d'éléments de Σ. Il est clair que Σ est l'ensemble des racines positives. On note $x \geq y$ cette relation d'ordre.

Considérons l'ensemble **P** des parties F de Σ telles que tout élément de Σ soit combinaison linéaire à coefficients ≥ 0 d'éléments de F et soit π un élément minimal de l'ensemble **P** ordonné par inclusion. On supposera numérotés les éléments de π sous la forme $a_1, a_2, \ldots, a_m$ et l'on posera $S_i = S_{a_i}$. On a alors la proposition fondamentale suivante :

Proposition 1. – *L'ensemble π jouit des propriétés suivantes :*

a) *π est une base de V (donc $m = n$).*

b) *Toute racine est de la forme $\pm \sum \lambda_i a_i$ avec $\lambda_i \geq 0$.*

c) *Les scalaires $u_{ij} = u(a_i, a_j)$ sont ≥ 0 pour $i \neq j$.*

Le b) résulte de la définition de π. Remarquons ensuite que l'on ne peut avoir $\lambda_i a_i - \lambda_j a_j \geq 0$ avec $\lambda_i, \lambda_j > 0$ et $i \neq j$. On aurait en effet dans ce cas une relation $\lambda_i a_i = \lambda_j a_j + \sum \mu_k a_k$ avec des coefficients $\mu_k \geq 0$. On ne pourrait avoir $\lambda_i \leq \mu_i$, car on en déduirait $\sum \nu_k a_k = 0$ avec $a_k > 0$, $\nu_k \geq 0$ et $\nu_j > 0$, ce qui est contradictoire ; on ne peut non plus avoir $\lambda_i > \mu_i$ car il en résulterait $(\lambda_i - \mu_i)a_i = \sum_{k \neq i} \pi_k a_k$ avec $\pi_k \geq 0$, et par suite a_i serait combinaison linéaire à coefficients ≥ 0 des a_k pour $k \neq i$, ce qui contredirait le caractère minimal de π.

Comme on a $S_i a_j > 0$ ou $-S_i a_j > 0$, et que $S_i a_j = a_j + u_{ij} a_i$, on déduit c) de ce qui précède.

Comme Δ engendre V, il en est de même de π, d'après b). Il suffit donc, pour prouver a), de montrer que les $a_i \in \pi$ sont linéairement indépendants. Dans le cas contraire, on aurait une relation de la forme

$$\sum_{i \in I} \lambda_i a_i = \sum_{j \in J} \mu_j a_j = u$$

avec $I \cap J = \varnothing$, $\lambda_i, \mu_j > 0$ et $I, J \neq \varnothing$. On a $(a_i \mid a_j) \leq 0$ pour $i \in I$ et $j \in J$ d'après c), et par suite de $\sum \lambda_i \mu_j (a_i \mid a_j) = (u \mid u) \geq 0$ on déduit $\lambda_i = \mu_j = 0$, ce qui est contradictoire. C.Q.F.D.

Corollaire 1. – *Pour qu'une racine $a > 0$ appartienne à π, il faut et il suffit qu'elle ne soit pas combinaison linéaire à coefficients > 0 de $r \geq 2$ racines positives.*

En effet, pour que a ne soit pas combinaison linéaire à coefficients > 0 de $r \geq 2$ racines positives distinctes, il faut et il suffit qu'elle ne soit pas une telle combinaison de racines a_i (d'après b)). Ceci signifie donc que a est proportionnelle à une des racines a_i donc lui est égale, d'après la condition 2) de la définition des systèmes de racines.

Corollaire 2. – *Soit π' une partie de Σ ; pour que toute racine a soit de la forme $\pm \sum_{b\in\pi'} \lambda_b b$ avec $\lambda_b \geq 0$, il faut et il suffit que $\pi' \supset \pi$.*

La condition est suffisante d'après le b) de la proposition 1 ; elle est nécessaire, car d'après le corollaire 1 toute racine $a_i \in \pi$ est proportionnelle à une racine appartenant à π', donc lui est égale.

Corollaire 3. – *Soit a une racine positive ; si $a \neq a_i$, on a $S_i a > 0$.*

Posons $a = \sum \lambda_j a_j$, d'où $S_i a = a - \mu a_i = \sum_{j\neq i} \lambda_j a_j + (\lambda_i - \mu) a_i$; mais comme a n'est pas proportionnelle à a_i, les scalaires λ_j pour $j \neq i$ sont ≥ 0 et l'un au moins n'est pas nul. Comme $S_i a$ est une racine, tous ses coefficients en fonctions des a_j doivent être de même signe ; comme l'un d'eux est > 0, ils sont tous > 0 et $S_i a > 0$.

On notera que $S_i a_i = -a_i < 0$, donc a_i est la seule racine > 0 dont la transformée par S_i soit < 0.

D'après le corollaire 2, la partie π de Δ ne dépend que de Σ ; on dit que les éléments de π sont les *racines fondamentales ou simples* et que π est un *système de racines simples*. On peut caractériser ainsi les systèmes de racines simples :

Proposition 2. – *Soient $b_1, \ldots, b_n$ des racines. Pour que $\pi' = \{b_i\}_{1\leq i\leq n}$ soit un système de racines simples (pour un ensemble Σ convenable de racines positives), il faut et il suffit que toute racine soit de la forme $\pm \sum \lambda_i b_i$ avec $\lambda_i \geq 0$.*

En effet, comme Δ engendre V, les b_i forment une base de V et par suite, il existe $x_1 \in V$ telle que $(x_1 \mid b_i) > 0$ pour $1 \leq i \leq n$; les racines a de la forme $\sum \lambda_i b_i$ avec $\lambda_i \geq 0$ sont caractérisées par la formule $(x_1 \mid a) > 0$; la proposition résulte alors du corollaire 2 de la proposition 1.

Nous caractériserons au numéro suivant les ensembles possibles de racines positives.

14.4 Relation d'ordre dans V

Nous supposons toujours fixé l'ensemble Σ des racines positives et notons $\pi = \{a_1, \ldots, a_n\}$ l'ensemble des racines simples. A côté de l'ordre déjà introduit dans V, nous considérerons *l'ordre lexicographique* dans V par rapport à la base $(a_1, \ldots, a_n)$ que nous noterons $x \succcurlyeq y$. C'est une relation d'ordre *total* dans V compatible avec la structure d'espace vectoriel réel et les éléments $x \succcurlyeq 0$ non nuls sont par définition les éléments de la forme $x = \lambda_k a_k + \sum_{j>k} \lambda_j a_j$ avec $1 \leq k \leq n$ et $\lambda_k > 0$. Notons aussi que la relation $x \geq y$ entraîne la relation $x \succcurlyeq y$ et que pour $a \in \Delta$, $a \succcurlyeq 0$ équivaut à $a \in \Sigma$.

Proposition 3. – *Soit $x > 0$ un élément de V ; il existe un entier i compris entre 1 et n tel que $x > S_i x$.*

Si l'on avait $(x \mid a_i) \leq 0$ pour toute racine simple a_i, on en déduirait $(x \mid y) \leq 0$ pour tout $y \geq 0$, d'où en particulier $(x \mid x) \leq 0$, ce qui contredit la relation $x \neq 0$; il y a donc un entier i tel que $(x \mid a_i) > 0$ d'où $x > S_i x$ par la formule (3).

Corollaire. – *Toute racine est de la forme $S_{i_1} \dots S_{i_p} a_{i_{p+1}}$, $p \geq 0$.*

Soit W l'ensemble des racines de la forme $S_{i_1} \dots S_{i_p} a_{i_{p+1}}$; il est clair que W contient les racines simples et que $S_i W \subset W$ pour tout i. Soit a une racine positive et supposons que W contienne toutes les racines positives $b \prec a$; il existe i tel que $S_i a < a$, donc $S_i a \prec a$; si $a \neq a_i$, on a $S_i a > 0$, donc $S_i a \in W$ et $a \in W$ et si $a = a_i$, on a aussi $a \in W$. De là résulte par récurrence que W contient Σ ; de plus si $a \in W$, on a aussi $-a \in W$ car $-S_{i_1} \dots S_{i_p} a_{i_{p+1}} = S_{i_1} \dots S_{i_p} S_{i_{p+1}} a_{i_{p+1}}$. On a donc bien $W = \Delta$.

Proposition 4. – *Soient F une partie de π et $x \in V$ tels que $x > S_a x$ (resp. $x \geq S_a x$) pour tout $a \in F$. Si H est le sous-groupe de G engendré par les réflexions S_a pour $a \in F$, on a $x > g \cdot x$ (resp. $x \geq g \cdot x$) pour tout $g \in H$ différent de 1.*

Supposons démontrée l'inégalité $x > g \cdot x$ (resp. $x \geq g \cdot x$) pour $g = S_{c_1} \dots S_{c_q} \neq 1$ quelle que soit la suite $(c_1, \dots, c_q)$ de $q < p$ éléments de F et soit $h = S_{b_1} \dots S_{b_p} \neq 1$ avec $b_i \in F$. Posons $h = h' S_{b_p}$ d'où

$$h \cdot x = h' \cdot S_{b_p} x = h' \cdot x - \lambda h' \cdot b_p \tag{7}$$

avec $\lambda > 0$ (resp. $\lambda \geq 0$) puisque $\lambda b_p = x - S_{b_p} \cdot x > 0$ (resp. ≥ 0). Dans ces conditions, si $h' \cdot b_p > 0$, on aura $h \cdot x < h' \cdot x < x$ (resp. $h \cdot x \leq h' \cdot x \leq x$) par l'hypothèse de récurrence.

Si $h' \cdot b_p < 0$, nous appliquerons le lemme suivant :

Lemme 1. – *Soient $b_1, \dots, b_p$ des racines simples telles que*

$$b = S_{b_1} \dots S_{b_{p-1}} b_p < 0\,. \tag{8}$$

Il existe un indice k tel que $1 \leq k \leq p$ et que

$$b = -S_{b_1} \dots S_{b_{k-1}} b_k \tag{9}$$

$$S_{b_1} \dots S_{b_p} = S_{b_1} \dots S_{b_{k-1}} S_{b_{k+1}} \dots S_{b_{p-1}}\,. \tag{10}$$

Posons $c_j = S_{b_{j+1}} \dots S_{b_{p-1}} b_p$ d'où $c_0 = b < 0$ et $c_p = b_p > 0$. Soit k le plus petit indice tel que $c_k > 0$; on a $k > 0$ et $S_{b_k} c_k = c_{k-1} < 0$; d'après le corollaire 3 de la proposition 1, ceci implique $b_k = c_k$, c'est-à-dire la formule (9) puisque $S_{b_k} b_k = -b_k$. De là, la formule $S_{g \cdot a} = g S_a g^{-1}$ pour $g \in G$ permet de déduire la formule

$$S_{b_k} = (S_{b_{k+1}} \dots S_{b_{p-1}}) S_{b_p} (S_{b_{k+1}} \dots S_{b_{p-1}})^{-1} \tag{11}$$

d'où $S_{b_k} \dots S_{b_{p-1}} = S_{b_{k+1}} \dots S_{b_p}$; comme on a $(S_{b_k})^2 = 1$, la formule (10) se déduit immédiatement de là.

Revenant à la démonstration de la proposition 4, ce lemme montre que si $h' \cdot b_p < 0$, h est le produit de $p-2$ réflexions associées à des éléments de F, et la formule $x > h \cdot x$ (resp. $x \geq h \cdot x$) résulte alors de l'hypothèse de récurrence. Comme on a $x > S_a x$ (resp. $x \geq S_a \cdot x$) pour $a \in F$, la proposition 4 est bien démontrée par récurrence.

Corollaire. – *Soit $x \in V$; pour que l'on ait $x > g \cdot x$ pour tout $g \in G$ différent de 1, il faut et il suffit que l'on ait $(x \mid a_i) > 0$ pour $1 \leq i \leq n$.*

En effet, comme on a $x - S_i x = 2a_i(x \mid a_i)/(a_i \mid a_i)$, les relations $x > S_i x$ et $(x \mid a_i) > 0$ sont équivalentes.

On remarquera que la relation $(x \mid a_i) > 0$ pour $1 \leq i \leq n$ équivaut à la relation $(x \mid a) > 0$ pour toute racine $a > 0$, ou encore à la relation $(x \mid y) > 0$ pour tout $y > 0$.

Venons-en à la caractérisation des ensembles Σ de racines positives.

Proposition 5. – *Soit Σ_0 un ensemble de racines vérifiant les deux conditions :*

a) *Si $b_j \in \Sigma_0$ $(1 \leq j \leq m)$ et si $\sum \lambda_j b_j$ avec $\lambda_j > 0$ est une racine, cette racine appartient à Σ_0.*

b) *Si a est une racine, on a $a \in \Sigma_0$ ou $-a \in \Sigma_0$.*

Alors, il existe $g \in G$ tel que $\Sigma \subset g \cdot \Sigma_0$.

Si Σ_0 vérifie les conditions a) et b) ci-dessus, il en est de même de $g \cdot \Sigma_0$ pour tout $g \in G$; il suffit donc de prouver que si $\Sigma \not\subset \Sigma_0$ et si $\Sigma \cap \Sigma_0$ possède r éléments, il existe une réflexion S_i telle que $\Sigma \cap S_i \Sigma_0$ ait $r+1$ éléments au moins. Or, comme on a $\Sigma \not\subset \Sigma_0$, il existe une racine simple $a_i \notin \Sigma_0$, puisque toute racine positive est combinaison linéaire à coefficients > 0 de racines simples et que Σ_0 satisfait à a).

Si $b \in \Sigma \cap \Sigma_0$ est différente de a_i, on a $S_i b \in \Sigma \cap S_i \Sigma_0$ (corollaire 3 de la proposition 1) ; mais comme $a_i \notin \Sigma_0$, on a $-a_i \in \Sigma_0$ d'après la condition b) et par suite $a_i \in \Sigma \cap S_i \Sigma_0$; comme $a_i \neq S_i b$ si $b > 0$, on a bien prouvé que $\Sigma \cap S_i \Sigma_0$ possède au moins $r+1$ éléments. Ceci achève la démonstration.

Corollaire. – *Pour qu'un ensemble Σ_0 de racines soit un ensemble de racines positives, il faut et il suffit qu'il vérifie les conditions* a) *et* b) *ci-dessus et la condition*

c) *Si a est une racine, on ne peut avoir $a \in \Sigma_0$ et $-a \in \Sigma_0$.*

De plus, si ces conditions sont remplies, il existe $g \in G$ tel que $\Sigma_0 = g \cdot \Sigma$.

Les conditions énoncées sont évidemment nécessaires ; pour montrer la suffisance de la dernière assertion, on peut supposer $\Sigma \subset \Sigma_0$ d'après la proposition 5. Si l'on avait $\Sigma \neq \Sigma_0$, il existerait une racine $a \in \Sigma_0$ non positive ; on aurait alors $-a \in \Sigma \subset \Sigma_0$, ce qui contredirait la condition c).

14.5 Génération du groupe G

Théorème 1. – (Coxeter) *Le groupe G est engendré par les réflexions S_i $(1 \leq i \leq n)$; si a_{ij} est l'ordre (fini) de l'élément S_iS_j de G, toutes les relations entre les S_i sont conséquences des relations :*

$$(S_iS_j)^{a_{ij}} = 1\,. \tag{12}$$

Introduisons le groupe $\mathbf{G}$ défini par les générateurs T_i $(1 \leq i \leq n)$ et les relations $(T_iT_j)^{a_{ij}} = 1$ et l'homomorphisme π de $\mathbf{G}$ dans G qui applique T_i sur S_i. On notera que $a_{ii} = 1$, donc que $(T_i)^2 = 1$.

a) π *est surjectif* : toute racine est de la forme $b = S_{i_1} \ldots S_{i_p} a_{i_{p+1}}$ d'où l'on déduit par la formule $gS_ag^{-1} = S_{g\cdot a}$ que $S_b = (S_{i_1} \ldots S_{i_p})S_{i_{p+1}}(S_{i_1} \ldots S_{i_p})^{-1}$ appartient au sous-groupe de G engendré par les S_i. Comme G est engendré par les réflexions S_b, on a bien montré que π est surjectif.

b) π *induit un isomorphisme du sous-groupe $\mathbf{H}_{ij}$ de $\mathbf{G}$ engendré par T_i et T_j sur le sous-groupe H_{ij} de G engendré par S_i et S_j* : il est clair que $\pi(\mathbf{H}_{ij}) = H_{ij}$; de plus si l'on pose $U = T_iT_j$ et $k = a_{ij}$, on a $U^k = 1$ et $T_iUT_iU = 1$, d'où $T_iU = U^{-1}T_i$ et par récurrence sur m, $T_iU^m = U^{-m}T_i$. Il en résulte immédiatement que les éléments U^m et U^mT_i (pour $0 \leq m < k$) forment un sous-groupe de $\mathbf{G}$, qui contient T_i et T_j donc est égal à $\mathbf{H}_{ij}$. Or les éléments $\pi(U^m) = (S_iS_j)^m$ pour $0 \leq m < k$ sont tous distincts et de déterminant 1, tandis que les éléments $\pi(U^mT_i) = (S_iS_j)^mS_i$ sont tous distincts et de déterminant -1 pour $0 \leq m < k$; il en résulte bien que la restriction de π à $\mathbf{H}_{ij}$ est injective.

c) *A toute racine positive a on peut associer un élément $T_a \in \mathbf{G}$ de manière à vérifier les relations :*

$$T_iT_aT_i^{-1} = T_{S_ia} \qquad \textit{pour } a \neq a_i \tag{13}$$

$$\pi(T_a) = S_a \tag{14}$$

$$T_{a_i} = T_i\,. \tag{15}$$

Les T_a seront construits par récurrence au moyen de l'ordre lexicographique ; supposons donc construits des T_a pour $0 \prec a \prec b$ de telle sorte que les formules (13) à (15) soient vérifiées lorsqu'elles ont un sens ($0 \prec S_ia \prec b$, $0 \prec a \prec b$ et $a_i \prec b$ respectivement). Si b est simple, soit $b = a_i$, nous poserons $T_b = T_i$; dans le cas contraire, nous choisirons un indice i tel que $b \succ S_ib$, donc $b \succ S_ib \succ 0$ puisque $b \neq a_i$ et nous poserons

$$T_b = T_iT_{S_ib}T_i^{-1}$$

d'où $\pi(T_b) = S_b$. Pour continuer la récurrence il suffira de vérifier que pour tout indice j tel que $b \succcurlyeq S_j b$, on a $T_j T_b T_j^{-1} = T_{S_j b}$ (on notera que les relations $b \succcurlyeq S_j b$, $b \geq S_j b$ et $(b \mid b_j) \geq 0$ sont équivalentes).

Si $S_b \in H_{ij}$, la formule précédente résultera alors des formules $\pi(T_a) = S_a$ et de l'assertion b) qui précède.

Dans le cas contraire, il résulte du corollaire 3 de la proposition 1 que les racines $h \cdot b$ sont > 0 pour $h \in H_{ij}$ et de la proposition 4 que ces racines sont $\leq b$ donc $\preccurlyeq b$. De plus, on peut évidemment se limiter au cas où $i \neq j$. Nous distinguerons alors deux cas :

$b \succ S_j b$: on a alors $h \cdot b \prec b$ pour $h \neq 1$ dans H_{ij}. On a $S_j b = (S_i S_j)^{k-1} S_i b$ avec $k = a_{ij}$ et les racines $(S_i S_j)^{\ell} S_i b$ et $S_j (S_i S_j)^{\ell-1} S_i b$ pour $1 \leq \ell < k$ sont toutes $\prec b$. De la formule (13), on déduit alors

$$T_{S_j b} = (T_i T_j)^{k-1} T_{S_i b} (T_i T_j)^{1-k} = U T_b U^{-1}$$

avec $U = (T_i T_j)^{k-1} T_i$ donc $U = T_j$ puisque $(T_i T_j)^k = 1$ et $(T_i)^2 = 1$. On a bien prouvé notre assertion dans ce cas.

$b = S_j b$: soit P le sous-espace de dimension 2 de V engendré par a_i et a_j et soit W le sous-espace de dimension $n-2$ de V orthogonal à P. Tout $h \in H_{ij}$ induit l'identité sur W ; de plus de $S_j b = b$, on déduit que b est orthogonale à a_j, donc aussi que la projection orthogonale b' de b sur P est orthogonale à a_j. Les relations $h \cdot b = b$ et $h \cdot b' = b'$ pour $h \in H_{ij}$ distinct de 1 sont équivalentes puisque $b - b' \in W$; elles signifient que h coïncide sur P avec la réflexion associée à un vecteur de P orthogonal à b' et non nul, donc que $h = S_j$. On a donc $b \succ h \cdot b$ pour $h \in H_{ij}$ différent de 1 et de S_j. Posant toujours $k = a_{ij}$, on aura $b = S_j b = (S_i S_j)^{k-1} S_i b$; comme $u_\ell = S_j (S_i S_j)^{\ell-1} S_i$ et $v_\ell = (S_i S_j)^{\ell-1} S_i$ sont différentes de 1 et S_j pour $1 \leq \ell < k$, on a $u_\ell \cdot b \prec b$ et $v_\ell \cdot b \prec b$ pour $1 \leq \ell < k$, d'où en appliquant le formule (13) un certain nombre de fois

$$T_{S_j b} = (T_i T_j)^{k-1} T_{S_i b} (T_i T_j)^{1-k}$$

et on achève la démonstration comme dans le premier cas.

d) *Si l'on a* $g \in \mathbf{G}$ *et* $\pi(g) \cdot \Sigma = \Sigma$, *on a* $g = 1$.

Supposons démontré que pour $q < p$, l'égalité $S_{i_1} \dots S_{i_q} \cdot \Sigma = \Sigma$ implique $T_{i_1} \dots T_{i_q} = 1$ pour toute suite $(i_1, \dots, i_q)$ d'entiers compris entre 1 et n et supposons que l'on ait $S_{i_1} \dots S_{i_p} \cdot a > 0$ pour toute racine $a > 0$. Appliquant à $a = a_{i_p}$, on voit qu'il existe un entier k tel que $1 \leq k < p$ et que $S_{i_m} \dots S_{i_p} a_{i_p}$ soit négatif pour $k < m \leq p$ mais que $S_{i_k} \dots S_{i_p} a_{i_p} > 0$. Utilisant le corollaire 3 de la proposition 1, on en conclut que $a_{i_k} = S_{i_{k+1}} \dots S_{i_{p-1}} a_{i_p}$; mais d'après c), ceci implique $T_{i_k} = (T_{i_{k+1}} \dots T_{i_{p-1}}) T_{i_p} (T_{i_{k+1}} \dots T_{i_{p-1}})^{-1}$, d'où $T_{i_k} \dots T_{i_{p-1}} = T_{i_{k+1}} \dots T_{i_p}$ et finalement $T_{i_1} \dots T_{i_p} = T_{i_1} \dots T_{i_{k-1}} T_{i_{k+1}} \dots T_{i_{p-1}}$. D'après l'hypothèse de récurrence, on en déduit bien $T_{i_1} \dots T_{i_p} = 1$.

Le théorème résulte alors immédiatement de d).

14.6 Chambres

Soit V' le complémentaire dans V de la réunion des hyperplans H_a ($a \in \Delta$). *Une chambre est une composante connexe de V', ou encore une partie convexe maximale de V'* ; comme une forme linéaire conserve un signe constant sur une partie connexe ou convexe, on voit immédiatement qu'une chambre C_0 est définie par les relations :

$$e(a)(x \mid a) > 0 \qquad \text{pour tout } a \in \Delta$$

$e(a)$ étant un scalaire égal à $+1$ ou -1 et tel que $e(a) = -e(-a)$. Il est clair que l'ensemble Σ_0 des racines a telles que $e(a) = +1$, ou ce qui revient au même $(x \mid a) > 0$ pour $x \in C_0$, vérifie les conditions a) b) et c) du corollaire de la proposition 5, donc est de la forme $g \cdot \Sigma$ avec $g \in G$. De plus, la chambre C définie par les conditions $(x \mid a) > 0$ pour toute racine $a \in \Sigma$, est aussi définie par les conditions $(x \mid a_i) > 0$ pour $1 \leq i \leq n$. Utilisant le corollaire de la proposition 4 et le d) de la démonstration du théorème 1, on en conclut :

Proposition 6. – *L'ensemble C des $x \in V$ tels que $(x \mid a) > 0$ pour toute racine $a \in \Sigma$ est une chambre ; les ensembles $g \cdot C$ ($g \in G$) forment une partition du complémentaire V' dans V de la réunion des hyperplans H_a. Toute partie convexe de V' est contenue dans une chambre et les chambres sont de la forme $g \cdot C$.*

14.7 Remarques finales

1) Soit G un groupe fini de transformations linéaires dans V engendré par des réflexions et ne laissant aucun vecteur non nul fixe.

Soit $S \in G$ une réflexion et soit D la droite de V formée des $x \in V$ tels que $S(x) = -x$; si $g \in G$ conserve la droite D, comme il est d'ordre fini, il ne peut induire que 1 ou -1 sur D. Considérons l'ensemble P de toutes les droites D associées aux symétries $S \in G$ et une partition $P = \bigcup_{i=1}^{m} G \cdot D_i$, choisissons un élément $a_i \neq 0$ dans chaque droite D_i et posons $\Delta = \bigcup_{i=1}^{m} (G \cdot a_i \cup G \cdot (-a_i))$; on définit ainsi un ensemble Δ vérifiant les conditions 1) 2) et 3) du n° 14.2. Par suite, le théorème 1 s'applique à tout groupe fini engendré par des réflexions. *Problème* : Existe-t-il un sous-ensemble $P' \underset{\neq}{\subset} P$ stable par G et tel que les réflexions correspondantes engendrent G ?

2) Soit Δ un système de racines dans V tel que le sous-groupe de V engendré par Δ soit discret, ou ce qui revient au même, soit de rang n sur l'anneau des entiers. Au choix, supposons que Δ soit un sous-ensemble d'un espace vectoriel sur le corps des nombres rationnels vérifiant les conditions 1)

à 3) du n° 14.2. Remplaçant au besoin les éléments de Δ par des multiples entiers convenables, on peut toujours supposer que les nombres $u(a, b)$ sont entiers ; il résulte alors immédiatement du corollaire de la proposition 3 que toute racine est de la forme $\pm\Sigma m_i a_i$ avec m_i entier ≥ 0.

3) Dans le cas 2) les racines simples a_i $(1 \leq i \leq n)$ forment une base de V et pour i et j quelconques, l'angle de a_i et a_j est de la forme $\pi - \pi/n_{ij}$ avec n_{ij} entier ≥ 2 ; on peut[3], par une méthode analogue à celle de l'exposé 13 du Séminaire S. Lie 1954/55, classer les systèmes de vecteurs a_i d'un espace euclidien linéairement indépendants dont les angles deux à deux sont de la forme $\pi - \pi/n_{ij}$ (n_{ij} entier ≥ 2). En dehors des cas étudiés dans *loc. cit.* et du cas $n = 2$, on trouve deux systèmes nouveaux notés H_3 et H_4.

Problème : Démontrer, sans utiliser la classification, que pour un tel système de vecteurs a_i, le groupe de transformations orthogonales engendré par les réflexions S_{a_i} est *fini* (si l'on avait la proposition 6, il suffirait d'utiliser une considération simple de volume).

[3] Voir le théorème 1 du chapitre 6, § 4.1 dans Bourbaki, *Groupes et algèbres de Lie*, Chap. 4, 5, 6, Masson, Paris, 1981.

15. Les systèmes linéaires sur G/B[1]

Notations. – On désigne par G un groupe algébrique semi-simple, par T un tore maximal de G, par B un groupe de Borel contenant T, par B^u l'ensemble des éléments unipotents de B, par $N(T)$ le normalisateur de T, par σ_0 un élément de $N(T)$ tel que l'opération correspondante du groupe de Weyl transforme la chambre associée à B en sa symétrique par rapport à l'origine, par $\widetilde{B}$ le groupe $\sigma_0^{-1} B \sigma_0$ et par $\widetilde{B}^u$ l'ensemble des éléments unipotents de $\widetilde{B}$.

15.1 Compléments au théorème de Bruhat

Rappelons que $\widetilde{B}\,B$ est une partie ouverte de G, et que l'application $(\widetilde{b}, b') \to \widetilde{b}\,b'$ de $\widetilde{B}^u \times B$ dans G est une bijection de $\widetilde{B}^u \times B$ sur une partie ouverte de G (n° 13.4, corollaire 2 au théorème 3). Nous nous proposons d'établir la

Proposition 1. – *L'application $(\widetilde{b}, b') \to \widetilde{b}\,b'$ est un isomorphisme de $\widetilde{B}^u \times B$ sur une sous-variété ouverte de G.*

Il nous suffira d'établir que cette application est birationnelle (*cf.* théorème 2 du n° 5.3, les variétés considérées étant normales puisque non singulières). Nous nous servirons pour cela de la notion d'espace tangent à une variété.

Soit x un point d'une variété U ; désignons par $\mathfrak{o}$ son anneau local et par $\mathfrak{m}$ l'idéal maximal de $\mathfrak{o}$; $\mathfrak{o}/\mathfrak{m}$ est donc un $\mathfrak{o}$-module, d'ailleurs identique à K. Rappelons qu'on appelle vecteur tangent à U en x toute dérivation (K-linéaire) de l'algèbre $\mathfrak{o}$ dans le module $\mathfrak{o}/\mathfrak{m}$. Les vecteurs tangents à U en x forment un espace vectoriel $\mathfrak{L}(x)$, l'espace tangent à U en x, canoniquement isomorphe au dual de l'espace vectoriel $\mathfrak{m}/\mathfrak{m}^2$, où $\mathfrak{m}^2$ est l'idéal engendré par les produits de deux éléments de $\mathfrak{m}$; si x est simple sur U, $\mathfrak{L}(x)$ est de dimension égale à celle de U ; dans le cas contraire, $\mathfrak{L}(x)$ est de dimension $> \dim U$. Soit f une fonction sur U à valeurs dans une variété V, définie en un point x, et soit $y = f(x)$; l'application $L \to L \circ \varphi$ (où φ est le cohomomorphisme de f) est une application linéaire $D_x f$ de l'espace tangent à U en x dans l'espace tangent à V en y, qu'on appelle la *dérivée de f en x*. Ceci dit, nous utiliserons le lemme suivant :

[1] Exposé de C. Chevalley, le 8.4.1957

Lemme 1. – *Soit f un morphisme bijectif d'une variété U sur une partie dense d'une variété V. Supposons qu'il existe un point $x \in U$ tel que $D_x f$ soit une application injective ; f est alors birationnel.*

Soit φ le cohomomorphisme de f, qui est un isomorphisme du corps F_V des fonctions numériques sur V sur un sous-corps du corps F_U des fonctions numériques sur U ; comme f est bijectif, F_U est une extension radicielle de $\varphi(F_V)$ (n° 8.1, proposition 1). Soit $y = f(x)$; soient $\mathfrak{o}_x$ et $\mathfrak{o}_y$ les anneaux locaux de x et de y, $\mathfrak{m}_x$ et $\mathfrak{m}_y$ leurs idéaux maximaux ; il résulte de l'hypothèse que l'application de $\mathfrak{m}_y/\mathfrak{m}_y^2$ dans $\mathfrak{m}_x/\mathfrak{m}_x^2$ déduite de φ est surjective, donc que $\mathfrak{o}_x$ est non ramifié par rapport à $\varphi(\mathfrak{o}_y)$ (n° 5.5) ; ceci entraîne, comme on le sait, que le corps des fractions F_U de $\mathfrak{o}_x$ est séparable sur $\varphi(F_V)$, donc lui est égal.

On sait par ailleurs que, si g est un isomorphisme d'une variété U sur une sous-variété d'une variété V, $D_x g$ est un isomorphisme de l'espace tangent à U en x sur un sous-espace de l'espace tangent à V en $g(x)$.

Ceci étant, nous pouvons aborder la démonstration de la proposition 1. Pour toute racine α de G par rapport à T, il existe un isomorphisme τ_α du groupe additif K sur un sous-groupe de G tel que $t\,\tau_\alpha(x)t^{-1} = \tau_\alpha(\alpha(t)x)$ pour tout $x \in K$ et tout $t \in T$. L'espace tangent à K au point 0 s'identifie canoniquement à K ; posons $X_\alpha = (D_0\,\tau_\alpha)(1)$; X_α est donc un élément non nul de l'espace tangent $\mathfrak{g}$ à G en e. Si la racine α est positive (resp. négative) sur la chambre associée à B, X_α appartient à l'espace tangent $\widetilde{\mathfrak{b}}^u$ (resp. $\mathfrak{b}^u$) à $\widetilde{B}^u$ (resp. B^u) en e. Soit par ailleurs $\mathfrak{t}$ l'espace tangent à T en e.

Lemme 2. – *La somme* $\mathfrak{t} + \sum_{\alpha \in R} KX_\alpha$ (où R est l'ensemble des racines, que nous supposerons ordonné d'une manière quelconque) *est directe.*

Pour tout $t \in T$, soit ζ_t l'automorphisme intérieur $s \to tst^{-1}$ de G. On a $\zeta_t(\tau_\alpha(x)) = \tau_\alpha(\alpha(t)x)$; si $c \in K$, l'homothétie de rapport c dans K est sa propre différentielle au point 0, d'où il résulte immédiatement que l'automorphisme $D_e\,\zeta_t$ de $\mathfrak{g}$ transforme X_α en $\alpha(t)X_\alpha$. Par ailleurs, comme T est commutatif, $D_e\,\zeta_t$ laisse invariants les éléments de $\mathfrak{t}$. Il existe un élément $t \in T$ tel que les $\alpha(t)$, pour toutes les racines α, soient des éléments mutuellement distincts et $\neq 1$; comme des vecteurs propres appartenant à des valeurs propres distinctes d'un opérateur linéaire sont linéairement indépendants, il en résulte bien que la somme $\sum_{\alpha \in R} KX_\alpha + \mathfrak{t}$ est directe.

Soient n le nombre des racines positives et ℓ la dimension de T ; soit R' (resp. R'') l'ensemble des racines positives (resp. négatives). Soit g l'application $(x_\alpha)_{\alpha \in R'} \to \prod_{\alpha \in R'} \tau_\alpha(x_\alpha)$; on sait que c'est une bijection de $K^{R'}$ sur $\widetilde{B}^u$ (théorème 1 du n° 13.2) ; soit $D_0 g$ sa dérivée à l'origine 0 de $K^{R'}$. L'espace tangent à $K^{R'}$ au point 0 s'identifie à $K^{R'}$; il est clair que l'espace $(D_0 g)(K^{R'})$ contient tous les X_α pour $\alpha \in R'$, et est par suite de dimension $\geq n = \dim K^{R'}$; il est donc exactement de dimension n, et $D_0 g$ est une

application injective. De plus, $(D_0 g)(K^{R'})$ est contenu dans $\widetilde{\mathfrak{b}}^u$, qui est de dimension égale à celle de $\widetilde{B}^u$, donc à n. Il résulte alors du lemme 1 que g est un isomorphisme de $K^{R'}$ sur $\widetilde{B}^u$ et on a $\widetilde{\mathfrak{b}}^u = \sum_{\alpha \in R'} KX_\alpha$. On voit de même que l'application $(t, (x_\alpha)_{\alpha \in R''}) \to t \prod_{\alpha \in R''} \tau_\alpha(x_\alpha)$ est un isomorphisme de la variété $T \times K^{R''}$ sur B qui applique $K^{R''}$ sur B^u et que $\mathfrak{b}^u = \sum_{\alpha \in R''} KX_\alpha$; l'espace tangent $\mathfrak{b}$ à B en e est $\mathfrak{t} + \mathfrak{b}^u$. Ceci étant, soit f l'application $(\widetilde{b}, b') \to \widetilde{b}\, b'$ de $\widetilde{B}^u \times B$ dans G ; il est clair que $(D_e f)(\widetilde{\mathfrak{b}}^u \times \mathfrak{b})$ contient $\widetilde{\mathfrak{b}}^u$ et $\mathfrak{b}$, donc est de dimension au moins égale à $2n + \ell = \dim G = \dim \widetilde{B}^u \times B$; procédant comme plus haut, on en déduit que f est un isomorphisme de $\widetilde{B}^u \times B$ sur une sous-variété ouverte de G.

De plus, la démonstration a donné les résultats suivants :

Corollaire 1. – *Soit R l'ensemble des racines de G par rapport à T, rangé dans un ordre quelconque ; soit R' (resp. R'') l'ensemble des racines de R qui sont positives (resp. négatives) sur la chambre associée à B. Alors $(x_\alpha)_{\alpha \in R'} \to \prod_{\alpha \in R'} \tau_\alpha(x_\alpha)$ est un isomorphisme de la variété $K^{R'}$ sur $\widetilde{B}^u$, $(x_\alpha)_{\alpha \in R''} \to \prod_{\alpha \in R''} \tau_\alpha(x_\alpha)$ est un isomorphisme de la variété $K^{R''}$ sur B^u, $(t, b^u) \to t b^u$ est un isomorphisme de la variété $T \times B^u$ sur B.*

Corollaire 2. – *L'application $(b^u, b') \to b^u\, \sigma_0\, b'$ est un isomorphisme de $B^u \times B$ sur une partie ouverte de G.*

On a en effet $b^u\, \sigma_0\, b' = \sigma_0(\sigma_0^{-1}\, b^u\, \sigma_0) b'$, et $\sigma_0^{-1}\, B^u\, \sigma_0 = \widetilde{B}^u$.

Corollaire 3. – *Soit π l'application canonique de G sur G/B ; posons $e_B = \pi(e)$, $x_0 = \sigma_0 \cdot e_B$. Alors $b \to b \cdot x_0$ est un isomorphisme de la variété B^u sur une sous-variété ouverte de G/B.*

En effet, $B^u\, \sigma_0\, B$ est une partie ouverte de G saturée par rapport à la relation d'équivalence définie par les multiplications à droite par les éléments de B. La sous-variété ouverte $\pi(B^u\, \sigma_0\, B)$ de G/B est donc variété quotient de $B^u\, \sigma_0\, B$ par la restriction de π à cette variété, et le corollaire 3 résulte immédiatement du corollaire 2.

Corollaire 4. – *Les variétés B^u, B, G, G/B sont rationnelles.*

Cela résulte immédiatement des corollaires précédents et du fait que T, qui est isomorphe à une puissance de la variété composée des points $\neq 0$ de K, est une variété rationnelle.

15.2 Les systèmes linéaires de diviseurs

Rappelons que, si U est une variété sans singularités, on appelle *diviseurs* sur U les éléments du groupe commutatif libre engendré par les sous-variétés

fermées de codimension 1 de U (variétés que nous appellerons les *hypersurfaces* de U). Si $D = \sum_i e_i V_i$ (les V_i étant des hypersurfaces distinctes et les e_i des entiers $\neq 0$) on appelle *support* de D, et on note $\operatorname{Supp} D$, l'ensemble $\bigcup_i V_i$. Si tous les e_i sont positifs, on dit que D est un *diviseur positif*.

Soit V une sous-variété fermée de codimension 1 de U. L'anneau local $\mathfrak{o}(V)$ de V est alors l'anneau d'une valuation discrète ω_V du corps F_U des fonctions numériques sur U, uniquement déterminée si on impose que son groupe des valeurs soit $\mathbf{Z}$. Si f est une fonction numérique $\neq 0$ sur U, il n'y a qu'un nombre fini de sous-variétés fermées V de codimension 1 telles que $\omega_V(f) \neq 0$; la somme $\sum_V \omega_V(f)V$ est un diviseur, qu'on appelle le diviseur de f et qu'on note (f) ; les diviseurs des fonctions $\neq 0$ sont dits *principaux*. Si f et g sont des fonctions numériques $\neq 0$, on a $(fg) = (f) + (g)$; les diviseurs principaux forment donc un groupe. On dit que deux diviseurs sont *linéairement équivalents* si leur différence est un diviseur principal. On appelle *système linéaire* sur U un ensemble Σ de diviseurs qui possède la propriété suivante : les éléments de Σ sont tous positifs ; il existe un diviseur D_0 et un sous-espace vectoriel E de dimension finie du corps F_U des fonctions numériques sur U tels que Σ se compose de tous les diviseurs $(f) + D_0$, où f parcourt l'ensemble des éléments $\neq 0$ de E. L'espace E est dit être un *espace de définition* de Σ ; tout autre espace de définition de Σ est de la forme gE, où g est une fonction numérique fixe non nulle. Si on suppose la variété U complète, les éléments de Σ sont en correspondance biunivoque avec les points de l'espace projectif $P(E)$ associé à E ; ceci définit sur Σ une structure d'espace projectif, bien déterminée à un isomorphisme près.

Ceci dit, nous allons étudier les systèmes linéaires de la variété complète sans singularités G/B. Nous désignerons par π l'application canonique de G sur G/B ; nous poserons $x_0 = \pi(\sigma_0)$, $\Omega_0 = B^u \cdot x_0$; on sait que Ω_0 est une sous-variété ouverte de G/B et que $b \to b \cdot x_0$ est un isomorphisme de la variété B^u sur Ω_0 ; Ω_0 est donc isomorphe à K^n si $n = \dim B^u$. Soient $\alpha_1, \ldots, \alpha_\ell$ les racines fondamentales relativement à B ; pour chaque k, soit σ_k une opération du normalisateur de T dont la classe modulo T soit la réflexion w_k par rapport à σ_k ; nous poserons $x_k = \sigma_k \cdot x_0$. On sait que G/B est la réunion de Ω_0, des $B^u x_k$ $(1 \leq k \leq \ell)$ et d'un certain nombre d'ensembles de codimensions > 1 (corollaire 2 au théorème 3 du n° 13.4) ; chaque $B^u x_k$ est de codimension 1 et contenu dans $\Omega - \Omega_0$; son adhérence, que nous désignerons par Δ_k, est donc une hypersurface contenue dans $\Omega - \Omega_0$, et les Δ_k $(1 \leq k \leq \ell)$ sont les seules hypersurfaces contenues dans $\Omega - \Omega_0$. Le groupe G, qui opère sur G/B, opère de manière évidente sur le groupe des diviseurs de G/B ; il est clair que toute opération de G transforme tout diviseur principal en un diviseur principal. D'une manière plus précise, si on désigne par μ_s le cohomomorphisme de la transformation de G/B définie par s, et si u est une fonction numérique sur G/B, on a $s \cdot (u) = (\mu_{s^{-1}}(u))$.

Proposition 2. – *Soit D un diviseur quelconque sur G/B. Il existe alors un système et un seul d'entiers e_k $(1 \leq k \leq \ell)$ tel que D soit linéairement équivalent à $\sum_k e_k \Delta_k$.*

Si V est une hypersurface de G/B qui rencontre Ω_0, $V \cap \Omega_0$ est une hypersurface de la variété Ω_0 ; il y a un homomorphisme ρ du groupe des diviseurs de G/B sur celui de Ω_0 qui applique une hypersurface quelconque V de G/B sur $V \cap \Omega_0$ si $V \cap \Omega_0 \neq \varnothing$, sur 0 dans le cas contraire. Il est clair que, pour toute fonction numérique u sur G/B, $\rho((u)) = (\rho(u))$ où $\rho(u)$ est la restriction de u à Ω_0. Par ailleurs, si W est une hypersurface de K^n, c'est l'ensemble des zéros dans K^n d'un polynôme irréductible w, et le diviseur W est (w) ; on en conclut que tout diviseur de K^n, et par suite aussi de Ω_0, est principal. Ceci dit, soit D un diviseur de G/B ; $\rho(D)$ peut alors se mettre sous la forme (v), où v est une fonction numérique sur Ω_0, qui est la restriction à Ω_0 d'une fonction numérique u sur G/B. Le diviseur $D - (u)$ appartient au noyau de ρ, qui est le groupe engendré par les Δ_k, de sorte que D est linéairement équivalent à une combinaison linéaire des Δ_k. Par ailleurs, si $\sum_{k=1}^{\ell} e_k \Delta_k$ est le diviseur d'une fonction numérique u, le diviseur de $\rho(u)$ est 0 ; or il est clair qu'une fonction numérique sur K^n dont le diviseur est nul est constante ; $\rho(u)$ est donc constante, et il en est de même de u, d'où $e_k = 0$ $(1 \leq k \leq \ell)$; la proposition 2 est donc établie.

Proposition 3. – *Chacune des hypersurfaces Δ_k est invariante par les opérations de B ; tout diviseur qui est transformé en lui-même par les opérations de B^u est une combinaison linéaire des Δ_k.*

Si $s \in B^u$, on a $sB^u x_k = B^u x_k$, d'où $s \cdot \Delta_k = \Delta_k$; si $t \in T$, on a $tB^u x_k = tB^u t^{-1} t x_k = B^u x_k$ puisque $tB^u t^{-1} = B^u$, $tx_k = x_k$, d'où $t \cdot \Delta_k = \Delta_k$; les Δ_k sont donc invariants par les opérations de B. Soit D un diviseur invariant par les opérations de B^u ; $\operatorname{Supp} D$ est alors transformé en lui-même par les opérations de B^u ; or Ω_0 est une orbite du groupe B^u opérant dans G/B, et n'est évidemment pas contenu dans $\operatorname{Supp} D$; on a donc $\operatorname{Supp} D \subset \Omega - \Omega_0$, ce qui démontre la deuxième assertion.

Proposition 4. – *Si $s \in G$ et si D est un diviseur de G/B, sD est linéairement équivalent à D.*

C'est vrai si $s \in B$ en vertu des propositions 2 et 3. Si s est un élément quelconque de G, il existe un $g \in G$ tel que $gsg^{-1} \in B$ (n° 6.6, théorème 6, b)) ; on a $sD = sg^{-1}gD = g^{-1}(gsg^{-1}) \cdot gD$; or $gsg^{-1} \cdot gD$ est linéairement équivalent à gD, donc sD est linéairement équivalent à $g^{-1}gD = D$.

Soit $(e) = (e_1, \ldots, e_\ell)$ une suite de ℓ entiers $e_k \geq 0$; nous désignerons par $D_{(e)}$ le diviseur $\sum_{k=1}^{\ell} e_k \Delta_k$. Nous allons montrer que les $sD_{(e)}$, $s \in G$, font partie d'un système linéaire. Pour tout $s \in G$, nous choisirons une fonction

numérique u_s sur G/B telle que $(u_s) = sD_{(e)} - D_{(e)}$; on peut supposer que $u_s = 1$ si $s \in B$ (proposition 3). Par ailleurs, nous poserons pour toute fonction numérique u sur G/B, $u^s = \mu_{s^{-1}}(u)$ ($\mu_{s^{-1}}$ étant le cohomomorphisme de l'automorphisme produit par s^{-1} dans G/B) ; on a donc $s \cdot (u) = (u^s)$. Comme toute fonction numérique sur G/B de diviseur 0 est une constante, et comme on a $(u_{s's}) = (u_s^{s'}) + (u_{s'})$, on a $u_{s's} = c(s', s) u_s^{s'} u_{s'}$, si $s, s' \in G$, avec $c(s', s) \in K^*$; il s'ensuit que $u_{s''s's} = c(s'', s's)\, c(s', s) u_s^{s''s'}\, u_{s'}^{s''}\, u_{s''}$, et par suite, si $b, b' \in B$, $\sigma \in G$,

$$u_{b\sigma b'} = c(b, \sigma b')\, c(\sigma, b')\, u_\sigma^b\,.$$

Par ailleurs, soit f l'application $b \to bx_0$ de B^u sur Ω_0 ; pour tout $s \in G$, la fonction u_s est partout définie[2] sur Ω_0, de sorte que $u_s \circ f$ est une fonction numérique partout définie sur B^u. Si $b \in B^u$, on a $u_s^b \circ f = (u_s \circ f)^b$, où v^b représente la transformée d'une fonction numérique v sur B^u par le cohomomorphisme de la translation à gauche par b^{-1}. On sait que, si v est partout définie sur B^u, les v^b, pour tous les $b \in B^u$, engendrent un espace vectoriel de dimension finie (n° 4.2, lemme 2). On en conclut que, si σ est un élément fixe de G, les $u_{b\sigma b'}$ pour tous les $b \in B^u$, $b' \in B$ engendrent un espace vectoriel de dimension finie ; comme G est la réunion d'un nombre fini d'ensembles de la forme $B^u \sigma B$, on en conclut que les u_s ($s \in G$) engendrent un espace vectoriel de dimension finie. *Nous désignerons par $\Sigma_{(e)}$ le plus petit système linéaire contenant tous les diviseurs $sD_{(e)}$, $s \in G$.*

Remarque. – Il n'est pas difficile d'établir (en utilisant le théorème de complète réductibilité des représentations linéaires de G) que, si le corps de base K est de caractéristique 0, $\Sigma_{(e)}$ est l'ensemble de tous les diviseurs positifs linéairement équivalents à $D_{(e)}$. Il n'en est plus en général ainsi dans le cas où K est de caractéristique $\neq 0$.

15.3 Représentations projectives du groupe G

Si $s \in G$, nous désignerons par $\rho_{(e)}(s)$ la permutation $D \to sD$ de l'ensemble $\Sigma_{(e)}$; il est clair que $\rho_{(e)}$ est un homomorphisme de G dans le groupe des permutations de $\Sigma_{(e)}$. Par ailleurs, *$\Sigma_{(e)}$ est muni d'une structure d'espace projectif ; montrons que les $\rho_{(e)}(s)$ sont des automorphismes de cet espace projectif.* Soit E l'espace vectoriel engendré par les u_s ; $\Sigma_{(e)}$ est donc l'espace projectif associé à E. Soit $D \in \Sigma_{(e)}$, $D - D_{(e)} = (u)$, où $u \in E$; on a $sD - D_{(e)} = (u^s\, u_s)$, et notre assertion résulte de ce que l'application $u \to u^s\, u_s$ est linéaire, donc un automorphisme de E. *Le groupe* $\mathrm{PL}(\Sigma_{(e)})$ *des automorphismes de $\Sigma_{(e)}$ possède une structure évidente de groupe algébrique*[3] *;*

[2] Le diviseur de u_s sur G/B est égal à $sD_{(e)} - D_{(e)}$, et $D_{(e)}$ est un diviseur positif porté par $\Omega - \Omega_0$; l'ensemble polaire de u_s est donc porté par $\Omega - \Omega_0$, et u_s est régulière en tout point de la variété normale Ω_0.

[3] C'est le quotient de $\mathrm{GL}(E)$ par son centre isomorphe à K^*.

montrons que $\rho_{(e)}$ est un morphisme de G dans $\mathrm{PL}(\Sigma_{(e)})$. Nous allons d'abord montrer que sa restriction à B est un morphisme. Si $s \in B$, on a $u_s = 1$, et il suffira de montrer que l'application qui, à tout $s \in B$ fait correspondre l'automorphisme $u \to u^s$ de E est une représentation rationnelle de B. Or, soit f' l'application $b \to bx_0$ de B sur Ω_0 ; pour tout $u \in E$, $u \circ f'$ est une fonction régulière sur B, et $u \to u \circ f'$ est un isomorphisme de E sur un sous-espace E' de l'espace des fonctions régulières sur B ; ce sous-espace est invariant par les cohomomorphismes des translations à gauche de B ; il est alors bien connu que l'application qui à tout $b \in B$ fait correspondre la restriction à E' du cohomomorphisme de la translation à gauche par b^{-1} est une représentation rationnelle de B (voir le n° 4.2). Ceci montre que la restriction de $\rho_{(e)}$ à B est un morphisme. On conclut alors au moyen du lemme suivant :

Lemme 3. – *Un homomorphisme h du groupe G dans un groupe algébrique H qui induit un morphisme de B dans H est lui-même rationnel.*

L'application $(b, b') \to h(b)\,h(\sigma_0)\,h(b')$ est évidemment un morphisme. Il en résulte (corollaire 2 de la proposition 1) que la restriction de h à la partie ouverte $U = B^u\,\sigma_0\,B$ de G est un morphisme. Si s_0 est un point quelconque de G, la formule $h(s_0\,s) = h(s_0)\,h(s)$ montre que la restriction de h à $s_0\,U$ est un morphisme ; comme G est la réunion des parties ouvertes $s_0\,U$, h est un morphisme.

Nous appellerons *représentation projective* d'un groupe G tout homomorphisme de G dans le groupe des automorphismes d'un espace projectif Σ sur K ; si $\varnothing$ et Σ sont les seules variétés linéaires de Σ stables par G et que $\Sigma \neq \varnothing$, nous dirons que ρ est *simple*. Avec cette terminologie, nous avons prouvé que $\rho_{(e)}$ est une représentation projective rationnelle de G, d'espace $\Sigma_{(e)}$.

Proposition 5. – *Les représentations projectives rationnelles $\rho_{(e)}$ sont simples.*

Soit Σ' une sous-variété linéaire $\neq \varnothing$ de $\Sigma_{(e)}$ stable par G. Comme Σ' est une variété complète, et que B est résoluble et connexe, il y a au moins un point D de Σ' qui est stable par les opérations de B (n° 6.1, théorème 1) ; alors D est de la forme $D_{(e')}$ pour un système convenable (e') d'entiers (proposition 3) ; comme $D_{(e')}$ est linéairement équivalent à $D_{(e)}$, il lui est égal (proposition 2), d'où $(e') = (e)$, et donc $D_{(e)} \in \Sigma'$. Ceci entraîne $\Sigma' = \Sigma_{(e)}$ puisque Σ' est stable par G.

Remarque. – On notera que le raisonnement que nous venons de faire montre que $\Sigma_{(e)}$ ne contient qu'un seul point invariant par B.

Si P est l'espace projectif associé à un espace vectoriel E, l'espace P^* des hyperplans de P s'identifie canoniquement à l'espace projectif associé au dual de E ; de plus, P s'identifie canoniquement au dual de P^*. Si ρ est une représentation projective de G d'espace P, on obtient une représentation

projective ρ^* de G, d'espace P^*, en associant à tout $s \in G$ la permutation $H \to sH$ des hyperplans de P ; on dit que ρ^* est la *contragrédiente de* ρ. Si ρ est rationnelle (resp. simple), il en est de même de ρ^* ; la représentation contragrédiente de ρ^* s'identifie à ρ.

Proposition 6. – *Toute représentation projective rationnelle simple de G est équivalente à l'une des représentations $\rho_{(e)}$ construites ci-dessus.*

Il suffira d'établir que, si ρ est une représentation projective rationnelle simple de G, d'espace P, la contragrédiente ρ^* de ρ est équivalente à l'une des représentations $\rho_{(e)}$. Il existe au moins un point y_0 de P qui est invariant par les opérations de $\rho(B)$, puisque B est résoluble (n° 6.1, théorème 1). Nous désignerons par Θ l'orbite de ce point relativement à G. L'application $s \to \rho(s)\cdot y_0$ définit par passage aux quotients un morphisme f de G/B sur la variété Θ ; Θ est donc une variété complète sans singularités. La sous-variété linéaire de P engendrée par Θ est stable par G, et par suite identique à P car ρ est simple ; Θ n'est donc contenue dans aucun hyperplan de P. Par ailleurs, il existe au moins un point H_0 de P^* invariant par les opérations de $\rho^*(B)$ (n° 6.1, théorème 1) ; H_0 est donc un hyperplan transformé en lui-même par les opérations de $\rho(B)$. Il est clair que deux hyperplans quelconques de P sont des diviseurs linéairement équivalents sur la variété P, et que les fonctions numériques v sur P telles que $(v)+H_0$ soit un hyperplan forment un espace vectoriel V de dimension finie. Comme Θ n'est contenue dans aucun hyperplan de P, toute fonction $v \in V$ induit une fonction numérique $\overline{v}$ sur Θ ; nous poserons $\psi(v) = \varphi(\overline{v})$, où φ est le cohomomorphisme de $f : G/B \to \Theta$; comme la relation $v \neq 0$ entraîne $\overline{v} \neq 0$, ψ est un isomorphisme de V sur un espace vectoriel E composé de fonctions numériques sur G/B. Il est clair que l'on a $f(s \cdot x) = \rho(s) \cdot f(x)$ si $s \in G$, $x \in G/B$; l'ensemble fermé $f^{-1}(H_0 \cap \Theta)$ est donc transformé en lui-même par les opérations de B ; comme cet ensemble n'est pas G/B tout entier, et comme Ω_0 est l'orbite de chacun de ses points relativement à B, on en conclut que $f^{-1}(\Theta \cap H_0) \subset \Omega - \Omega_0$. Si $v \in V$, la fonction $\overline{v}$ est définie en tout point de Θ n'appartenant par à H_0, d'où il résulte que $\psi(v)$ est définie en tout point de Ω_0, et par suite que son diviseur est de la forme $D - D'$ où D, D' sont des diviseurs positifs tels que D' soit combinaison linéaire des Δ_k. Comme E est de dimension finie, il résulte immédiatement de là qu'il y a un système (e) et un seul d'entiers ≥ 0 tels que l'ensemble des $\psi(v) + D_{(e)}$ $(v \in V,\ v \neq 0)$ se compose de diviseurs positifs et n'ait pas de composante fixe (*i.e.* il n'existe aucune hypersurface de G/B qui intervienne avec un coefficient > 0 dans tous les diviseurs de l'ensemble). Pour tout $H \in P^*$, désignons par v_H une fonction telle que $(v_H) = H - H_0$, et posons $j(H) = (\psi(v_H)) + D_{(e)}$. Si s est un élément de G, et v une fonction numérique sur P (resp. sur Θ, sur G/B) nous désignerons par v^s la transformée de v par le cohomomorphisme de $\rho(s^{-1})$ (resp. de la restriction de $\rho(s^{-1})$ à Θ, de l'automorphisme de G/B défini par s^{-1}). Il est clair que, si v induit sur Θ une fonction $\overline{v}$, v^s induit sur Θ la fonction $\overline{v}^s$; comme $f(s \cdot x) = \rho(s) \cdot f(x)$ si $x \in G/B$, $s \in G$, on en déduit que $\psi(v^s) =$

$(\psi(v))^s$ si $v \in V$. Pour simplifier, nous désignerons par sH le transformé d'un hyperplan H de P par $\rho(s)$. Il est clair que l'on a $v_{sH} = cv_H^s\, v_{sH_0}$, d'où $\psi(v_{sH}) = c(\psi(v_H))^s\, \psi(v_{sH_0})$, c étant un élément $\neq 0$ de K ; on en déduit qu'il existe un diviseur A_s, ne dépendant pas de H, tel que $j(sH) = sj(H) + A_s$. Comme l'ensemble des $j(H)$ pour tous les $H \in P^*$ n'a pas de composante fixe, il en est de même de l'ensemble des $sj(H)$; on en conclut immédiatement que $A_s = 0$, $j(sH) = sj(H)$. Par ailleurs, P^* peut être identifié de manière évidente à l'espace projectif associé à V ; comme ψ est un isomorphisme de V sur E, j est un isomorphisme de l'espace projectif P^* sur le système linéaire $j(P^*)$. Ce dernier contient $D_{(e)}$, car $j(H_0) = D_{(e)}$; de plus, il est stable par les opérations de G ; il contient donc $\Sigma_{(e)}$. Comme $j^{-1}(\Sigma_{(e)})$ est une variété linéaire de P^* transformée en elle-même par toutes les opérations de $\rho^*(G)$, cette variété est P^* tout entier, et l'on a $j(P^*) = \Sigma_{(e)}$. L'existence de l'isomorphisme j montre que la représentation ρ^* est équivalente à $\rho_{(e)}$.

Corollaire 1. – *Si ρ est une représentation projective rationnelle simple de G, il existe un unique point de l'espace de ρ qui soit invariant par les opérations de $\rho(B)$.*

Cela résulte immédiatement de la proposition 6 et de la remarque qui suit la démonstration de la proposition 5.

Corollaire 2. – *Soit ρ une représentation linéaire rationnelle simple de G. L'ensemble des points de l'espace V de ρ qui sont invariants par les opérations de B^u est un sous-espace de dimension* 1.

Soit $P(V)$ l'espace projectif associé à V ; pour tout $s \in G$, soit $\rho'(s)$ l'automorphisme de $P(V)$ défini par l'automorphisme $\rho(s)$ de V ; il est clair que ρ' est une représentation projective rationnelle simple de G. Soit V_0 l'ensemble des points de V invariants par B^u ; cet espace est transformé en lui-même par les opérations de $\rho(T)$; il a donc une base $(x_1, \ldots, x_m)$ composée de points tels que les espaces Kx_i soient invariants par les opérations de $\rho(T)$; mais les points Kx_i de $P(V)$ sont alors invariants par B, d'où $m \leq 1$. Réciproquement, il y a au moins un $x \neq 0$ de V tel que Kx soit invariant par B ; dans ces conditions, on a, pour $s \in B$, $\rho(s) \cdot x = a(s)x$, $a(s) \in K^*$: il est clair que la fonction a est un caractère rationnel du groupe B ; elle est donc constante et de valeur 1 sur le groupe unipotent B^u.

16. Les poids dominants[1]

16.1 Groupe linéaire associé à une représentation projective

Soit G un groupe algébrique semi-simple, et soit ρ une représentation rationnelle projective de G ; supposons que l'espace de ρ soit l'espace projectif $P(V)$ associé à un espace vectoriel V. Il y a un homomorphisme canonique ω du groupe $\mathrm{SL}(V)$ des automorphismes de determinant 1 de V sur le groupe $\mathrm{PL}(V)$ des automorphismes de $P(V)$; $\omega^{-1}(\rho(G))$ est un sous-groupe fermé de $\mathrm{SL}(V)$; la composante neutre $\widetilde{G}$ de ce groupe sera appelée le *groupe linéaire associé* à la représentation projective ρ. Soient B un groupe de Borel de G et T un tore maximal contenu dans B ; alors $\rho(B)$ est un groupe de Borel de $\rho(G)$, et $\rho(T)$ en est un tore maximal. Le noyau de ω est un sous-groupe fini du centre de $\mathrm{SL}(V)$; la composante neutre $\widetilde{T}$ dans $\omega^{-1}(\rho(T))$ est un groupe résoluble dont les éléments unipotents forment un groupe fini ; c'est donc un tore, et c'est évidemment un tore maximal de $\widetilde{G}$. Pour tout tore T, nous désignerons dans ce qui suit par $X(T)$ le groupe des caractères rationnels de T et par $X^{\mathbf{Q}}(T)$ l'espace vectoriel $\mathbf{Q} \otimes X(T)$ sur le corps $\mathbf{Q}$ des nombres rationnels. Ceci étant, il est clair que le cohomomorphisme de la restriction de ω à $\widetilde{T}$ définit un isomorphisme de $X(\rho(T))$ sur un sous-groupe d'indice fini de $X(\widetilde{T})$, qui se prolonge en un isomorphisme de $X^{\mathbf{Q}}(\rho(T))$ sur $X^{\mathbf{Q}}(\widetilde{T})$; désignons par ζ_0 l'isomorphisme réciproque de $X^{\mathbf{Q}}(\widetilde{T})$ sur $X^{\mathbf{Q}}(\rho(T))$. Le cohomomorphisme de la restriction de ρ à T définit un isomorphisme de $X(\rho(T))$ sur un sous-groupe de $X(T)$ qui se prolonge en un isomorphisme de $X^{\mathbf{Q}}(\rho(T))$ sur un sous-espace de $X^{\mathbf{Q}}(T)$; en le composant avec ζ_0, on obtient un isomorphisme ζ de $X^{\mathbf{Q}}(\widetilde{T})$ sur un sous-espace de $X^{\mathbf{Q}}(T)$.

L'espace V possède une base $(v_1, \ldots, v_n)$ composée de vecteurs qui sont des vecteurs propres pour les opérations de $\widetilde{T}$; soit $\widetilde{t} \cdot v_i = \widetilde{\chi}_i(\widetilde{t})\, v_i$; les $\widetilde{\chi}_i$ sont alors des éléments de $X(\widetilde{T})$. Leurs images par l'isomorphisme ζ sont des éléments de $X^{\mathbf{Q}}(T)$ qui sont appelés les *poids* de la représentation ρ. Il convient d'observer que, bien que les χ_i n'appartiennent pas en général à $X(T)$, leurs différences mutuelles sont dans $X(T)$: cela résulte de ce que, si l'on pose $\widetilde{s} \cdot v_i = \sum_{j=1}^{n} a_{ji}(\widetilde{s})\, v_j$ pour $\widetilde{s} \in \mathrm{SL}(V)$, les rapports mutuels des fonc-

[1] Exposé de C. Chevalley, le 29.4.1957

tions $\widetilde{s} \to a_{ji}(\widetilde{s})$ sont les images par le cohomomorphisme de ω de fonctions numériques sur $\mathrm{PL}(V)$.

Supposons maintenant que la représentation projective ρ soit simple. On sait qu'il existe un point et un seul de $P(V)$ qui est invariant par les opérations de $\rho(B)$; ce point peut se mettre sous la forme Kv, où v est un élément $\neq 0$ de V, et on peut supposer que v est le premier élément de la base $(v_1, \ldots, v_n)$ choisie plus haut. Ceci étant, le poids χ_1 s'appelle le *poids dominant* de la représentation ρ. Nous nous proposons dans ce qui suit de déterminer les poids dominants des représentations projectives simples $\rho_{(e)}$ que nous avons construites précédemment.

16.2 Poids dominants des représentations projectives simples

Si $\rho = \rho_{(e)}$, nous pouvons prendre pour V l'espace vectoriel engendré par les fonctions numériques v sur G/B dont les diviseurs sont de la forme $s \cdot D_{(e)} - D_{(e)}$, où s parcourt les éléments de G ($D_{(e)}$ étant défini comme au n° 15.2). Soit R l'ensemble des racines qui sont négatives sur la chambre associée à B, ces racines étant rangées dans un ordre quelconque. Soit π l'application canonique de G sur G/B. Pour toute racine α, soit τ_α un isomorphisme de K sur un sous-groupe de G tel que l'on ait $t\,\tau_\alpha(\xi)\,t^{-1} = \tau_\alpha(\alpha(t)\,\xi)$ pour tout $\xi \in K$ et tout $t \in T$ (théorème 1 du n° 13.2). Si on désigne par x_0 le point de G/B qui est invariant par les opérations du groupe de Borel $\widetilde{B}$ opposé à B, tout élément x de l'ensemble ouvert $\Omega_0 = \pi(B^u)$ se met d'une manière et d'une seule sous la forme $\prod_{\alpha\in R} \tau_\alpha(u_\alpha(x)) \cdot x_0$, les $u_\alpha(x)$ étant dans K ; de plus, chaque u_α est une fonction numérique partout définie sur Ω_0 et l'algèbre des fonctions numériques partout définies sur Ω_0 est engendrée par les u_α (que nous identifions aux fonctions sur G/B qui les prolongent) (corollaires 1 et 3 à la proposition 1 du n° 15.1). Les fonctions appartenant à V sont partout définies sur Ω_0. Pour tout élément s de G, nous désignons par v^s la transformée d'une fonction numérique v sur G/B par le cohomomorphisme de l'application $x \to s^{-1} \cdot x$ de G/B sur lui-même. Si w_s est une fonction de diviseur $s \cdot D_{(e)} - D_{(e)}$, la relation $v \in V$ entraîne $v^s\, w_s \in V$, et on a (en posant $\rho = \rho_{(e)}$), $\rho(s) \cdot Kv = Kv^s\, w_s$. Si $\widetilde{s}$ est un élément de $\widetilde{G}$ tel que $\omega(\widetilde{s}) = \rho(s)$, on a donc $\widetilde{s} \cdot v = c_s\, v^s\, w_s$, où c_s est une constante. Si $s \in B$, on peut prendre $w_s = 1$. On peut former une base $(v_1, \ldots, v_n)$ de V, contenant $1 = v_1$, telle que l'on ait, pour $t \in T$, $v_i^t = \chi_i'(t)\, v_i$, les χ_i' étant des éléments de $X(T)$. Si $\widetilde{t} \in \widetilde{T}$, $\omega(\widetilde{t}) = \rho(t)$, on aura $\widetilde{t} \cdot v_i = c(\widetilde{t})\, \chi_i'(t)\, v_i$. Si nous désignons par $d(t)$ le déterminant de l'application $v \to v^t$, il résulte du fait que $\det \widetilde{t} = 1$ que $c^n(\widetilde{t})\, d(t) = 1$; les poids χ_i de la représentation ρ seront, en notation additive,

$$\chi_i = \chi_i' - n^{-1}\, d\,.$$

Comme on a $v_1^s = v_1$ pour tout élément s de B, on a $\chi_1' = 1$ (0 en notation additive!) et le poids fondamental est $-n^{-1}\,d$. Mais il n'est pas facile de calculer la fonction d au moyen des entiers e_i ; nous allons donc suivre tout à l'heure une autre méthode pour calculer le poids fondamental.

Pour le moment, nous observons que l'on a $u_\alpha^t = \alpha(t^{-1})\,u_\alpha$, comme il résulte tout de suite des formules $t^{-1}\,\tau_\alpha(\xi)\,t = \tau_\alpha(\alpha(t^{-1})\,\xi)$ et du fait que $t \cdot x_0 = x_0$. On en déduit que, si $u = \prod_{\alpha \in R} u_\alpha^{k(\alpha)}$ est un monôme en les u_α (les $k(\alpha)$ étant des exposants positifs), on a $u^t = \Big(\prod_{\alpha \in R} \alpha(t)^{-k(\alpha)}\Big) u$; comme V est contenu dans l'algèbre $K[\ldots, u_\alpha, \ldots]$, on en conclut que les χ_i' sont tous de la forme $-\sum_{\alpha \in R} k(\alpha)\,\alpha$, où les $k(\alpha)$ sont des entiers ≥ 0. Comme on a $\chi_i - \chi_j = \chi_i' - \chi_j'$, on en déduit la

Proposition 1. – *Soit ρ une représentation projective rationnelle simple de G. Les différences mutuelles des poids de ρ sont des combinaisons linéaires à coefficients entiers des racines. Si χ_1 est le poids fondamental de ρ (relativement à un groupe de Borel B) et χ un poids quelconque de ρ, $\chi_1 - \chi$ est une combinaison linéaire à coefficients entiers ≥ 0 de celles des racines qui sont négatives sur la chambre associée à B.*

Retournons pour un moment au cas où ρ est une représentation projective rationnelle quelconque de G. Les poids de ρ sont des éléments de l'espace vectoriel $X^{\mathbf{Q}}(T)$ sur lequel opère le groupe de Weyl de G ; nous allons établir la

Proposition 2. – *Les poids d'une représentation projective rationnelle de G sont permutés entre eux par les opérations du groupe de Weyl.*

Soient s une opération du normalisateur de T et w l'opération correspondante du groupe de Weyl. Soit $\widetilde{s}$ un élément du groupe $\widetilde{G}$ tel que $\omega(\widetilde{s}) = \rho(s)$; il est clair que $\widetilde{s}$ normalise $\widetilde{T}$; si t, $\widetilde{t}$ sont des éléments de T, $\widetilde{T}$ respectivement tels que $\rho(t) = \omega(\widetilde{t})$, on a aussi $\rho(sts^{-1}) = \omega(\widetilde{s}\,\widetilde{t}\,\widetilde{s}^{-1})$. Il correspond à $\widetilde{s}$ un automorphisme $\widetilde{w}$ de $X(\widetilde{T})$ qui change tout élément $\widetilde{\chi}$ de ce groupe en la fonction $\widetilde{t} \to \widetilde{\chi}(\widetilde{s}^{-1}\,\widetilde{t}\,\widetilde{s})$. Si ζ est l'isomorphisme défini plus haut de $X^{\mathbf{Q}}(\widetilde{T})$ sur un sous-espace de $X^{\mathbf{Q}}(T)$, on vérifie facilement que $w \cdot \zeta(\widetilde{\chi}) = \zeta(\widetilde{w} \cdot \widetilde{\chi})$ pour tout $\widetilde{\chi} \in X^{\mathbf{Q}}(\widetilde{T})$. Ceci étant, si v est un vecteur $\neq 0$ de V tel que l'on ait $\widetilde{t} \cdot v = \widetilde{\chi}(\widetilde{t})\,v$ ($\widetilde{\chi}(\widetilde{t}) \in K$) pour tout $\widetilde{t} \in \widetilde{T}$, on aura $\widetilde{t} \cdot (\widetilde{s} \cdot v) = \widetilde{\chi}(\widetilde{s}^{-1}\,\widetilde{t}\,\widetilde{s})\,\widetilde{s} \cdot v$; la proposition 2 résulte immédiatement de là.

Revenons maintenant au cas où $\rho = \rho_{(e)}$. Soient $\alpha_1, \ldots, \alpha_\ell$ les racines fondamentales par rapport à B ; pour déterminer le poids fondamental χ_1, nous allons déterminer les éléments $\chi_1 - w_k \cdot \chi_1$, où w_k est la réflexion par rapport à α_k. Pour montrer que la connaissance de ces éléments suffit à déterminer χ_1, il suffit de montrer qu'il n'y a aucun élément $\chi \neq 0$ de $X^Q(T)$ qui soit invariant par les w_k. Or, les points fixes de w_k sont les éléments de

l'hyperplan H_k de $X^{\mathbf{Q}}(T)$ orthogonal de α_k relativement à une forme quadratique définie positive invariante par W. L'intersection des H_k est réduite à 0 puisque $\alpha_1, \ldots, \alpha_\ell$ forment une base de $X^{\mathbf{Q}}(T)$ (n° 13.3, théorème 2).

Pour déterminer les $\chi_1 - w_k \cdot \chi_1$, nous avons à déterminer les fonctions de V dont les diviseurs sont les $\sigma_k \cdot D_{(e)} - D_{(e)}$, σ_k étant une opération du normalisateur de T qui définit la réflexion par rapport à la racine α_k, opération que nous pouvons prendre dans le centralisateur Z_k de la composante neutre du noyau de α_k. Nous avons pour cela à déterminer les hypersurfaces $\sigma_k \cdot \Delta_{k'}$ $(1 \leq k,\, k' \leq \ell)$, les $\Delta_{k'}$ étant les hypersurfaces définies avant la proposition 2 du n° 15.2.

Désignons par P_α le groupe $\tau_\alpha(K)$. Soit C_k le groupe engendré par les P_α pour les racines α qui sont négatives sur la chambre associée à B et qui sont $\neq \alpha_k$; c'est un sous-groupe invariant de B^u, et, si l'on pose $P_k = P_{\alpha_k}$, on a $B^u = C_k\, P_k$ et $Z_{\mathbf{Q}}$ normalise C_k (propositions 4 du n° 13.2 et 6 du n° 13.3) ; il en résulte $\sigma_k\, C_k\, \sigma_k^{-1} = C_k$. Par ailleurs, l'ensemble $Z_k\, x_0$ est une courbe complète qui contient deux points invariants par les opérations de T, à savoir x_0 et $\sigma_k \cdot x_0 = x_k$ (*cf.* lemme 1, n° 12.1) et $P_k\, x_0$ contient tous les points $\neq x_k$ de cette courbe. Comme σ_k appartient à Z_k, on en conclut que σ_k permute entre eux tous les points $\neq x_0$ de $P_k\, x_0$. On a $\sigma_k(C_k\, x_0) = C_k\, x_k \subset \Delta_k$; on on conclut que l'ensemble des points $x \in \Omega_0$ tels que $\sigma_k \cdot x$ n'appartienne pas à Ω_0 est $C_k\, x_0$, et que cet ensemble est transformé par σ_k en une partie de Δ_k, d'ailleurs dense puisque $C_k\, x_0$ est une sous-variété de codimension 1 de Ω_0. Comme il n'existe aucun point de Ω_0 dont l'image par σ_k soit un point de $\Omega - \Omega_0$ n'appartenant pas à Δ_k, on voit que, si $k' \neq k$, $\sigma_k^{-1}(\Delta_{k'})$ est contenu dans $\Omega - \Omega_0$, donc est de la forme $\Delta_{k''}$; par ailleurs, le diviseur $\sigma_k^{-1}(\Delta_{k'}) - \Delta_{k'} = \Delta_{k''} - \Delta_{k'}$ est principal ; il en résulte que l'on a

$$\sigma_k(\Delta_{k'}) = \Delta_{k'} \quad \text{si} \quad k' \neq k\,. \tag{1}$$

Par ailleurs, si on pose $u_k = u_{\alpha_k}$, il est clair que $C_k\, x_0$ est l'ensemble des points $x \in \Omega_0$ tels que $u_k(x) = 0$; si on désigne par Δ'_k l'adhérence de $C_k\, x_0$ dans G/B, le diviseur de u_k est de la forme $\Delta'_k - D$, où D est un diviseur tel que $\operatorname{Supp} D \subset \Omega - \Omega_0$, donc une combinaison linéaire de $\Delta_1, \ldots, \Delta_\ell$. Ce diviseur est linéairement équivalent à Δ'_k, donc à $\sigma_k(\Delta'_k) = \Delta_k$; il est donc égal à Δ_k (n° 15.2, propositions 2 et 4), d'où

$$(u_k) = \Delta'_k - \Delta_k = \sigma_k \cdot \Delta_k - \Delta_k\,. \tag{2}$$

Ceci étant, si $(e) = (e_1, \ldots, e_k)$, les formules (1) et (2) entraînent

$$\sigma_k \cdot D_{(e)} - D_{(e)} = e_k(u_k) = (u_k^{e_k})\,. \tag{3}$$

Comme $u_k^t = (\alpha_k(t))^{-1}\, u_k$, on en conclut que

$$\chi_1 - w_k \cdot \chi_1 = e_k\, \alpha_k\,. \tag{4}$$

Cette formule établit d'abord le résultat suivant :

Proposition 3. – *Soient* (e) *et* (e') *des suites distinctes de* ℓ *entiers* ≥ 0. *Si* $(e) \neq (e')$, *les représentations projectives* $\rho_{(e)}$, $\rho_{(e')}$ *sont inéquivalentes.*

Ces représentations n'ont en effet pas le même poids dominant.

16.3 Le groupe des poids

Si maintenant λ est une représentation linéaire (non plus projective) rationnelle de G, d'espace V, celui-ci admet une base composée de vecteurs v_i tels que $\lambda(t)\, v_i = \chi_i(t)\, v_i$, pour $t \in T$, les χ_i étant des éléments de $X(T)$; ces éléments sont appelés les *poids* de la représentation linéaire λ.

Proposition 4. – *Les poids de toute représentation linéaire rationnelle de* G *sont aussi des poids de représentations projectives simples de* G.

Soit λ une représentation linéaire rationnelle de G, d'espace V ; soit $(V_0, V_1, \ldots, V_h)$ une suite de Jordan-Hölder de V, considéré comme module sur K et sur G. Les V_i/V_{i-1} sont les espaces de représentations simples λ_i de G. Comme toute représentation de T est semi-simple, il y a, pour $1 \leq i \leq h$, un sous-espace W_i de V_i stable par les opérations de $\lambda(T)$ et tel que V_i soit somme directe de V_{i-1} et de W_i. Il en résulte que tout poids de λ est aussi un poids de l'une des λ_i ; il suffira donc d'établir la proposition 4 dans le cas d'une représentation simple λ. On déduit alors de λ une représentation projective simple ρ de G, opérant sur l'espace projectif associé à V ; il suffira, pour établir la proposition 4, de prouver que $\lambda(G)$ est le groupe linéaire associé à la représentation projective ρ ; tout revient donc à établir que l'on a $\lambda(G) \subset \mathrm{SL}(V)$; c'est ce qui résultera du

Lemme 1. – *Le groupe* G *est son propre groupe des commutateurs.*

Soit G' le groupe des commutateurs de G. Si α est une racine, la formule $t\, \tau_\alpha(\xi)\, t^{-1} = \tau_\alpha(\alpha(t)\, \xi)$ $(t \in T,\ \xi \in K)$ montre que $\tau_\alpha(\xi) \in G'$ (car $\alpha \neq 1$). Par ailleurs, si σ est un élément du groupe de Weyl, $\sigma\, t\, \sigma^{-1}\, t^{-1}$ appartient à G' si $t \in T$. Soit T' le sous-groupe de T engendré par les éléments de cette forme (pour tous les $t \in T$ et tous les éléments σ du normalisateur de T). Ce groupe est manifestement fermé et connexe (n° 3.3, théorème 2) ; si χ est un caractère rationnel de T qui est égal à 1 sur T', il est clair que χ est invariant par les opérations du groupe de Weyl ; nous avons déjà vu qu'il en résulte que $\chi = 1$. On a donc $T' = T$, d'où $T \subset G'$, et par suite $B \subset G'$. Comme tout élément de G est conjugué à un élément de B, on a $G = G'$, ce qui démontre le lemme 1 et la proposition 4.

On démontrera plus loin un résultat beaucoup plus précis que le lemme 1 : si H est un sous-groupe invariant fermé quelconque de G, G/H est semi-simple.

Nous désignerons par Π le sous-groupe de $X^{\mathbf{Q}}(T)$ engendré par les poids de toutes les représentations projectives simples de G ; ce groupe s'appelle

le *groupe des poids*. On appelle *représentations projectives fondamentales* les représentations projectives simples $\rho_1, \ldots, \rho_\ell$ déterminées par les systèmes suivants d'entiers e_k :

$$(1, 0, \ldots, 0)\,,\ (0, 1, \ldots, 0), \ldots, (0, 0, \ldots, 1)\,.$$

Les poids dominants de ces représentations sont appelés les *poids dominants fondamentaux* (ou simplement "poids fondamentaux") ; nous les noterons $\varpi_1, \ldots, \varpi_\ell$. Il résulte de la formule établie plus haut que l'on a $\varpi_k - w_k \cdot \varpi_k = \alpha_k$; ceci démontre[2] que le groupe des poids contient comme sous-groupe le groupe Π_0 engendré par les racines, que nous appellerons *groupe des racines*. Le poids dominant de la représentation $\rho_{(e)}$, où $(e) = (e_1, \ldots, e_\ell)$, est évidemment $\sum_{k=1}^{\ell} e_k\, \varpi_k$. Tenant compte de la proposition 1, on en déduit que Π est engendré par $\varpi_1, \ldots, \varpi_\ell$ et par les racines. Comme le groupe G lui-même est isomorphe à un groupe linéaire, il résulte de la proposition 4 que l'on a

$$\Pi_0 \subset X(T) \subset \Pi\,.$$

Nous démontrerons un peu plus loin (corollaire 3 de la proposition 5) que le groupe des poids est déjà engendré par les poids dominants fondamentaux. On peut voir dès maintenant qu'il en est bien ainsi dans le cas où $\ell = 1$: en effet, si α est la racine fondamentale, le poids dominant fondamental est $\alpha/2$, en vertu de la formule

$$\alpha/2 - (-\alpha/2) = \alpha\,.$$

16.4 Les sous-groupes semi-simples de rang 1 de G

Soit α une racine ; désignons par Q_α la composante neutre dans le noyau de α et par Z_α le centralisateur de Q_α ; on sait que Z_α/Q_α est un groupe semi-simple de rang 1 et de dimension 3. Nous allons maintenant montrer que le groupe dérivé Z'_α de Z_α est semi-simple de rang 1 et de dimension 3. Nous démontrerons d'abord que $Z'_\alpha \cap Q_\alpha$ est fini ; cela résultera du

Lemme 2. – *Soient Z un groupe linéaire algébrique connexe et Z' son groupe dérivé ; le centre de Z ne contient aucun tore de dimension > 0 contenu dans Z'.*

Soit T' un tore contenu dans le centre de Z et dans Z'. Soit V l'espace vectoriel sur lequel opère Z ; soit $(V_0, \ldots, V_h)$ une suite de Jordan-Hölder de V, considéré comme espace vectoriel à opérateurs admettant Z comme

[2] En effet, Π est invariant par W d'après la proposition 2 ; il contient donc les α_k d'après la formule précédente, et toute racine est transformée d'une racine fondamentale par un élément de W (n° 13.3, proposition 5, a)).

ensemble d'opérateurs ; chaque V_i/V_{i-1} est donc l'espace d'une représentation simple ρ_i de Z. Les éléments de l'intersection N des noyaux des ρ_i sont unipotents, de sorte que $N \cap T' = \{e\}$ (l'élément neutre). Par ailleurs, si $t' \in T'$, $\rho_i(t')$ est une homothétie, de rapport disons c_i ; de plus, comme $t' \in Z'$, on a $\det \rho_i(t') = 1$, d'où $c_i^{d_i} = 1$ si $d_i = \dim V_i/V_{i-1}$; le groupe $T'/(N \cap T') = T'$ est donc bien fini.

Le groupe P_α est contenu dans Z_α, donc dans Z'_α en vertu de la formule $t\,\tau_\alpha(\xi)\,t^{-1} = \tau_\alpha(\alpha(t)\,\xi)$ $(t \in T,\ \xi \in K)$. Si $t \in T$, on peut écrire $t^2 = (t(t^\sigma)^{-1})(tt^\sigma)$, où l'on désigne par σ un élément de Z_α appartenant au normalisateur de T sans appartenir à T, et par t^σ l'élément $\sigma\, t\, \sigma^{-1}$. L'élément $t(t^\sigma)^{-1}$ appartient à Z'_α ; tt^σ appartient à la composante neutre dans le groupe des éléments de T qui commutent à σ, donc à Q_α. Comme tout élément de T est le carré d'un élément de T, on voit que l'on a $T \subset Z'_\alpha\, Q_\alpha$. Le groupe $Z'_\alpha\, Q_\alpha/Q_\alpha$ contient $P_\alpha\, Q_\alpha/Q_\alpha$, $P_{-\alpha}\, Q_\alpha/Q_\alpha$ et T/Q_α ; c'est donc Z_α/Q_α tout entier, d'où $Z'_\alpha\, Q_\alpha = Z_\alpha$. L'homomorphisme canonique de Z_α sur Z_α/Q_α induit un épimorphisme de noyau fini de Z'_α ; il en résulte que Z'_α est de dimension 3. Si R est son radical, RQ_α/Q_α est dans le radical de Z_α/Q_α, donc se réduit à son élément neutre et l'on a donc $R \subset Q_\alpha \cap Z'_\alpha$; R est donc fini, et par suite réduit à son élément neutre, ce qui montre que Z'_α est semi-simple. Le groupe Z'_α contient un tore maximal T_α contenu dans T ; comme $P_\alpha \subset Z'_\alpha$, il est clair que les racines de Z'_α par rapport à T_α sont les restrictions de α et de α^{-1} à T_α. Le groupe $X(T_\alpha)$ contient le groupe engendré par α et est contenu dans le groupe engendré par $\alpha/2$, comme on l'a vu ci-dessus. Par ailleurs, ce groupe est en dualité avec le groupe $\Gamma(T_\alpha)$ des groupes à un paramètre de T_α ; on en conclut que $\Gamma(T_\alpha)$ contient un élément γ_α tel que $\langle \gamma_\alpha, \alpha \rangle = 2$; il est engendré par γ_α si $\alpha/2 \in X(T_\alpha)$, par $\gamma_\alpha/2$ dans le cas contraire. Il est clair que la réflexion par rapport à α transforme tout élément de $X(T_\alpha)$, donc aussi de $\Gamma(T_\alpha)$, en son opposé. Ceci établit la

Proposition 5. – *Pour toute racine α de G, il existe un élément*[3] *γ_α du groupe $\Gamma(T)$ des groupes à un paramètre de T qui possède les propriétés suivantes : on a $\alpha(\gamma_\alpha) = 2$ et la réflexion par rapport à la racine α transforme γ_α en $-\gamma_\alpha$.*

Si χ est un élément quelconque de $X^{\mathbf{Q}}(T)$, on a[4]

$$w_\alpha \cdot \chi = \chi - \langle \gamma_\alpha, \chi \rangle\, \alpha \ ; \tag{5}$$

comme $\langle \gamma_\alpha, \chi \rangle$ est entier pour tout $\chi \in X(T)$, on obtient le

Corollaire 1. – *Si w_α est la réflexion par rapport à α, et χ un élément quelconque de $X(T)$, $w_\alpha \cdot \chi - \chi$ est un multiple entier de α.*

[3] Dans la terminologie actuelle (2003), γ_α s'appelle la *coracine* associée à la racine α.

[4] D'où aussi $w_\alpha \cdot \gamma = \gamma - \langle \gamma, \alpha \rangle\, \gamma_\alpha$ pour toute racine α et tout γ dans $\Gamma^{\mathbf{Q}}(T)$.

En particulier, pour toute racine β, $w_\alpha \cdot \beta - \beta$ est un multiple entier de α. Rappelons que l'on désigne par $w_1, \ldots, w_\ell$ les réflexions par rapport aux racines fondamentales $\alpha_1, \ldots, \alpha_\ell$; on a

$$w_k \cdot \alpha_{k'} = \alpha_{k'} + c(k, k')\, \alpha_k \tag{6}$$

où les $c(k, k')$ sont des entiers, qu'on appelle *les entiers de Cartan* ; en posant $\gamma_k = \gamma_{\alpha_k}$, on a $c(k, k') = -\langle \gamma_k, \alpha_{k'} \rangle$, $c(k, k) = -2$, et $c(k, k') \geq 0$ si $k' \neq k$ (car toute racine α est combinaison linéaire à coefficients tous de même signe[5] des α_k). Comme le groupe de Weyl est engendré par les w_k, on voit que ses opérations transforment en lui-même le groupe additif engendré par $\alpha_1, \ldots, \alpha_\ell$; comme toute racine est la transformée de l'une des racines fondamentales par une opération du groupe de Weyl (n° 13.3, proposition 5, a)), on a le

Corollaire 2. – *Les racines fondamentales constituent une base du groupe Π_0 des racines.*

Posons $\gamma_k = \gamma_{\alpha_k}$; comme on a

$$w_k \cdot \varpi_{k'} = \varpi_{k'} - \delta_{k,k'}\, \alpha_k \tag{7}$$

on a

$$\langle \gamma_{k'}, \varpi_k \rangle = \delta_{k,k'}\,. \tag{8}$$

Les poids dominants fondamentaux forment donc une base du groupe des éléments $\chi \in X^Q(T)$ tels que les nombres rationnels $\langle \gamma_k, \chi \rangle$ soient entiers. Or ce groupe contient $X(T)$ donc aussi les racines ; comme le groupe des poids est engendré par les ϖ_k et par les racines, on obtient le

Corollaire 3. – *Les poids dominants fondamentaux forment une base du groupe Π des poids.*

Remarque. Des formules (6) et (8) on déduit facilement la relation

$$\alpha_k = -\sum_{k'=1}^{\ell} c(k', k)\, \varpi_{k'}\,. \tag{9}$$

On sait que $(\alpha_1, \ldots, \alpha_\ell)$ est une base de Π_0 sur $\mathbf{Z}$ et de $X^{\mathbf{Q}}(T)$ sur $\mathbf{Q}$. Il en résulte que Π_0 est d'indice fini dans le groupe Π de base $(\varpi_1, \ldots, \varpi_\ell)$ sur $\mathbf{Z}$ et l'on a

$$(\Pi : \Pi_0) = |\det(c(k, k'))|\,.$$

On peut aussi montrer que le centre Z de G est dual du groupe commutatif fini $X(T)/\Pi_0$.

[5] Cela peut se prouver ainsi : $(\alpha_1, \ldots, \alpha_\ell)$ est une base sur $\mathbf{Q}$ du dual $X^{\mathbf{Q}}(T)$ de $\Gamma^{\mathbf{Q}}(T)$, la chambre $\mathcal{C}(B)$ de $\Gamma^{\mathbf{Q}}(T)$ associée à B est définie par les inégalités $\langle \gamma, \alpha_k \rangle > 0$ pour $1 \leq k \leq \ell$, et le signe de $\langle \gamma, \alpha \rangle$ reste constant pour γ dans $\mathcal{C}(B)$.

17. Les sous-groupes radiciels[1]

17.1 Notations

Nous désignerons par G un groupe algébrique semi-simple, par T un tore maximal de G, par R l'ensemble des racines de G par rapport à T ; pour tout $\alpha \in R$, nous désignerons par τ_α un isomorphisme de K sur un sous-groupe de G tel que l'on ait

$$t\,\tau_\alpha(\xi)t^{-1} = \tau_\alpha(\alpha(t)\xi) \qquad (t \in T\,,\ \xi \in K)\ ;$$

nous poserons $P_\alpha = \tau_\alpha(K)$.

Nous désignerons par Q_α la composante neutre dans le noyau de α, par Z_α le centralisateur de Q_α, par Z'_α le groupe dérivé de Z_α, par T_α le tore maximal[2] de Z'_α contenu dans T ; nous désignerons par w_α la réflexion par rapport à la racine α, et par σ_α un élément du normalisateur de T_α dans Z'_α n'appartenant pas à T_α ; σ_α appartient donc au normalisateur de T et sa classe suivant T est w_α.

Pour tout tore T', nous désignerons par $\Gamma(T')$ le groupe des groupes à un paramètre de T' et par $X(T')$ le groupe des caractères rationnels de T' ; nous poserons $\Gamma^{\mathbf{Q}}(T') = \mathbf{Q} \otimes \Gamma(T')$, $X^{\mathbf{Q}}(T') = \mathbf{Q} \otimes X(T')$; on rappelle que les tores contenus dans T' sont en correspondance biunivoque avec les sous-espaces de l'espace vectoriel $X^{\mathbf{Q}}(T')$, le tore qui correspond à un sous-espace Y de $X^{\mathbf{Q}}(T')$ étant l'ensemble des éléments t tels que $\chi(t) = 1$ pour tout $\chi \in Y \cap X(T')$. Les espaces vectoriels $\Gamma^{\mathbf{Q}}(T')$ et $X^{\mathbf{Q}}(T')$ sont en dualité l'un avec l'autre ; il y a une correspondance biunivoque entre les sous-espaces Z de $\Gamma^{\mathbf{Q}}(T')$ et les sous-tores de T' ; si T'' est le tore associé à Z, on a $\Gamma(T'') = Z \cap \Gamma(T')$. Le groupe $\Gamma(T_\alpha)$ contient un élément γ_α tel que $\langle \gamma_\alpha, \alpha \rangle = 2$, $w_\alpha(\gamma_\alpha) = -\gamma_\alpha$.

17.2 Sous-groupe radiciel associé à un ensemble fermé de racines

Nous dirons qu'un ensemble S de racines est *fermé*[3] si toute combinaison linéaire à coefficients entiers de racines de S qui est une racine appartient à S.

---

[1] Exposé de C. Chevalley, le 6.5.1957

[2] On a $T_\alpha = T \cap Z'_\alpha = \operatorname{Supp} \gamma_\alpha$.

[3] Bourbaki dit "clos et symétrique".

Nous désignerons par S un ensemble fermé de racines et par H le groupe engendré par les Z'_α pour tous les $\alpha \in S$. Les Z'_α étant des groupes connexes, il en est de même de H d'après le théorème 2 du n° 3.3. Nous nous proposons de démontrer le théorème suivant :

Théorème 1. – *Le groupe H est semi-simple ; le groupe $T_H = T \cap H$ est un tore maximal de H ; les racines de H par rapport à T_H sont les restrictions à T_H des éléments de S ; il existe un groupe de Borel B de G contenant T tel que $B_H = B \cap H$ soit un groupe de Borel de H ; B_H est engendré par les P_α pour celles des racines $\alpha \in S$ qui sont négatives sur la chambre de Weyl associée à B.*

Nous aurons besoin au cours de la démonstration d'un résultat relatif aux formules de multiplication dans la partie unipotente B^u d'un groupe de Borel B de G contenant T. Désignons par R_- l'ensemble des racines α qui sont négatives sur la chambre associée à B ; nous supposerons l'ensemble R_- ordonné d'une manière quelconque. On sait que l'algèbre $K[B^u]$ des fonctions régulières sur B^u est engendrée par des fonctions v_α ($\alpha \in R_-$) telles que l'on ait

$$s = \prod_{\alpha \in R_-} \tau_\alpha(v_\alpha(s)) \qquad (s \in B^u)\,.$$

Il en résulte que l'on a

$$v_\alpha(ss'^{-1}) = P_\alpha(\ldots, v_\beta(s), \ldots, v_{\beta'}(s'), \ldots)\,,$$

les $P_\alpha(\ldots, X_\beta, \ldots, Y_{\beta'}, \ldots)$ étant des polynômes à coefficients dans K en $2n$ arguments X_β, $Y_{\beta'}$, (si n est le nombre d'éléments de R_-).

Lemme 1. – *Le polynôme $P_\alpha(\ldots, X_\beta, \ldots, Y_{\beta'}, \ldots)$ est combinaison linéaire des monômes $\prod_{\beta \in R_-} X_\beta^{i(\beta)}\, Y_\beta^{j(\beta)}$ pour lesquels on a $\sum_{\beta \in R_-} (i(\beta) + j(\beta))\,\beta = \alpha$.*

On a évidemment, pour tout élément $t \in T$, $v_\alpha(tst^{-1}) = \alpha(t)\, v_\alpha(s)$; tenant compte de ce que $t(ss'^{-1})t^{-1} = tst^{-1}(ts't^{-1})^{-1}$, il vient

$$P_\alpha(\ldots, \beta(t)X_\beta, \ldots, \beta'(t)Y_{\beta'}, \ldots) = \alpha(t)P_\alpha(\ldots, X_\beta, \ldots, Y_{\beta'}, \ldots)\,.$$

Si donc on désigne par c le coefficient du monôme $\prod_{\beta \in R_-} X_\beta^{i(\beta)}\, Y_\beta^{j(\beta)}$ dans P_α, il vient

$$c \prod_{\beta \in R} (\beta(t))^{i(\beta)}\, (\beta(t))^{j(\beta)} = c\,\alpha(t)\ ;$$

il en résulte bien que l'on a $c = 0$ si α n'est pas égal à $\sum_{\beta \in R_-} (i(\beta) + j(\beta))\,\beta$ (en notation additive), ce qui démontre le lemme 1.

Corollaire. – *Soit A une partie de R_- qui possède la propriété suivante : si $\beta_1, \ldots, \beta_s$ sont des éléments de A tels que $\alpha = \beta_1 + \cdots + \beta_s$ soit un racine,*

alors, on a $\beta \in A$. L'ensemble B' des éléments de la forme $\prod_{\alpha\in A} s_\alpha$, où $s_\alpha \in P_\alpha$ pour tout $\alpha \in A$, et où A est muni de la structure d'ordre induite par celle de R_-, est un sous-groupe de B^u.

Les éléments s de B' sont caractérisés par la condition que l'on ait $v_\alpha(s) = 0$ pour tout $\alpha \notin A$. Ceci étant, si α est une racine de R_- n'appartenant pas à A et si on met α sous la forme $\sum_{\beta\in R_-} (i(\beta) + j(\beta))\,\beta$, il y a ou bien une racine $\beta \notin A$ telle que $i(\beta) > 0$ ou bien $j(\beta) > 0$; dans les deux cas on a $\prod_{\beta\in R_-} (v_\beta(s))^{i(\beta)}(v_\beta(s'))^{j(\beta)} = 0$ si s, s' sont dans B', ce qui démontre le corollaire.

Lemme 2. *Soient $\alpha_1, \ldots, \alpha_r$ des racines linéairement indépendantes ; la composante neutre T' dans $Q_{\alpha_1} \cap \ldots \cap Q_{\alpha_r}$ est un tore de codimension r dans T ; le groupe T'' engendré par $T_{\alpha_1}, \ldots, T_{\alpha_r}$ est un tore de dimension r ; $T' \cap T''$ est fini, et on a $T = T'\,T''$.*

Le groupe T' est la composante neutre dans l'intersection des noyaux de $\alpha_1, \ldots, \alpha_r$; il en résulte que $\Gamma(T')$ est l'ensemble des $\gamma \in \Gamma(T)$ tels que $\langle\gamma, \alpha_i\rangle = 0$ $(1 \leq i \leq r)$; comme les α_i sont linéairement indépendantes, ces éléments engendrent un sous-espace de codimension r de $\Gamma^{\mathbf{Q}}(T)$, ce qui démontre la première assertion. Munissons $\Gamma^{\mathbf{Q}}(T)$ d'une forme quadratique définie positive invariante par les opérations du groupe de Weyl ; $\Gamma^{\mathbf{Q}}(T_\alpha)$ est alors, pour toute racine α, la droite orthogonale à l'hyperplan de $\Gamma^{\mathbf{Q}}(T)$ d'équation $\alpha = 0$. L'espace vectoriel engendré par les $\Gamma^{\mathbf{Q}}(T_{\alpha_i})$ est donc le complémentaire orthogonal de l'intersection des hyperplans $\alpha_i = 0$ et est par suite de dimension r puisque $\alpha_1, \ldots, \alpha_r$ sont linéairement indépendantes. Cet espace est contenu dans $\Gamma^{\mathbf{Q}}(T'')$; par ailleurs il est de la forme $\Gamma^{\mathbf{Q}}(T_0'')$, où T_0'' est un tore qui, contenant chacun des T_{α_i}, contient T'' ; on en conclut que $T'' = T_0''$, donc que T'' est de dimension r. Les éléments de $\Gamma(T')$ sont dans tous les hyperplans $\alpha_i = 0$, donc orthogonaux aux éléments de $\Gamma(T'')$; on en conclut que $\Gamma(T') \cap \Gamma(T'') = \{0\}$, donc que $T' \cap T''$ est fini ; l'homomorphisme canonique de $T'\,T''$ sur $T'\,T''/T'$ induit un homomorphisme de noyau fini de T'', d'où $\dim T'\,T''/T' \geq \dim T'' = r$ et par suite $\dim T'\,T'' \geq r + \dim T' = \dim T$, d'où $T'\,T'' = T$. Ceci démontre le lemme 2.

Ceci dit, nous allons aborder la démonstration du théorème 1.

Si α est une racine de S, w_α transforme une racine β en $\beta - \langle\gamma_\alpha, \beta\rangle\,\alpha$, et $\beta(\gamma_\alpha)$ est entier ; il en résulte que w_α transforme en lui-même le sous-groupe de $X(T)$ engendré par S, donc aussi l'ensemble S et le sous-espace Y de $X^{\mathbf{Q}}(T)$ engendré par S. Appliquant les résultats de la proposition 1 du n° 14.3 aux éléments de S et à l'espace vectoriel déduit de Y par extension du corps de base au corps des nombres réels, on voit que, si $r = \dim Y$, il y a r éléments linéairement indépendants $\alpha_1, \ldots, \alpha_r$ de S tels que *tout élément de S puisse se mettre sous forme de combinaison linéaire à coefficients tous*

≥ 0 *ou tous* ≤ 0 *de* $\alpha_1, \ldots, \alpha_r$; ces coefficients sont rationnels, car $\alpha_1, \ldots, \alpha_r$ forment une base de Y sur $\mathbf{Q}$. Nous poserons $w_i = w_{\alpha_i}$, $P_i = P_{\alpha_i}$, $Q_i = Q_{\alpha_i}$, $Z'_i = Z'_{\alpha_i}$, $T_i = T_{\alpha_i}$, $\sigma_i = \sigma_{\alpha_i}$. Tout élément α de S est le transformé de l'un des α_i par une opération w du groupe engendré par $w_1, \ldots, w_r$ (corollaire à la proposition 3, n° 14.4) ; comme on a $w_\alpha = w w_i w^{-1}$ si $\alpha = w \cdot \alpha_i$, on voit que le groupe W_H engendré par les w_α ($\alpha \in S$) est déjà engendré par les w_i. De plus, les opérations de W_H transforment en lui-même le groupe engendré par $\alpha_1, \ldots, \alpha_r$ (car $w_i \cdot \alpha_j$ est de la forme $\alpha_j - k\,\alpha_i$ avec k entier, donc appartient à ce groupe si $1 \leq i, j \leq r$) et par suite *tout élément de* S *est combinaison linéaire à coefficients entiers des* α_i.

Soient T' la composante neutre dans $\bigcap_{i=1}^{r} Q_i$ et $T_H = T_1 \ldots T_r$. Il résulte du lemme 2 que l'on a $T_H T' = T$ et que $T_H \cap T'$ est fini. Les éléments de T' commutent avec ceux de H ; en effet, si $\alpha \in S$, α est combinaison linéaire à coefficients entiers des α_i, d'où $\alpha(T') = \{1\}$; ceci montre que T' commute avec les éléments de P_α et de $P_{-\alpha}$; il commute évidemment avec ceux de T_α ; comme l'ensemble $P_\alpha\, T_\alpha\, P_{-\alpha}$ est ouvert dans Z'_α, c'en est un ensemble de générateurs, ce qui montre que T' commute avec les éléments de Z'_α ; ceci étant vrai pour tout α dans S, on a prouvé que T' commute avec les éléments de H. Comme chaque Z'_α est son propre groupe dérivé, H est son propre groupe dérivé ; il résulte alors du lemme 2 du n° 16.4 que $H \cap T'$ est fini. Le tore T_H est contenu dans H ; il est donc contenu dans un tore maximal $\overline{T}_H$ de H ; comme les éléments de T' commutent avec ceux de $\overline{T}_H$, $\overline{T}_H\, T'$ est un tore qui, contenant $T_H T' = T$, lui est identique. Comme $\overline{T}_H \cap T'$ est fini, il en résulte que $\overline{T}_H / T_H$ est fini, d'où $\overline{T}_H = T_H$; donc T_H est un tore maximal de H. Le groupe $H \cap T$ est un sous-groupe commutatif de H qui contient T_H et dont les éléments sont semi-simples ; il en résulte que $H \cap T = T_H$ (car le centralisateur de T_H dans H est le produit direct de T_H par un groupe unipotent[4]) ; on a en particulier $T_\alpha \subset T_H$ pour toute racine $\alpha \in S$. De plus, si $\alpha \in S$, l'élément σ_α, qui est dans H et dans le normalisateur de T, est dans le normalisateur de T_H. Nous désignerons par N_H le groupe engendré par T_H et par les σ_i ($1 \leq i \leq r$) ; N_H / T_H est donc isomorphe au groupe W_H ; pour tout élément w de W_H, nous choisirons un élément σ_w de N_H qui produise l'opération w du groupe de Weyl de G.

Il existe au moins un élément γ de $\Gamma^{\mathbf{Q}}(T)$ tel que l'on ait $\langle \gamma, \alpha_i \rangle < 0$ ($1 \leq i \leq r$), puisque $\alpha_1, \ldots, \alpha_r$ sont linéairement indépendants. Choisissons d'autre part un élément γ_1 appartenant à une chambre de l'espace $\Gamma^{\mathbf{Q}}(T)$; on peut alors trouver un nombre rationnel a tel que l'on ait $\langle \gamma + a\gamma_1, \rho \rangle \neq 0$ pour toute racine ρ de G et de plus $\langle \gamma + a\gamma_1, \alpha_i \rangle < 0$ ($1 \leq i \leq r$) ; l'élément $\gamma' = \gamma + a\,\gamma_1$ appartient alors à une chambre de l'espace $\Gamma^{\mathbf{Q}}(T)$ sur laquelle $\alpha_1, \ldots, \alpha_r$ sont négatives ; soit B le groupe de Borel qui correspond à cette chambre. Nous désignerons par R_- l'ensemble des racines de G qui sont négatives sur la chambre associée à B, ensemble que nous supposerons

[4] Cela résulte du théorème 1 du n° 7.1 et du théorème 2 du n° 6.3.

ordonné d'une manière quelconque, et par S_- l'ensemble $S \cap R_-$; S_- se compose des éléments de S qui sont des combinaisons linéaires à coefficients ≤ 0 de $\alpha_1, \ldots, \alpha_r$. Si une combinaison linéaire à coefficients entiers > 0 d'éléments de S_- est une racine, cette racine est dans S_-. Nous désignerons par B_H^u le sous-groupe de B engendré par les P_α pour $\alpha \in S_-$; ce sous-groupe se compose des éléments de la forme $\prod_{\alpha \in S_-} s_\alpha$, avec $s_\alpha \in P_\alpha$ pour tout $\alpha \in S_-$, d'après le corollaire du lemme 1 appliqué à $A = S_-$; nous poserons $B_H = B_H^u \, T_H$. Nous nous proposons de démontrer le :

Lemme 3. – *Le groupe H est la réunion des ensembles $B_H \, \sigma_w \, B_H$ pour tous les $w \in W_H$.*

Observons d'abord que H est identique au groupe H' engendré par les Z'_i $(1 \leq i \leq r)$. En effet, le groupe H' contient T_H et les éléments σ_i $(1 \leq i \leq r)$, donc N_H. Si α est un élément quelconque de S, il y a une opération $w \in W_H$ et un indice i $(1 \leq i \leq r)$ tels que $w \cdot \alpha_i = \alpha$, d'où $\sigma_w \, Z'_i \, \sigma_w^{-1} = Z'_\alpha$; comme $\sigma_w \in H'$, on a $Z'_\alpha \subset H'$, ce qui démontre notre assertion. Désignant par E la réunion des $B_H \, \sigma_w \, B_H$, il suffira donc de montrer que $Z'_i \, E \subset E$ $(1 \leq i \leq r)$. Soit $S_-^{(i)}$ l'ensemble des éléments $\neq \alpha_i$ de S_-. Soit C_i le groupe engendré par les P_α pour $\alpha \in S_-^{(i)}$; on a $B_H^u = C_i \, P_i$. Comme C_i est un sous-groupe fermé de codimension ≤ 1 dans B_H^u, c'est un sous-groupe invariant de B_H^u. Par ailleurs, si $\alpha \in S_-^{(i)}$, $w_i \cdot \alpha$ est de la forme $\alpha + k \, \alpha_i$; comme α n'est pas multiple de α_i, il y a au moins un indice $j \neq i$ tel que le coefficient de α_j dans l'expression de α comme combinaison linéaire de $\alpha_1, \ldots, \alpha_r$ soit > 0 ; il en résulte que le coefficient de α_j dans l'expression de $w_i \cdot \alpha$ est > 0, donc que $w_i \cdot \alpha \in S_-^{(i)}$; comme on a $\sigma_i \, P_\alpha \, \sigma_i^{-1} = P_{w_i \cdot \alpha}$, on en conclut que σ_i appartient au normalisateur de C_i. Ce normalisateur contient donc $P_i \, T_i \, \sigma_i \, P_i$, qui est dense dans Z'_i ; il en résulte que Z'_i est contenu dans le normalisateur de C_i. On a donc $Z'_i \, B_H \, \sigma_w \, B_H = C_i \, Z'_i \, P_i \, T_H \, \sigma_w \, B_H = C_i \, Z'_i \, \sigma_w \, T_H \, B_H$ puisque $P_i \subset Z'_i$ et que σ_w appartient au normalisateur de T_H. Supposons d'abord que $w^{-1} \cdot \alpha_i \in S$; dans ce cas, observons que Z'_i est la réunion de $P_i \, T_i$ et de $P_i \, \sigma_i \, P_i$, et que $P_i \, \sigma_w = \sigma_w \, P_{w^{-1} \cdot \alpha_i}$ est contenu dans $\sigma_w \, B_H$. Comme $C_i \, P_i \, T_i \subset B_H$, on a dans ce cas $Z'_i \, B_H \, \sigma_w \, B_H \subset E$. Dans le cas où $w^{-1} \cdot \alpha_i$ n'appartient pas à S, posons $w' = w_i \, w$, d'où $w'^{-1} \cdot \alpha_i = -w^{-1} \cdot \alpha_i \in S$; comme $Z'_i = Z'_i \, \sigma_i$, on a $Z'_i \, \sigma_w = Z'_i \, \sigma_i \, \sigma_w$ qui est contenu dans $Z'_i \, \sigma_{w'} \, T_H$ puisque $\sigma_i \, \sigma_w \equiv \sigma_{w'} \pmod{T_H}$. On est alors ramené au cas précédent, et on voit que, dans tous les cas, on a $Z'_i \, B_H \, \sigma_w \, B_H \subset E$, ce qui montre bien que l'on a $E = H$.

Lemme 4. – *B_H est un groupe de Borel de H.*

Comme c'est un sous-groupe résoluble connexe de H, il est en tout cas contenu dans un groupe de Borel $\overline{B}_H$ de B_H. La formule $H = \bigcup_{w \in W_H} B_H \, \sigma_w \, B_H$ montre alors que, pour établir l'égalité $\overline{B}_H = B_H$, il suffit de prouver que

$\sigma_w \notin \overline{B}_H$ si w est une opération distincte de l'identité de W_H. Or on sait qu'il existe au moins une racine $\alpha \in S_-$ telle que $w \cdot \alpha \notin S_-$ (proposition 6 du n° 14.6) ; on a alors $w \cdot \alpha = -\beta$ où β est une racine de S_-. Le groupe engendré par B_H et σ_w contient donc P_β, T_β et $P_{-\beta}$, ce qui montre qu'il contient le groupe non résoluble Z'_β, et établit le lemme 4.

Comme $B \cap H$ est un sous-groupe résoluble de H contenant B_H, on a $B \cap H = B_H$. Si M est le radical de H, M est contenu dans B_H et $M \cap B_H^u$ est engendré par ceux des P_α qu'il contient (car ce sous-groupe est transformé en lui-même par les opérations de T ; *cf.* proposition 1 du n° 13.1). Or, pour toute racine $\alpha \in S_-$, $M \cap Z'_\alpha$ est un sous-groupe résoluble invariant de Z'_α, donc fini, ce qui montre que l'on a $P_\alpha \not\subset M$ et que $M \cap B_H^u = \{e\}$. Le groupe algébrique connexe M ne contient donc aucun élément unipotent $\neq e$, ce qui montre que ses éléments sont semi-simples et que c'est un tore ; étant invariant dans H, il appartient au centre de H ; mais, comme H est son propre groupe dérivé, son centre ne contient aucun tore de dimension > 0 (lemme 2 du n° 16.4) ; M est donc fini, d'où $M = \{e\}$, ce qui montre que H *est semi-simple*.

On a $\tau_\alpha(K) = P_\alpha \subset H$ pour tout $\alpha \in S$, ce qui montre que les restrictions à T_H des racines de S sont des racines de H ; comme la dimension du groupe de Borel B_H de H est égale au nombre d'éléments de S_-, donc à la moitié du nombre d'éléments de S, il en résulte que les restrictions à T_H des racines de S sont toutes les racines de H. Le théorème 1 est établi.

Remarque. – Pour toute racine $\alpha \in S$, désignons par $\overline{\alpha}$ la restriction de α à T_H ; il est clair que la réflexion $w_{\overline{\alpha}}$ par rapport à $\overline{\alpha}$, considérée comme opérant dans $\Gamma(T_H)$, n'est autre que la restriction à $\Gamma(T_H)$ de l'opération w_α sur $\Gamma(T)$. Par ailleurs, l'inclusion $T_H \to T$ définit un homomorphisme $j : X(T) \to X(T_H)$ et il est clair que, si l'on considère w_α (resp. $w_{\overline{\alpha}}$) comme opérant dans $X(T)$ (resp. $X(T_H)$), le diagramme

$$\begin{array}{ccc} X(T) & \xrightarrow{j} & X(T_H) \\ {\scriptstyle w_\alpha}\downarrow & & \downarrow{\scriptstyle w_{\overline{\alpha}}} \\ X(T) & \xrightarrow{j} & X(T_H) \end{array}$$

est commutatif ; il en résulte que, si β est une autre racine de S et si $w_\alpha \cdot \beta = \beta + k\alpha$, on a $w_{\overline{\alpha}} \cdot \overline{\beta} = \overline{\beta} + k\overline{\alpha}$.

Les groupes définis à partir d'un ensemble fermé S de racines par le procédé indiqué ci-dessus s'appellent les *sous-groupes radiciels de* G.

17.3 Groupes quotients des groupes semi-simples

Nous nous proposons maintenant d'étudier les sous-groupes invariants connexes fermés de G, et notamment de prouver qu'ils sont radiciels (théorème 2). Etablissons d'abord la :

Proposition 1. – *Soient A le groupe des automorphismes de G et J le groupe des automorphismes intérieurs de G ; le groupe A/J est alors fini. Si B est un groupe de Borel contenant le tore maximal T, A/J est isomorphe à un groupe de permutations de l'ensemble des racines fondamentales par rapport à B.*

Un automorphisme u de G transforme B en un groupe de Borel, qui est conjugué à B dans G ; il existe donc un automorphisme $u_1 \in uJ$ tel que $u_1(B) = B$; u_1 transforme T en un tore maximal contenu dans B, qui est conjugué à T dans B ; il existe donc un automorphisme $u_2 \in u_1 J = uJ$ tel que $u_2(B) = B$, $u_2(T) = T$. Si A_0 est le groupe de tous les automorphismes de G qui conservent T et B, on a donc $A = A_0 J$. Si α est une racine, il en est évidemment de même de la fonction $\alpha' : t \to \alpha(u_2^{-1}(t))$; de plus, on a $u_2(P_\alpha) = P_{\alpha'}$. Si α est négative sur la chambre associée à B, on a $P_\alpha \subset B$, d'où $P_{\alpha'} \subset B$, et α' est négative sur la chambre associée à B ; l'application $\alpha \to \alpha'$ permute donc entre elles les racines fondamentales relatives à B. Soit A_1 le groupe des automorphismes de G qui conservent B et T et qui conservent toutes les racines relatives à T ; le groupe A_1 est d'indice fini dans A_0 et le groupe $A_1 J$ est donc d'indice fini dans $A_0 J = A$.

Nous allons maintenant montrer que $A_1 \subset J$. Soit à partir de maintenant u un élément de A_1 ; on a donc $u(P_\alpha) = P_\alpha$ pour toute racine α. Comme les seuls automorphismes de K sont les homothéties, il y a un élément $c_\alpha \neq 0$ de K tel que l'on ait $u(\tau_\alpha(\lambda)) = \tau_\alpha(c_\alpha\, \lambda)$ $(\lambda \in K)$. Soient $\alpha_1, \ldots, \alpha_\ell$ les racines fondamentales par rapport à B ; comme elles sont linéairement indépendantes, il y a un élément t de T tel que $c_{\alpha_i} = \alpha_i(t)$ $(1 \leq i \leq \ell)$; multipliant u par l'automorphisme intérieur produit par t^{-1}, on se ramène au cas où les c_{α_i} $(1 \leq i \leq \ell)$ sont égaux à 1 ; supposons désormais qu'il en soit ainsi ; u laisse donc fixes les éléments des groupes P_{α_i}. Par ailleurs, u laisse fixes les éléments de T ; en effet, les éléments de la forme $u(t)t^{-1}$ $(t \in T)$ forment un sous-groupe connexe T_0 de T sur lequel chaque racine est constante de valeur 1 ; comme les racines engendrent $X^{\mathbf{Q}}(T)$, il en résulte que T_0 se réduit à l'élément neutre, ce qui montre que u laisse fixes les éléments de T. Par ailleurs, on a $u(P_{-\alpha_i}) = P_{-\alpha_i}$; comme $P_{\alpha_i}\, T_{\alpha_i}\, P_{-\alpha_i}$ est un système de générateurs de Z'_{α_i}, u transforme le groupe Z'_{α_i} en lui-même ; comme le normalisateur de T_{α_i} dans Z'_{α_i} est $T_{\alpha_i} \cup T_{\alpha_i}\, \sigma_{\alpha_i}$, on a $u(\sigma_{\alpha_i}) = t_0\, \sigma_{\alpha_i}$, t_0 étant un élément de T_{α_i}. Or, soit s' un élément distinct de l'élément neutre de $P_{-\alpha_i}$; rappelons que Z'_{α_i} est la réunion des ensembles disjoints $P_{\alpha_i}\, T_{\alpha_i}\, \sigma_{\alpha_i}\, P_{\alpha_i}$ et $P_{\alpha_i}\, T_{\alpha_i}$; s' peut donc se mettre sous la forme $s_1\, t_1\, \sigma_{\alpha_i}\, s_2$, où $s_1, s_2 \in P_{\alpha_i}$, $t_1 \in T_{\alpha_i}$; s_1, s_2 et t_1 sont laissés fixes par u, et on a

$$s'^{-1}\, u(s') = s_2\, \sigma_{\alpha_i}^{-1}\, t_0\, \sigma_{\alpha_i}\, s_2 \ ;$$

cet élément est d'une part dans $P_{-\alpha_i}$ et d'autre part, comme le montre le second membre, dans $P_{\alpha_i}\, T_{\alpha_i}$; c'est donc l'élément neutre, ce qui montre que u laisse invariants les éléments de $P_{-\alpha_i}$ ainsi que σ_{α_i} ; on en déduit que u laisse invariants tous les éléments du groupe Z'_{α_i}, et par suite aussi du groupe $Z_{\alpha_i} = T Z'_{\alpha_i}$. Or on sait que les groupes Z_{α_i} $(1 \leq i \leq \ell)$ engendrent le groupe G (théorème 2, n° 12.4) ; u est donc l'automorphisme identique, d'où $A_1 \subset J$.

Terminons la démonstration de la proposition 1. On a $A_1 \subset A_0$ par définition et l'on vient de prouver la relation $A_1 \subset J$, d'où $A_1 \subset A_0 \cap J$. Notons J_T le groupe des automorphismes intérieurs de G induits par des éléments de T ; comme T normalise T et B, on a $J_T \subset A_1$. Par ailleurs, tout élément de J est de la forme $\mathrm{int}(g)$ où g normalise T et B, d'où $g \in N(T) \cap B = T$ (n° 13.3, théorème 1 et corollaire 3). On a donc $A_0 \cap J = A_1 = J_T$, et puisque l'on a $A = A_0\, J$, le groupe A/J est isomorphe à A_0/A_1. Ce dernier groupe est de manière évidente isomorphe à un groupe de permutations des racines fondamentales.

Corollaire. – *Soit H un sous-groupe invariant fermé connexe de G ; alors H est semi-simple. Si H' est la composante neutre dans le centralisateur de H dans G, on a $G = HH'$ et $H \cap H'$ est fini. Le groupe G/H est semi-simple.*

Le radical de H est évidemment transformé en lui-même par tout automorphisme de H ; c'est donc un sous-groupe résoluble invariant connexe de G, ce qui montre qu'il se réduit à son élément neutre[5]. Si l'on fait correspondre à tout $s \in G$ l'automorphisme $h \to shs^{-1}$ de H, on obtient un homomorphisme de G sur un groupe A d'automorphismes de H, qui contient le groupe J des automorphismes intérieurs de H ; le groupe A/J est donc fini d'après la proposition 1. Or, si H'_0 est le centralisateur de H dans G, l'image réciproque de J par l'homomorphisme en question est le sous-groupe fermé HH'_0 ; comme ce sous-groupe est d'indice fini dans G et que G est connexe, il est égal à G, d'où $HH' = G$ puisque H' est d'indice fini dans H'_0. Le groupe $H \cap H'$ est dans le centre de H, et il est donc fini puisque H est semi-simple. L'homomorphisme canonique de G sur G/H induit un épimorphisme rationnel de H' sur G/H ; H' est semi-simple comme sous-groupe invariant fermé connexe de G ; alors G/H est semi-simple en vertu du

Lemme 5. – *Si ρ est un épimorphisme rationnel de noyau fini de G sur un groupe algébrique G', celui-ci est semi-simple.*

Le noyau N de ρ, étant un sous-groupe invariant fini de G, est dans le centre de G ; si M' est le radical de G', $\rho^{-1}(M')/N$ est isomorphe à M', donc résoluble ; $\rho^{-1}(M')$ est donc un sous-groupe invariant résoluble de G, et est par suite fini, ce qui démontre le lemme 5.

[5] Car G est semi-simple !

17.4 Caractérisation des sous-groupes invariants

Théorème 2. – *Tout sous-groupe invariant fermé connexe H de G est radiciel. Pour qu'une partie S de l'ensemble R des racines R de G détermine un sous-groupe radiciel invariant H de G, il faut et il suffit que chacun des ensembles S et $R-S$ soit fermé ; s'il en est ainsi, le groupe radiciel déterminé par $R-S$ est la composante neutre dans le centralisateur de H.*

A) Soit H un sous-groupe invariant fermé connexe de G, et soit H' la composante neutre dans son centralisateur. Soient T_H (resp. $T_{H'}$) un tore maximal de H (resp. H') et B_H (resp. $B_{H'}$) un groupe de Borel de H (resp. H'). Alors $B_H\,B_{H'}$ est résoluble et connexe, donc contenu dans un groupe de Borel de G, et $T_H\,T_{H'}$ est un tore, donc contenu dans un tore maximal de G. Comme tous les tores maximaux de G sont conjugués, on peut supposer que $T_H\,T_{H'} \subset T$. Comme $G = HH'$, un élément de T peut se mettre sous la forme ss', avec $s \in H$, $s' \in H'$; comme s' et ss' commutent avec les éléments de T_H, il en est de même de s, d'où $s \in T_H$ puisque T_H est son propre centralisateur dans H ; on voit même que $s' \in T_{H'}$, d'où $T = T_H\,T_{H'}$.

Soit B un groupe de Borel de G contenant $B_H\,B_{H'}$, donc T ; le groupe $B \cap H$ (resp. $B \cap H'$) est un sous-groupe résoluble de H (resp. H') contenant B_H (resp. $B_{H'}$) ; on a donc $B_H = B \cap H$, $B_{H'} = B \cap H'$, ce qui montre que B_H, $B_{H'}$ sont des sous-groupes invariants de B. Un élément de B se met sous la forme $s_1\,s'_1$ où $s_1 \in H$, $s'_1 \in H'$; comme $s_1\,s'_1$ et s'_1 appartiennent au normalisateur de B_H, il en est de même de s_1, d'où $s_1 \in B_H$, puisque B_H est son propre normalisateur dans H ; on voit de même que $s'_1 \in B_{H'}$, ce qui montre que $B = B_H\,B_{H'}$.

Soit B_H^u l'ensemble des éléments unipotents de B_H ; comme c'est un sous-groupe invariant de B contenu dans B^u, il est engendré par ceux des P_α qu'il contient. Soient R_- l'ensemble des racines de G qui sont négatives sur la chambre associée à B et S_- l'ensemble des $\alpha \in R_-$ tels que $P_\alpha \subset B_H$; il est clair que la condition $\alpha \in R_- - S_-$ entraîne $P_\alpha \in B_{H'}$. Soit $\alpha \in S_-$; le groupe $P_{-\alpha}$, qui est conjugué à P_α dans G, est contenu dans H; or Z'_α *est engendré par* P_α *et* $P_{-\alpha}$; en effet, le normalisateur dans Z'_α du groupe engendré par P_α et $P_{-\alpha}$ contient T_α, et est donc identique à Z'_α, puisque $P_\alpha\,T_\alpha\,P_{-\alpha}$ est un ensemble de générateurs de Z'_α ; le groupe engendré par P_α et $P_{-\alpha}$ est donc un sous-groupe invariant de Z'_α, et par suite semi-simple (corollaire du théorème 1) ; comme tout groupe semi-simple de dimension > 0 est de dimension ≥ 3, le groupe engendré par P_α et $P_{-\alpha}$ est Z'_α tout entier. On a donc $Z'_\alpha \subset H$ pour tout $\alpha \in S_-$; de plus, il est clair que le groupe $\widetilde{B}_H$ engendré par les $P_{-\alpha}$ pour $\alpha \in S_-$ est le groupe de Borel de H opposé à B_H (relativement à T_H) ; le groupe engendré par les Z'_α pour $\alpha \in S_-$ contient $B_H\,\widetilde{B}_H$, qui est une partie ouverte de H ; ce groupe est donc identique à H. Soit S l'ensemble composé de S_- et des opposées des racines de S_- ; comme les éléments de $T_{H'}$ commutent avec ceux de H, il est clair que les racines appartenant à S prennent la valeur 1 sur $T_{H'}$. On voit de même que H' est

engendré par les Z'_α pour $\alpha \in R_- - S_-$; comme $R - S$ est l'ensemble des $\pm\alpha$ pour $\alpha \in R_- - S_-$, les racines de $R - S$ prennent la valeur 1 sur T_H. Comme $T_H\, T_{H'} = T$, aucune racine ne peut être égale à 1 à la fois sur T_H et sur $T_{H'}$; S (resp. $R - S$) est donc l'ensemble de toutes les racines de G qui sont égales à 1 sur $T_{H'}$ (resp. T_H), ce qui montre que S et $R - S$ sont fermés.

B) Nous allons maintenant prouver que si H est le groupe radiciel défini par une partie fermée S de R telle que $R - S$ soit fermée, alors H est invariant dans G.

Lemme 6. – *Soit S un ensemble fermé de racines tel que $R - S$ soit fermé. Soient $\alpha \in S$ et $\beta \in R - S$. Il n'existe aucune racine de la forme $i\alpha + j\beta$ où i et j sont des entiers > 0.*

Soient w_α et w_β les réflexions par rapport aux racines α et β respectivement ; on a

$$w_\alpha \cdot \beta = \beta + k\alpha\,, \qquad w_\beta \cdot \alpha = \alpha + k'\beta\,,$$

où k, k' sont des entiers. Les racines sont des éléments de l'espace vectoriel $X^{\mathbf{Q}}(T)$ sur le corps des nombres rationnels, sur lequel opère le groupe de Weyl. Choisissons une forme quadratique définie positive invariante par le groupe de Weyl ; désignant par $(\lambda \mid \mu)$ le produit scalaire de deux éléments λ, μ relativement à cette forme quadratique, on a

$$k = -2\,(\alpha \mid \beta)\,(\alpha \mid \alpha)^{-1}\,, \qquad k' = -2\,(\alpha \mid \beta)\,(\beta \mid \beta)^{-1}\ ;$$

comme $\beta \neq \pm\alpha$, α et β sont linéairement indépendantes, d'où il résulte que l'on a $kk' < 4$; k et k' étant de même signe, l'un au moins de ces entiers est ≤ 1 en valeur absolue. Or $\alpha \pm \beta$ ne peut être ni dans S ni dans $R - S$ (qui sont des parties fermées) et n'est par suite pas une racine ; l'un des nombres k, k' est donc nul, ce qui entraîne $(\alpha \mid \beta) = 0$. Ceci montre que *toute racine de S est orthogonale à toute racine de $R - S$*. Si $i\alpha + j\beta$ était une racine et appartenait disons à S, on aurait $(i\alpha + j\beta \mid \beta) = 0$, d'où $j(\beta \mid \beta) = 0$, et donc $j = 0$ en contradiction avec l'hypothèse $j > 0$; on voit de même que $i\alpha + j\beta$ ne peut être dans $R - S$.

Lemme 7. – *Sous les hypothèses du lemme* 6*, les sous-groupes P_α et P_β de G commutent.*

Il existe au moins un groupe de Borel B contenant T tel que α et β soient négatives sur la chambre associée à B ; en effet, α et β étant linéairement indépendantes, l'ensemble des $\gamma \in \Gamma^{\mathbf{Q}}(T)$ tels que $\langle \gamma, \alpha \rangle < 0$ et $\langle \gamma, \beta \rangle < 0$ est une partie ouverte non vide de $\Gamma^{\mathbf{Q}}(T)$, et rencontre par suite au moins une chambre. Ceci étant, il résulte du lemme 6 et du corollaire au lemme 1 que $P_\alpha\, P_\beta$ est un sous-groupe de B. Comme les éléments de ce groupe sont unipotents et comme P_α et P_β en sont des sous-groupes fermés de codimension 1, P_α et P_β sont des sous-groupes invariants de $P_\alpha\ P_\beta$. Si $s \in P_\alpha$, on a $s\,\tau_\beta(\xi)s^{-1} = \tau_\beta(c(s)\xi)$ pour tout $\xi \in K$, avec $c(s) \in K^*$ (le groupe multiplicatif des éléments $\neq 0$ de K). L'application $s \to c(s)$ est un homomorphisme

rationnel (puisque $\tau_\alpha(c(s)) = s\,\tau_\alpha(1)s^{-1}$) de P_α dans K^* ; il en résulte que $c(s) = 1$ pour tout $s \in P_\alpha$, donc que tout élément de P_α commute avec tout élément de P_β.

Soit S un ensemble fermé de racines tel que $R - S$ soit fermé, et soient $\alpha \in S$, $\beta \in R - S$. Nous avons vu plus haut que Z'_α (resp. Z'_β) est engendré par P_α et $P_{-\alpha}$ (resp. P_β et $P_{-\beta}$) ; comme $-\alpha \in S$, $-\beta \in R - S$, le lemme 7 prouve que tout élément de Z'_α commute avec tout élément de Z'_β. Soient H et H' les groupes radiciels définis par les ensembles S et $R - S$ respectivement ; il résulte de ce qu'on vient d'établir que tout élément de H' commute avec tout élément de H. Par ailleurs, le groupe HH' contient Z'_α pour toute racine α ; comme il contient tous les T_α, il contient T, donc aussi les $Z_\alpha = Z'_\alpha T$, ce qui montre que c'est G tout entier. La formule $HH' = G$ montre alors que H et H' sont des sous-groupes distingués de G. Le théorème 2 est donc établi.

17.5 Composantes (presque) simples

Soit S un ensemble fermé de racines tel que $R - S$ soit fermé ; si $\alpha \in S$, $\beta \in R - S$, $w_\alpha \cdot \beta$ est de la forme $\beta + k\,\alpha$, k étant un entier ; cet entier est nul puisque $i\alpha + j\beta$ n'est pas racine si $i \neq 0$, $j \neq 0$ (lemme 5). Soit Σ un système fondamental de racines ; alors Σ est la réunion de $\Sigma \cap S = \Sigma_1$ et de $\Sigma \cap (R - S) = \Sigma_2$, et, si $\alpha \in \Sigma_1$, $\beta \in \Sigma_2$, l'entier de Cartan relatif à α et β est nul d'après ce qui précède. Supposons réciproquement donnée une décomposition $\Sigma = \Sigma_1 \cup \Sigma_2$ de Σ en deux ensembles tels que l'entier de Cartan relatif à une racine de Σ_i et une racine de Σ_j soit nul si $i \neq j$. Soit S (resp. S') l'ensemble des racines qui sont combinaisons linéaires de racines de Σ_1 (resp. Σ_2). Alors toute racine appartient soit à S soit à S'. En effet, si α appartient par exemple à Σ_1, w_α permute entre elles les racines de S et laisse invariantes les racines appartenant à Σ_2, donc aussi toutes celles de S' ; de même, si $\alpha \in \Sigma_2$, w_α laisse invariantes les racines de S et permute entre elles celles de S'. Comme le groupe de Weyl est engendré par les w_α pour $\alpha \in \Sigma$, ses opérations transforment chacun des ensembles S, S' en lui-même. Comme tout racine est transformée d'une racine de Σ par une opération du groupe de Weyl, il en résulte bien que $S \cup S'$ est l'ensemble de toutes les racines. Par ailleurs, il est clair que S et S' sont fermés.

Munissons $X^{\mathbf{Q}}(T)$ d'un produit scalaire défini par une forme quadratique définie positive et invariante par le groupe de Weyl ; on voit alors tout de suite que, α et β étant des racines, une condition nécessaire et suffisante pour que w_α laisse β fixe est que α et β soient orthogonales.

Nous dirons qu'un système de racines est *simple* s'il est impossible de le décomposer en deux parties fermées non vides disjointes. Il résulte alors du théorème 2 que l'on a la

Proposition 2. – *Pour que G n'admette pas d'autres sous-groupes invariants fermés connexes que $\{e\}$ et lui-même, il faut et il suffit que l'ensemble de ses racines soit simple.*

Par ailleurs, dans le cas général, soient $S_1, \ldots, S_h$ les éléments minimaux de l'ensemble des parties $S \neq \varnothing$ de l'ensemble R des racines telles que S et $R - S$ soient fermés ; il est clair que R est la réunion des ensembles disjoints S_i. On a donc le résultat suivant :

Proposition 3. – *Le groupe G contient un certain nombre de sous-groupes fermés invariants connexes G_i qui possèdent les propriétés suivantes : pour tout i, l'ensemble des racines de G_i est simple ; on a $G = G_1 \ldots G_h$; si $i \neq j$, tout élément de G_i commute avec tout élément de G_j ; le groupe $G_i \cap \prod_{j \neq i} G_j$ est fini.*

De plus, on voit facilement que l'ensemble des groupes G_i est bien déterminé par la connaissance de G.

Nous appellerons *presque simple* un groupe semi-simple dont l'ensemble des racines est simple ; les notations étant celles de la proposition 3, nous dirons que les G_i sont les *composantes presque simples* de G.

18. Les isogénies[1]

18.1 Généralités sur les isogénies

Rappelons que, si G et G' sont des groupes algébriques, on appelle *isogénie* de G sur G' un épimorphisme rationnel de noyau fini de G sur G'. Il est clair que, s'il existe une isogénie de G sur G', on a $\dim G = \dim G'$. Si H est un sous-groupe fermé de G, $f(H)$ est un sous-groupe fermé de G'. Le noyau N de f est un sous-groupe invariant fini de G, donc contenu dans le centre de G. Si H' est un sous-groupe fermé connexe de G', il existe un sous-groupe fermé connexe H et un seul de G tel que $f(H) = H'$, à savoir la composante neutre H_0 dans $f^{-1}(H')$. En effet, comme f est surjectif, on a $f(f^{-1}(H')) = H'$; $f(H_0)$ est donc un sous-groupe fermé d'indice fini de H', d'où $f(H_0) = H'$ puisque H' est connexe. Par ailleurs, si H est un sous-groupe fermé connexe de $f^{-1}(H')$, on a $H \subset H_0$. Comme f est de noyau fini, on a $\dim H_0 = \dim H'$, et, si $f(H) = H'$, on a $\dim H = \dim H' = \dim H_0$, d'où $H = H_0$.

Soit f une isogénie du groupe connexe G sur le groupe (connexe) G' ; soient Φ et Φ' les corps de fonctions numériques sur G et G' respectivement. Le cohomomorphisme φ de f est alors un isomorphisme φ de Φ' sur un sous-corps Φ_1 de Φ.

On peut montrer que la connaissance de Φ_1 détermine l'isogénie f à un isomorphisme près ; d'une manière précise, si f' et f'' sont des isogénies de G sur des groupes G' et G'' dont les cohomomorphismes appliquent les corps de fonctions numériques sur G' et G'' sur le même sous-corps Φ_1 de Φ, il existe un isomorphisme h de G' sur G'' tel que $h \circ f' = f''$. On peut aussi caractériser comme suit les sous-corps Φ_1 de Φ qui correspondent à des isogénies de G. Pour tout $s \in G$, désignons par $\lambda(s)$ et $\mu(s)$ les cohomomorphismes des translations à gauche et à droite par s dans G ; pour qu'un sous-corps Φ_1 de Φ (contenant K) soit attaché à une isogénie de G, il faut et suffit que Φ soit une extension algébrique de degré fini de Φ_1 et que Φ_1 soit transformé en lui-même par les opérations $\lambda(s)$, $\mu(s)$ pour tout $s \in G$. L'isogénie f est dite *radicielle* si Φ est une extension radicielle de Φ_1 ; on dit de plus que f est radicielle de hauteur 1 si on a $\Phi^p \subset \Phi_1$, où Φ^p est le corps des puissances p-ièmes des fonctions de Φ. On montre que Φ_1 est alors déterminé par la connaissance de celles des dérivations invariantes à gauche (ou d'ailleurs à droite) qui sont nulles sur Φ_1 ; ces dérivations forment un sous-espace vectoriel $\mathfrak{a}$ de l'algèbre de Lie $\mathfrak{g}$ de G, qui est stable relativement à la représentation adjointe de G et

[1] Exposé de C. Chevalley, le 25.11.1957

à l'opération de puissance p-ième dans $\mathfrak{g}$. Réciproquement, on peut montrer que tout sous-espace $\mathfrak{a}$ de $\mathfrak{g}$ satisfaisant à ces conditions est attaché à une isogénie radicielle f de hauteur 1. Nous ne démontrerons pas ces résultats, qui ne seront pas utilisés dans la suite. Nous allons cependant démontrer la :

Proposition 1. – *Pour tout groupe algébrique connexe G, dont nous désignerons le corps des fonctions numériques par Φ, et pour toute puissance q de l'exposant caractéristique de K, il existe une isogénie de G sur un groupe G' dont le cohomomorphisme applique le corps des fonctions numériques sur G' sur le corps Φ^q des puissances q-ièmes des éléments de Φ.*

Il est bien connu que l'ensemble des points de G peut être muni d'une structure de variété telle que les fonctions numériques sur cette variété soient les puissances q-ièmes des fonctions de Φ ; désignons cette variété par G'. L'application identique f de G est un morphisme de G dans G' dont le cohomomorphisme est l'isomorphisme d'inclusion de Φ^q dans Φ. Il reste à montrer que l'application $(s,t) \to st$ est un morphisme de la variété $G' \times G'$ dans G'. Or cette application est un morphisme de $G \times G$ dans G ; son cohomomorphisme est un isomorphisme μ de Φ sur un sous-corps du corps des fonctions numériques sur $G \times G$, qui s'identifie au corps des fractions de $\Phi \otimes \Phi$. Il est clair que $\mu(\Phi^q)$ est contenu dans le corps des fractions de $\Phi^q \otimes \Phi^q$, donc dans le corps des fonctions numériques sur $G' \times G'$; la restriction de μ à Φ^q est le cohomomorphisme d'une fonction m' (*a priori* non nécessairement partout définie) sur la variété $G' \times G'$ à valeurs dans G' et que l'on a $m' \odot f = f \odot m$ en désignant par m la multiplication dans G, d'où $m'(s,t) = st$ si m' est définie en (s,t). Par ailleurs, G et G' ont même topologie, et le graphe M de m est une sous-variété fermée de $G \times G \times G$, donc aussi de $G' \times G' \times G'$ (car $G' \times G' \times G'$ est la variété dont les points sont ceux de $G \times G \times G$ et dont les fonctions numériques sont les puissances q-ièmes des fonctions sur $G \times G \times G$). Il en résulte que M est l'adhérence du graphe de m' dans $G' \times G' \times G'$. La projection $(s,t,u) \to (s,t)$ de $G' \times G' \times G'$ sur $G' \times G'$ induit une bijection π de M sur $G' \times G'$ qui est aussi un morphisme birationnel. Comme G est une variété normale, il en est de même de G' ; on en déduit que π est un isomorphisme de M sur $G' \times G'$ (n° 5.3, théorème 2), donc que m' est partout définie et que G' est un groupe.

Nous appellerons *isogénie des puissances q-ièmes* l'isogénie f du groupe G que l'on vient de définir ; du point de vue ensembliste, c'est l'application identique de G.

Proposition 2. – *Soit f une isogénie d'un groupe algébrique connexe G sur un groupe algébrique connexe G'. Si l'un des groupes G, G' est semi-simple (resp. presque-simple), il en est de même de l'autre.*

Soient H un sous-groupe fermé connexe de G et $f(H) = H'$. Si H est invariant (resp. résoluble) dans G, il est clair que H' est invariant (resp. résoluble) dans G'. Réciproquement, si H' est invariant dans G', $f^{-1}(H')$ est invariant dans G, et il en est de même de H qui est la composante neutre

dans $f^{-1}(H')$. Si H' est résoluble, il en est de même de H ; car, si N est le noyau de f , $f^{-1}(H)/N$ est isomorphe à H', donc résoluble, et N est dans le centre de $f^{-1}(H')$, ce qui montre que $f^{-1}(H')$ est résoluble ; la proposition 2 résulte immédiatement de là.

18.2 Isomorphisme spécial associé à une isogénie

Soit maintenant G un groupe semi-simple, et soit T un tore maximal de G. Si α est une racine de G par rapport à T, il existe un isomorphisme τ_α du groupe additif K sur un sous-groupe fermé dans G tel que $t\,\tau_\alpha(\xi)t^{-1} = \tau_\alpha(\alpha(t)\xi)$ si $\xi \in K$, $t \in T$; nous dirons que τ_α est *associé à* α ; les éléments de $\tau_\alpha(K)$ sont unipotents ; nous dirons que le groupe $\tau_\alpha(K)$ est un *sous-groupe unipotent de* G *associé à* α.

Lemme 1. – *Soit* P *un sous-groupe fermé connexe de dimension* 1 *de* G *composé d'éléments unipotents et dont le normalisateur contient* T *; il existe une racine* α *et une seule telle que* P *soit associé à* α.

Le groupe PT est résoluble et connexe ; il est donc contenu dans un groupe de Borel B de G, et P est contenu dans l'ensemble B^u des éléments unipotents de B. Soient α_i $(1 \leq i \leq N)$ les racines de G qui sont négatives sur la chambre de Weyl associée à B ; il existe alors pour chaque i un groupe P_i associé à α_i contenu dans B^u, et P est le produit de ceux des P_i qu'il contient (n° 13.2, théorème 1). Comme $\dim P = 1$, il existe un i tel que $P_i = P$. Soit τ_i un isomorphisme de K sur $P_i = P$ associé à α_i ; si P est associé à une racine α, soit τ un isomorphisme de K sur P associé à α. Comme τ et τ_i sont des isomorphismes, on a $\tau(\xi) = \tau_i(c\,\xi)$ avec un $c \neq 0$ de K (n° 9.1, lemme 1) ; il en résulte aussitôt que $\alpha = \alpha_i$. C.Q.F.D.

Soit maintenant f une isogénie de G sur un groupe G' ; alors $T' = f(T)$ est un tore maximal de G', et la restriction f_T de f à T est une isogénie de T sur T'. Elle détermine un isomorphisme $\theta' \to \theta' \circ f_T$ du groupe $X(T')$ des caractères rationnels de T' sur un sous-groupe du groupe $X(T)$ des caractères rationnels de T. Comme $\dim T = \dim T'$, cet isomorphisme se prolonge en un isomorphisme φ de l'espace vectoriel $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(T)$, que nous appellerons *l'isomorphisme attaché à* f. Soit α une racine de G par rapport à T, et soit P_α le groupe unipotent associé à α ; alors f induit une isogénie f_α de P_α sur un sous-groupe connexe P'_α de dimension 1 de G' dont les éléments sont unipotents et dont le normalisateur contient T' ; P'_α est donc le groupe unipotent associé à une racine α' bien déterminée de G' ; nous dirons que α et α' *se correspondent par l'isogénie* f.

Réciproquement, soit α' une racine de G' et soit $P'_{\alpha'}$ le groupe unipotent qui lui est associé ; c'est l'image par f d'un sous-groupe connexe P de dimension 1 de G, et d'un seul. Il est clair que le normalisateur de P contient T. Le groupe P est résoluble (*cf.* la démonstration de la proposition 1) et n'est

pas un tore, car sinon $P'_{\alpha'} = f(P)$ serait un tore. Comme $\dim P = 1$, il en résulte que P est composé d'éléments unipotents ; c'est donc le groupe unipotent associé à une racine α de G. La correspondance que nous avons établie entre racines de G et racines de G' définit donc une bijection de l'ensemble des premières sur l'ensemble des secondes. Soient de plus τ_α, $\tau'_{\alpha'}$, des isomorphismes de K sur P_α et $P'_{\alpha'}$ respectivement ; on a donc, pour $\xi \in K$, $f(\tau_\alpha(\xi)) = \tau'_{\alpha'}(m(\xi))$, où m est une isogénie de K sur K ; $m(\xi)$ s'exprime comme polynôme en ξ. Si $t \in T$, $t' = f(t)$, on a

$$t' f(\tau_\alpha(\xi))\, t'^{-1} = f(t\, \tau_\alpha(\xi)\, t^{-1}) = f(\tau_\alpha(\alpha(t)\xi))$$

d'où $\alpha'(t')\, m(\xi) = m(\alpha(t)\xi)$. Comme $m(\xi)$ est un polynôme en ξ, ce polynôme est homogène ; si $q(\alpha)$ est son degré, on a $\alpha'(t') = (\alpha(t))^{q(\alpha)}$, ce qui donne, en notation additive,

$$\varphi(\alpha') = q(\alpha)\alpha\,.$$

De plus, comme m est un homomorphisme de K dans lui-même, $q(\alpha)$ est une puissance de l'exposant caractéristique de K.

Définition 1. – *Soient G et G' des groupes algébriques semi-simples, T et T' des tores maximaux de G et G', $X(T)$ et $X(T')$ les groupes des caractères rationnels de T et T'. Un isomorphisme φ de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(T)$ est dit spécial*[2] *si les conditions suivantes sont satisfaites :*

a) *on a $\varphi(X(T')) \subset X(T)$;*

b) *il existe une bijection ψ de l'ensemble des racines de G par rapport à T sur l'ensemble des racines de G' par rapport à T' telle que l'on ait $\varphi(\psi(\alpha)) = q(\alpha)\alpha$ pour toute racine α de G, $q(\alpha)$ étant une puissance de l'exposant caractéristique de K ; les $q(\alpha)$ sont alors appelés les exposants radiciels de φ.*

On notera que ψ et les $q(\alpha)$ sont alors uniquement déterminés par φ, car si α_1 et α_2 sont des racines telles que $\alpha_2 = c\,\alpha_1$, avec c rationnel > 0, on a $c = 1$.

L'isomorphisme attaché à une isogénie est donc toujours spécial. *C'est l'un des objets essentiels de ce séminaire d'établir que, réciproquement, tout isomorphisme spécial est attaché à une isogénie.*[3]

18.3 Propriétés des isomorphismes spéciaux

Proposition 3. – *Soient G un groupe algébrique semi-simple, T un tore maximal de G, q une puissance de l'exposant caractéristique de K, f l'isogénie*

[2] Lorsque K est de caractéristique 0, un isomorphisme spécial est un isomorphisme φ de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(T)$ appliquant $X(T')$ dans $X(T)$ et induisant une bijection de l'ensemble des racines de G' sur l'ensemble des racines de G. On a $q(\alpha) = 1$ pour toute racine α de G.

[3] L'unicité de l'isogénie en question (à automorphisme intérieur près) sera établie au n° 23.2, proposition 2.

des puissances q-ièmes de G, G′ le groupe f(G), T′ le groupe f(T). L'isomorphisme spécial φ de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(T)$ attaché à f applique X(T′) sur qX(T) ; ses exposants radiciels sont tous égaux à q.

Soit H un sous-groupe fermé connexe de G, et soit $f(H) = H'$. Pour qu'une fonction numérique u sur G soit définie en un point $s \in H$, il faut et suffit que u^q, considérée comme fonction sur G', soit définie en s ; il en résulte immédiatement que la restriction de f à H est l'isogénie des puissances q-ièmes pour H. Prenant $H = T$, on voit que les caractères rationnels de T' sont les puissances q-ièmes des caractères rationnels de T d'où $\varphi(X(T')) = qX(T)$. Prenant pour H le groupe $\tau_\alpha(K)$, où τ_α est un isomorphisme associé à une racine α, on voit qu'il existe un isomorphisme τ' de K sur H' tel que $f(\tau_\alpha(\xi)) = \tau'(\xi^q)$, ce qui montre que l'exposant radiciel relatif à α est q.

Proposition 4. – *Soit V un espace vectoriel de dimension finie sur K ; soit f_V l'application naturelle de* GL(V) *sur le groupe projectif* PL(V). *Soient G un sous-groupe fermé semi-simple de* GL(V), *G′ le groupe $f_V(G)$, f la restriction de f_V à G. Les exposants radiciels de l'isomorphisme spécial attaché à f sont tous égaux à* 1.

Soit T un tore maximal de G. Si P est un groupe associé à une racine α de G par rapport à T, P est contenu dans l'ensemble N des éléments unipotents d'un groupe de Borel de GL(V) ; il suffira de montrer que f_V induit un isomorphisme de N sur un sous-groupe de PL(V). Or, il existe une base $(e_1, \ldots, e_n)$ de V telle que l'on ait, pour $s \in N$, $s \cdot e_i \equiv e_i \Big(\mathrm{mod} \sum_{j>i} Ke_j\Big)$; si on pose $s \cdot e_i = e_i + \sum_{j>i} u_{ji}(s)e_j$, les u_{ji} $(j > i)$ engendrent l'algèbre affine de N. Posons, pour $t \in \mathrm{GL}(V)$, $t \cdot e_i = \sum_{j=1}^{n} v_{ji}(t)e_j$; les fonctions $v_{ji}/v_{j'i'}$ sont les images par le cohomomorphisme de f_V de fonctions numériques sur PL(V). Or, si $j > i$, $s \in N$, on a $u_{ji}(s) = v_{ji}(s)$; les u_{ji} sont donc les images par le cohomomorphisme de la restriction f_N de f_V à N de fonctions numériques partout définies sur $f_V(N)$, ce qui démontre notre assertion.

Proposition 5. – *Soient G et G′ des groupes algébriques semi-simples, T et T′ des tores maximaux de G et G′ respectivement et φ un isomorphisme spécial de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(T)$. L'application $\varphi_W : w' \to \varphi \circ w' \circ \varphi^{-1}$ induit alors un isomorphisme du groupe de Weyl W′ de G′ sur le groupe de Weyl W de G ; si w′ est la réflexion par rapport à une racine α′ de G′, $\varphi_W(w')$ est la réflexion par rapport à la racine α de G telle que $\varphi(\alpha') = q(\alpha)\alpha$, $q(\alpha) > 0$. Si α et β sont des racines de G transformées l'une de l'autre par une opération de W, les exposants radiciels correspondant à α et à β sont égaux. Soient $\alpha_1, \ldots, \alpha_n$ des racines de G et α'_i les racines de G′ telles que $\varphi(\alpha'_i) = q_i\,\alpha_i$, $q_i > 0$; pour que $\alpha_1, \ldots, \alpha_n$ forment un système fondamental de racines de G, il faut et il suffit que $\alpha'_1, \ldots, \alpha'_n$ forment un système fondamental de racines de G′. Supposons qu'il en soit ainsi ; soient w_i et w'_i les réflexions par rapport à*

α_i, α'_i respectivement ; posons $w_i(\alpha_j) = \alpha_j + c(i,j)\alpha_i$, $w'_i(\alpha'_j) = \alpha'_j + c'(i,j)\alpha'_i$. *On a alors* $c(i,j) = c'(i,j)q_i\, q_j^{-1}$.

Il est clair que l'application $\varphi_{W'} : w' \to \varphi \circ w' \circ \varphi^{-1}$ est un isomorphisme de W' sur un groupe d'automorphismes de $X^{\mathbf{Q}}(T)$.

Soit w' un élément de W', et soit $w = \varphi \circ w' \circ \varphi^{-1}$. Si β est une racine de G, on a $\varphi^{-1}(\beta) = (q(\beta))^{-1}\beta'$, où β' est une racine de G', d'où

$$(w' \circ \varphi^{-1})(\beta) = (q(\beta))^{-1}\,\gamma'$$

si γ' est la racine $w'(\beta')$; on a donc $w(\beta) = q(\gamma)(q(\beta))^{-1}\gamma$ si $\varphi(\gamma') = q(\gamma)\gamma$. Il existe donc une permutation ϖ de l'ensemble des racines de G telle que $w(\beta) = c(\beta)\,\varpi(\beta)$ avec un nombre rationnel $c(\beta) > 0$. Supposons maintenant que w' soit la réflexion par rapport à une racine α' ; on a alors

$$\gamma' = \beta' + a(\beta')\alpha'\,,$$

$a(\beta')$ étant un entier ; si l'on pose $\varphi(\alpha') = q(\alpha)\alpha$, on a $w(\beta) = \beta + r(\beta)\alpha$, $r(\beta)$ étant un nombre rationnel.

Par ailleurs, il est clair que $w(\alpha) = -\alpha$. Soit w_α la réflexion par rapport à α. On a donc

$$(w_\alpha\, w)(\beta) = c(\beta)\,\varpi'(\beta) = \beta + s(\beta)\alpha$$

où $c(\beta)$, $s(\beta)$ sont des nombres rationnels et ϖ' est une permutation de l'ensemble des racines ; de plus, $(w_\alpha\, w)(\alpha) = \alpha$. Soit k l'ordre de la permutation ϖ' ; on a $(w_\alpha\, w)^k(\beta) = c_1(\beta)\beta = \beta + ks(\beta)\alpha$ avec $c_1(\beta)$ rationnel. Or, si on prend $\beta \neq \pm\alpha$, α et β sont linéairement indépendantes, d'où $c_1(\beta) = 1$, $s(\beta) = 0$. On a aussi $s(\pm\alpha) = 0$; $w_\alpha\, w$ est donc l'identité, d'où $w = w_\alpha$. Autrement dit, on a $\varphi_W(w_{\alpha'}) = w_\alpha$. Comme les groupes de Weyl W et W' sont engendrés par les réflexions par rapport aux racines, il en résulte que $w' \to \varphi \circ w' \circ \varphi^{-1}$ est un isomorphisme de W' sur W. Les notations étant les mêmes qu'au début, on a $w \in W$, donc $w(\beta)$ est une racine, d'où $q(\beta) = q(\gamma)$, $\gamma = w(\beta)$.

Comme φ est un isomorphisme d'espaces vectoriels, une condition nécessaire et suffisante pour que $\alpha_1, \ldots, \alpha_n$ soient linéairement indépendantes est qu'il en soit ainsi de $\alpha'_1, \ldots, \alpha'_n$; de plus une condition nécessaire et suffisante pour que toute racine de G puisse s'exprimer comme combinaison linéaire à coefficients rationnels tous ≥ 0 ou tous ≤ 0 des α_i est que toute racine de G' puisse s'exprimer comme combinaison linéaire à coefficients rationnels tous ≥ 0 ou tous ≤ 0 des α'_i ; l'avant-dernière assertion de la proposition 5 résulte de là. On a $\varphi \circ w'_i = w_i \circ \varphi$, d'où $w_i(\varphi(\alpha'_j)) = q_j\,\alpha_j + c'(i,j)q_i\,\alpha_i$ et

$$w_i(\varphi(\alpha'_j)) = q_j\, w_i(\alpha_j) = q_j(\alpha_j + c(i,j)\alpha_i)\,,$$

ce qui démontre la dernière assertion.

18.4 Comparaison des isogénies

Proposition 6. – *Soient G, G', G'' des groupes algébriques semi-simples, f' et f'' des isogénies de G sur G' et G'' respectivement, T un tore maximal de G, $T' = f'(T)$, $T'' = f''(T)$, φ' et φ'' les isomorphismes de $X^{\mathbf{Q}}(T')$ et $X^{\mathbf{Q}}(T'')$ sur $X^{\mathbf{Q}}(T)$ attachés à f' et f'' respectivement. Supposons qu'il existe un isomorphisme spécial γ de $X^{\mathbf{Q}}(T'')$ sur $X^{\mathbf{Q}}(T')$ tel que $\varphi' \circ \gamma = \varphi''$. Il existe alors une isogénie unique g de G' sur G'' qui applique T' sur T'' telle que γ soit l'isomorphisme spécial attaché à g et que $g \circ f' = f''$. Si γ applique $X(T'')$ sur $X(T')$ et si ses exposants radiciels sont égaux à 1, g est un isomorphisme.*

La restriction de γ à $X(T'')$ est un isomorphisme de ce groupe sur un sous-groupe d'indice fini de $X(T')$; il existe donc une isogénie g_T de T' sur T'' telle que $\theta'' \circ g_T = \gamma(\theta'')$ si $\theta'' \in X(T'')$; il résulte immédiatement de la formule $\varphi' \circ \gamma = \varphi''$ que

$$g_T \circ f'_T = f''_T$$

en désignant par f'_T, f''_T respectivement les restrictions de f' et f'' à T.

Soient α une racine de G par rapport à T, τ_α un isomorphisme de K sur un sous-groupe de G associé à α, $P_\alpha = \tau_\alpha(K)$, α' et α'' les racines de G' et G'' telles que $\varphi'(\alpha') = q'(\alpha)\alpha$, $\varphi''(\alpha'') = q''(\alpha)\alpha$, avec $q'(\alpha) > 0$, $q''(\alpha) > 0$. Il résulte de la définition des exposants radiciels qu'il existe des isomorphismes $\tau'_{\alpha'}$, $\tau''_{\alpha''}$ de K sur $f'(P_\alpha)$ et $f''(P_\alpha)$ respectivement tels que l'on ait, pour tout $\xi \in K$, les égalités

$$f'(\tau_\alpha(\xi)) = \tau'_{\alpha'}(\xi^{q'(\alpha)}), \ f''(\tau_\alpha(\xi)) = \tau''_{\alpha''}(\xi^{q''(\alpha)}).$$

Par ailleurs, γ étant spécial, $\gamma(\alpha'')$ est de la forme $\overline{q}(\alpha)\,\overline{\alpha'}$, où $\overline{q}(\alpha)$ est un entier > 0 et $\overline{\alpha'}$ une racine de G'. Comme $\varphi' \circ \gamma = \varphi''$, on a

$$\varphi''(\alpha'') = \overline{q}(\alpha)\,\varphi'(\overline{\alpha'}) = q''(\alpha)\alpha.$$

Il en résulte que $\overline{\alpha'} = \alpha'$, $\overline{q}(\alpha)\,q'(\alpha) = q''(\alpha)$; il existe par suite un homomorphisme g_α de $f'(P_\alpha)$ sur $f''(P_\alpha)$ tel que $g_\alpha(\tau'_{\alpha'}(\xi)) = \tau''_{\alpha''}(\xi^{\overline{q}(\alpha)})$ pour tout $\xi \in K$, et l'on a

$$g_\alpha \circ f'_\alpha = f''_\alpha$$

en désignant respectivement par f'_α et f''_α les restrictions de f' et f'' à P_α.

Choisissons un groupe de Borel B de G contenant T ; soient $\alpha_1, \ldots, \alpha_N$ les racines qui sont négatives sur la chambre associée à B ; le groupe B^u des éléments unipotents de B est alors le produit des P_{α_i} $(1 \leq i \leq N)$ (théorème 1 du n° 13.2). De plus, il existe un groupe de Borel C de G contenant T tel que le groupe C^u des éléments unipotents de C soit le produit des $P_{-\alpha_i}$ $(1 \leq i \leq N)$; l'application $(b, t, c) \to btc$ est un isomorphisme de la variété $B^u \times T \times C^u$ sur une sous-variété ouverte U de G (n° 13.4, corollaire 2 du théorème 3).

Les groupes $B' = f(B)$, $C' = f(C)$ sont des groupes de Borel de G' contenant T'. Soit α'_i la racine de G' telle que $\varphi'(\alpha'_i) = q'(\alpha_i)\alpha_i$; le groupe unipotent associé à α'_i est le sous-groupe $f(P_{\alpha_i})$ de B', tandis que le groupe unipotent associé à $-\alpha'_i$ est $f(P_{-\alpha_i}) \subset C'$. Il en résulte que les α'_i (resp. $-\alpha'_i$) sont les racines qui sont négatives sur la chambre associée à B' (resp. C'). Désignant par B'^u et C'^u les groupes d'éléments unipotents de B' et C' respectivement, B'^u (resp. C'^u) est le produit des $f'(P_{\alpha_i})$ (resp. $f'(P_{-\alpha_i})$) et

$$(b', t', c') \to b't'c'$$

est un isomorphisme de $B'^u \times T' \times C'^u$ sur une sous-variété ouverte U' de G' (*loc. cit.*) ; on a $U' = f'(U)$.

Il existe donc un morphisme g_U de la variété U' dans G'' tel que l'on ait

$$g_U\Big(\Big(\prod_{i=1}^{N} s'_i\Big)\, t'\Big(\prod_{i=1}^{N} \widetilde{s}'_i\Big)\Big) = \prod_{i=1}^{N} g_{\alpha_i}(s'_i)\, g_T(t') \prod_{i=1}^{N} g_{-\alpha_i}(\widetilde{s}'_i)$$

si $s'_i \in f'(P_{\alpha_i})$, $\widetilde{s}'_i \in f'(P_{-\alpha_i})$ $(1 \leq i \leq N)$. De plus, il est clair que

$$g_U \circ f'_U = f''_U\,,$$

en désignant par f'_U et f''_U respectivement les restrictions de f' et f'' à U. L'application g_U se prolonge en une fonction g sur G' à valeurs dans G''. *Nous allons montrer que cette fonction est partout définie et est un homomorphisme.*

Soient s un élément de G, $s' = f'(s)$, $s'' = f''(s)$; désignons par λ, λ', λ'' les translations à gauche par s, s', s'' dans G, G', G'' respectivement. On va démontrer que $g \odot \lambda' = \lambda'' \odot g$ (on rappelle que $g \odot \lambda'$, par exemple, est l'unique fonction sur G' à valeurs dans G'' qui prolonge l'application $g \circ \lambda'$). On a évidemment $g \odot f' = f''$, d'où $\lambda'' \odot g \odot f' = \lambda'' \odot f''$; comme f', f'' sont des homomorphismes on a

$$\lambda'' \circ f'' = f'' \circ \lambda = g \odot f' \odot \lambda = g \odot \lambda' \odot f'\,,$$

d'où

$$\lambda'' \odot g \odot f' = g \odot \lambda' \odot f'\,.$$

Comme f' est surjectif, il en résulte tout de suite que $\lambda'' \odot g = g \odot \lambda'$. Si donc g est définie en un point s'_0, elle l'est aussi en $\lambda'(s'_0) = s's'_0$. Ceci étant vrai pour tout $s \in G$, g est partout définie, et l'on peut écrire $g \circ f' = f''$, $\lambda'' \circ g = g \circ \lambda'$, d'où $g(f'(s)s'_0) = f''(s)\, g(s'_0) = g(f'(s))\, g(s'_0)$ pour tout $s \in G$ et tout $s'_0 \in G'$. Comme f' est surjectif, g est un homomorphisme. L'image réciproque par f' du noyau de g est contenue dans le noyau de f'' et est donc finie, ce qui montre que le noyau de g est fini ; on a $g(G') = g(f'(G)) = f''(G) = G''$, ce qui démontre que g est surjectif ; g est donc une isogénie et,

comme f' est surjectif, g est l'unique homomorphisme de G' dans G'' tel que $f'' = g \circ f'$. On a

$$g(T') = g_T(T') = T'' \ ;$$

si γ^* est l'isomorphisme de $X^{\mathbf{Q}}(T'')$ sur $X^{\mathbf{Q}}(T')$ attaché à g, il résulte immédiatement de la formule $g \circ f' = f''$ que $\varphi' \circ \gamma^* = \varphi'' = \varphi' \circ \gamma$, d'où $\gamma^* = \gamma$.

Supposons maintenant que $\gamma(X(T'')) = X(T')$ et que les exposants radiciels de γ soient égaux à 1 ; γ^{-1} est alors évidemment un isomorphisme spécial, et il existe donc une isogénie g' de G'' sur G' telle que $g' \circ f'' = f'$. On a

$$g \circ g' \circ f'' = f'' \ ;$$

comme f'' est surjectif, $g \circ g'$ est l'application identique de G''. De même, $g' \circ g$ est l'application identique de G' ; g est donc alors un isomorphisme, et la proposition 6 est établie.

Proposition 7. – *Soient G, G', G'' des groupes algébriques semi-simples, f' et f'' des isogénies de G' et G'' sur G respectivement, T un tore maximal de G, T' et T'' les tores maximaux de G' et G'' tels que $f'(T') = f''(T'') = T$, φ' et φ'' les isomorphismes de $X^{\mathbf{Q}}(T)$ sur $X^{\mathbf{Q}}(T')$ et $X^{\mathbf{Q}}(T'')$ attachés à f' et f'' respectivement. Supposons qu'il existe un isomorphisme spécial γ de $X^{\mathbf{Q}}(T'')$ sur $X^{\mathbf{Q}}(T')$ tel que $\gamma \circ \varphi'' = \varphi'$. Il existe alors une isogénie g de G' sur G'' qui applique T' sur T'' telle que γ soit l'isomorphisme attaché à g et que $f'' \circ g = f'$. Si l'on suppose que $\gamma(X(T'')) = X(T')$ et que les exposants radiciels de γ sont égaux à 1, g est un isomorphisme.*

Etablissons d'abord le

Lemme 2. – *Soient f' et f'' des isogénies de groupes algébriques connexes G' et G'' sur un groupe G. Il existe alors un groupe algébrique connexe H et des isogénies h' et h'' de H sur G' et G'' tels que $f' \circ h' = f'' \circ h''$.*

Soit H_0 l'ensemble des $(s', s'') \in G' \times G''$ tels que $f'(s') = f''(s'')$; c'est évidemment un sous-groupe fermé de $G' \times G''$. Soit H la composante neutre dans H_0 ; les projections de $G' \times G''$ sur G' et G'' induisent les homomorphismes h' et h'' de H dans G' et G'' respectivement, et l'on a $f' \circ h' = f'' \circ h''$. Comme f' et f'' sont surjectifs, les projections de $G' \times G''$ sur ses deux facteurs induisent des épimorphismes h_0 et h'_0 de H_0 sur G' et G'' ; comme H est d'indice fini dans H_0 et que G' et G'' sont connexes, h' et h'' sont surjectifs ; les noyaux de f', f'' étant finis, il en est évidemment de même de ceux de h'_0, h''_0, donc aussi de ceux de h', h''.

Ceci dit, passons à la démonstration de la proposition 7 ; soit H un groupe algébrique connexe qui admet des isogénies h' et h'' sur G' et G'' respectivement telles que $f' \circ h' = f'' \circ h''$; soit T_H le tore maximal de H tel que

$$(f' \circ h')(T_H) = (f'' \circ h'')(T_H) = T \ ;$$

on a évidemment $h'(T_H) = T'$, $h''(T_H) = T''$. Soient η', η'' les isomorphismes de $X^{\mathbf{Q}}(T')$ et $X^{\mathbf{Q}}(T'')$ sur $X^{\mathbf{Q}}(T_H)$ associés respectivement à h', h'' ; on a donc $\eta' \circ \varphi' = \eta'' \circ \varphi''$, d'où $\eta' \circ \gamma \circ \varphi'' = \eta'' \circ \varphi''$ et par suite $\eta' \circ \gamma = \eta''$. Il résulte de la proposition 6 qu'il existe une isogénie $g : G' \to G''$ telle que $g \circ h' = h''$, $g(T') = T''$ et que l'isomorphisme de $X^{\mathbf{Q}}(T'')$ sur $X^{\mathbf{Q}}(T')$ attaché à g soit γ. On a $f'' \circ g \circ h' = f'' \circ h'' = f' \circ h'$; comme h' est surjectif, on a $f'' \circ g = f'$. La seconde assertion de la proposition 7 résulte de la proposition 6.

19. Les diagrammes de Dynkin[1]

19.1 Le diagramme de Dynkin d'un groupe semi-simple

Soient G un groupe algébrique semi-simple, T un tore maximal de G, $X(T)$ le groupe des caractères rationnels de T, $(\alpha_1, \ldots, \alpha_n)$ l'ensemble des racines fondamentales de G par rapport à T et à un sous-groupe de Borel B contenant T (n° 13.3, définition 3) ; on note w_i la réflexion par rapport à α_i. On suppose l'espace vectoriel $X^{\mathbf{Q}}(T)$ muni d'une forme quadratique définie positive invariante par le groupe de Weyl, et on note $(\lambda \mid \mu)$ le produit scalaire relativement à cette forme quadratique. On a

$$w_i \cdot \alpha_j = \alpha_j + c(i,j)\,\alpha_i\,,$$

les $c(i,j)$ étant des entiers que l'on appelle les *entiers de Cartan* ; on a

$$c(i,i) = -2\,, \quad c(i,j) \geq 0 \quad \text{si } i \neq j\,,$$

$$c(i,j) = -2\,(\alpha_i \mid \alpha_j)\,(\alpha_i \mid \alpha_i)^{-1}\ ;$$

il en résulte que, si $c(i,j) \neq 0$, d'où $c(j,i) \neq 0$, on a

$$c(i,j)\,(c(j,i))^{-1} = (\alpha_j \mid \alpha_j)\,(\alpha_i \mid \alpha_i)^{-1}\,.$$

On appelle *diagramme de Dynkin* du groupe G un objet constitué par un graphe à n sommets $S_1, \ldots, S_n$ et par des nombres σ_i attachés à ces sommets et qui se décrit de la manière suivante : si $i \neq j$, S_i et S_j sont joints par une arête du graphe si et seulement si $c(i,j) \neq 0$, *i.e.* si et seulement si $(\alpha_i \mid \alpha_j) \neq 0$; dans ce cas, S_i et S_j ne sont joints que par une seule arête ; il n'y a aucune arête du graphe dont les extrémités coïncident avec un même sommet ; si C est l'ensemble des sommets d'une composante connexe du graphe, les nombres σ_i relatifs aux sommets $S_i \in C$ sont proportionnels aux $(\alpha_i \mid \alpha_i)$, le facteur de proportionalité étant tel que le plus petit des σ_i pour $S_i \in C$ soit 1.

Le diagramme de Dynkin est déterminé à un isomorphisme près par le groupe G. Cela résulte facilement des faits suivants : deux tores maximaux de G peuvent se déduire l'un de l'autre par un automorphisme intérieur de G ; une fois T fixé, deux systèmes de racines fondamentales peuvent se déduire

[1] Exposé de C. Chevalley, le 9.12.1957

l'un de l'autre par une opération du groupe de Weyl[2] ; si S_i et S_j sont des sommets qui sont les extrémités d'une arête, on a

$$\sigma_j \, \sigma_i^{-1} = c(i,j) \, (c(j,i))^{-1} , \tag{1}$$

ce qui montre que la connaissance des entiers de Cartan détermine les rapports mutuels des σ_i relatifs aux sommets S_i d'une même composante connexe du diagramme.

Réciproquement, la connaissance du diagramme de Dynkin permet de calculer les entiers de Cartan. En effet, on a $c(i,i) = -2$, $c(i,j) = 0$ si S_i, S_j sont des sommets distincts qui ne sont les extrémités d'aucune arête ; enfin, si S_i et S_j sont les extrémités d'une arête, les entiers $c(i,j)$, $c(j,i)$ sont déterminés par la formule (1) et par le fait que ce sont des entiers > 0 dont le produit est < 4.

19.2 Diagrammes admissibles

Définition 1. – *Nous appellerons* diagramme admissible *un objet constitué par un graphe fini et par des nombres $\sigma_i > 0$ associés aux sommets $S_1, \ldots, S_n$ du graphe qui possède les propriétés suivantes :*

1) *deux sommets distincts ne sont jamais joints par plus d'une arête ; aucune arête n'a ses extrémités confondues en un même sommet ;*

2) *pour chaque composante connexe C du graphe, le plus petit des nombres σ_i attachés aux sommets de C est 1 ;*

3) *si S_i et S_j sont les extrémités d'une arête du graphe, $\sigma_j \, \sigma_i^{-1}$ se met sous la forme $c(i,j) \, (c(j,i))^{-1}$ où $c(i,j)$, $c(j,i)$ sont des entiers > 0 de produit < 4 ;*

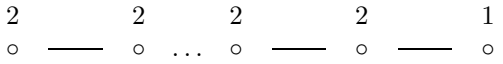
4) *posant de plus $c(i,i) = -2$, $c(i,j) = 0$ si S_i et S_j sont des sommets distincts qui ne sont liés par aucune arête, il existe un espace vectoriel V sur le corps des nombres rationnels de dimension égale au nombre des sommets, une base $(\alpha_1, \ldots, \alpha_n)$ de V et une forme quadratique définie positive sur V tels que l'on ait $c(i,j) = -2 \, (\alpha_i \mid \alpha_j) \, (\alpha_i \mid \alpha_i)^{-1}$ pour tout couple (i,j).*

Il est clair que les composantes connexes d'un diagramme admissible sont encore des diagrammes admissibles. On peut déterminer tous les diagrammes admissibles connexes (*cf.* Séminaire Sophus Lie, 1954/55, exposé 13) : on trouve les types suivants, où l'indice désigne le nombre de sommets (par exemple E_6 a 6 sommets) :

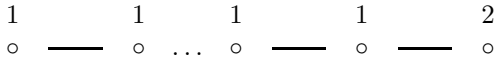
[2] En effet, d'après le corollaire 3 du théorème 1 du n° 9.3, deux sous-groupes de Borel B_1 et B_2 de G contenant T se déduisent l'un de l'autre par une opération du groupe de Weyl de T.

Type A_n $(n \geq 1)$:

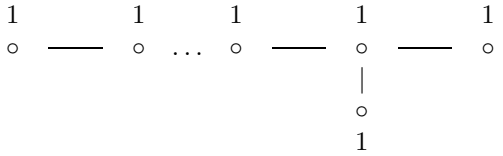
Type B_n $(n \geq 3)$:



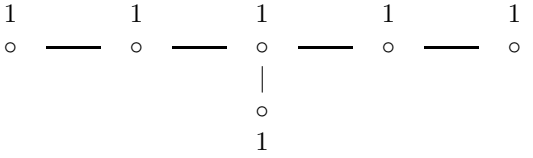
Type C_n $(n \geq 2)$:



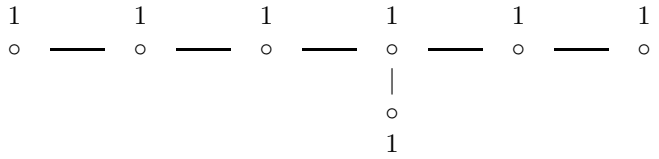
Type D_n $(n \geq 4)$:



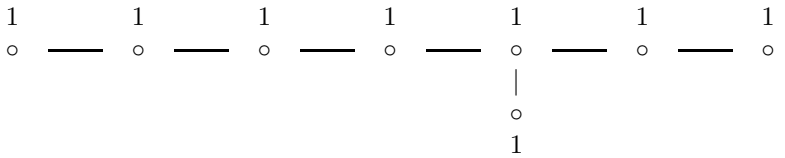
Type E_6 :



Type E_7 :



Type E_8 :



Type F_4 :

Type G_2 :

Si un diagramme admissible se décompose en diagrammes connexes de types $T_1, \ldots, T_h$ (chaque T_k étant l'un des symboles A_n, B_n, C_n, D_n, E_6, E_7, E_8, F_4, G_2), nous dirons qu'il est de type $T_1 + \ldots + T_h$. Nous dirons qu'un groupe semi-simple G est de type T si ses diagrammes de Dynkin sont de type T.

19.3 Système de racines associé à un diagramme admissible

Considérons un diagramme admissible D; utilisons les mêmes notations que dans la définition 1. Pour chaque i, les formules $w_i \cdot \alpha_j = \alpha_j + c(i,j)\alpha_i$ définissent un automorphisme w_i d'ordre 2 de V qui laisse invariante la métrique de l'espace V. Comme les matrices qui représentent les w_i par rapport à la base $(\alpha_1, \ldots, \alpha_n)$ sont entières, le groupe W engendré par les w_i est fini ; il s'appelle le *groupe de Weyl du diagramme*. Les transformés des α_i par les opérations de W sont des combinaisons linéaires à coefficients entiers tous de même signe des α_i. Les transformés des α_i par toutes les opérations de W forment un ensemble fini dont les éléments s'appellent les *racines*. Par ailleurs, il y a une base $(\varpi_1, \ldots, \varpi_n)$ de V composée d'éléments ϖ_i tels que l'on ait

$$w_i \cdot \varpi_i = \varpi_i - \alpha_i \qquad w_i \cdot \varpi_j = \varpi_j \qquad \text{si } i \neq j \ ;$$

ces éléments s'appellent les *poids fondamentaux*.

Si l'on suppose que D est le diagramme de Dynkin d'un groupe G (relativement à un tore maximal T et à un système de racines fondamentales $(\alpha_1, \ldots, \alpha_n)$) et si l'on prend $V = X^{\mathbf{Q}}(T)$, les racines du diagramme sont celles du groupe, et les poids fondamentaux du diagramme sont ceux du groupe. Il en résulte que la connaissance du diagramme de Dynkin de G détermine les expressions des racines de G et de ses poids fondamentaux comme combinaisons linéaires des racines fondamentales. Par ailleurs, la connaissance du nombre des racines de G détermine la dimension de G en vertu du

Lemme 1. – *Si G est un groupe algébrique semi-simple et T un tore maximal de G,* $\dim G$ *est la somme de* $\dim T$ *et du nombre des racines.*

Choisissons en effet un groupe de Borel B de G contenant T, et désignons par B^u l'ensemble des éléments unipotents de B ; la dimension de B^u est alors égale au nombre N des racines qui sont < 0 sur la chambre de Weyl associée à B (théorème 1 du n° 13.2 et proposition 1 du n° 13.1). Par ailleurs, la dimension de G/B est égale à celle de B^u (corollaire 2 au théorème 3 du n° 13.4) ; comme

$$\dim B = \dim B^u + \dim T\,,$$

on a $\dim G = \dim B + \dim G/B = 2\dim B^u + \dim T = 2N + \dim T$; or $2N$ est le nombre de toutes les racines.

Nous appellerons *dimension de groupe* d'un diagramme admissible D la somme du nombre des sommets de D et du nombre des racines de D.

19.4 Racines et poids fondamentaux des divers types

I. *Type* A_n. La dimension de groupe est $(n+1)^2 - 1$. Il existe $n+1$ éléments ω_i de V tels que

$$\alpha_i = \omega_i - \omega_{i+1} \quad (1 \leq i \leq n)\,, \qquad \sum_{i=1}^{n+1} \omega_i = 0 \ ;$$

on a

$$\omega_k = (n+1)^{-1}\Big(-\sum_{i=1}^{k-1} i\,\alpha_i + \sum_{i=k}^{n}(n-i+1)\alpha_i\Big)\,.$$

L'opération w_i échange ω_i et ω_{i+1} en laissant ω_j fixe si $j \neq i,\ i+1$; le groupe W se compose des automorphismes de V qui permutent entre eux les éléments ω_i de toutes les manières possibles. Les racines sont les $\pm \sum_{k\leq i\leq k'} \alpha_i$ pour $1 \leq k \leq k' \leq n$; ce sont aussi les $\omega_i - \omega_j$ pour $i \neq j$. Les poids fondamentaux sont les

$$\varpi_k = \omega_1 + \ldots + \omega_k \qquad (1 \leq k \leq n) \ ;$$

on a aussi

$$\varpi_k = (n+1)^{-1}\,(n+1-k)\sum_{i=1}^{k-1} i\,\alpha_i + (n+1)^{-1}\,k\sum_{i=k}^{n}(n-i+1)\,\alpha_i\,.$$

II. *Type* B_n. La dimension de groupe est $n(2n+1)$. Il existe une base $(\omega_1, \ldots, \omega_n)$ de V telle que

$$\alpha_i = \omega_i - \omega_{i+1} \quad (1 \leq i \leq n-1)\,, \qquad \alpha_n = \omega_n \ ;$$

on a

$$\omega_k = \sum_{i=k}^{n} \alpha_i\,.$$

Si $i < n$, w_i échange ω_i et ω_{i+1} et laisse fixe ω_j si $j \neq i,\ i+1$; l'opération w_n change ω_n en $-\omega_n$ et laisse ω_i fixe si $i \neq n$. Le groupe W se compose des automorphismes de V définis par les formules

$$w \cdot \omega_i = e(i)\, \omega_{\pi(i)}$$

où π est une permutation quelconque de $\{1, \ldots, n\}$ et où les $e(i)$ sont des entiers égaux à ± 1. Les racines sont les

$$\omega_i - \omega_j \quad (i \neq j)\,, \qquad \pm\omega_i\,,\ \pm(\omega_i + \omega_j) \quad (i \neq j)\,.$$

Les poids fondamentaux sont

$$\varpi_k = \omega_1 + \ldots + \omega_k \quad (1 \leq k < n)\ ,\ \varpi_n = \tfrac{1}{2} \textstyle\sum_{i=1}^{n} \omega_i\ ;$$

on a

$$\varpi_k = \sum_{i=1}^{k} i\, \alpha_i + k \sum_{i=k+1}^{n} \alpha_i\ (1 \leq k < n)\,,\ \varpi_n = \tfrac{1}{2} \textstyle\sum_{i=1}^{n} i\, \alpha_i\,.$$

III. *Type* C_n. La dimension de groupe est $n(2n+1)$. Il existe une base $(\omega_1, \ldots, \omega_n)$ de V telle que

$$\alpha_i = \omega_i - \omega_{i+1} \quad (1 \leq i < n)\,, \qquad \alpha_n = 2\,\omega_n\,.$$

Si $i < n$, w_i échange ω_i et ω_{i+1} et laisse fixe ω_j si $j \neq i,\ i+1$; l'opération w_n change ω_n en $-\omega_n$ et laisse ω_i fixe si $i \neq n$. Le groupe W se compose des automorphismes de V définis par les formules

$$w \cdot \omega_i = e(i)\, \omega_{\pi(i)}$$

où π est une permutation quelconque de $\{1, \ldots, n\}$ et où les $e(i)$ sont des entiers égaux à ± 1. Les racines sont les

$$\omega_i - \omega_j \quad (i \neq j)\,, \qquad \pm 2\omega_i\,, \quad \pm(\omega_i + \omega_j) \quad (i \neq j)\,.$$

Les poids fondamentaux sont

$$\varpi_k = \omega_1 + \ldots + \omega_k \quad (1 \leq k \leq n)\ ;$$

on a

$$\varpi_k = \sum_{i=1}^{k} i\, \alpha_i + k \sum_{i=k+1}^{n-1} \alpha_i + \tfrac{1}{2} k\, \alpha_n \qquad (1 \leq k < n)$$

$$\varpi_n = \sum_{i=1}^{n-1} i\, \alpha_i + \tfrac{1}{2}\, n\, \alpha_n\,.$$

IV. *Type* D_n. La dimension de groupe est $n(2n-1)$. Il existe une base $(\omega_1, \ldots, \omega_n)$ de V telle que

$$\alpha_i = \omega_i - \omega_{i+1} \quad (1 \leq i < n) \qquad \alpha_n = \omega_{n-1} + \omega_n\,.$$

Si $i < n$, w_i échange ω_i et ω_{i+1} et laisse ω_j fixe si $j \neq i, i+1$; l'opération w_n transforme ω_{n-1} en $-\omega_n$, ω_n en $-\omega_{n-1}$ et laisse ω_i fixe si $i \neq n-1, n$. Le groupe W se compose des automorphismes de V définis par les formules

$$w \cdot \omega_i = e(i)\, \omega_{\pi(i)}$$

où π est une permutation quelconque de $\{1, \ldots, n\}$ et où les $e(i)$ sont des entiers égaux à ± 1, avec $\prod_{i=1}^{n} e(i) = 1$. Les racines sont les

$$\omega_i - \omega_j \quad (i \neq j), \quad \pm(\omega_i + \omega_j) \quad (i \neq j)\,.$$

Les poids fondamentaux sont

$$\varpi_k = \omega_1 + \ldots + \omega_k \ (1 \leq k \leq n-2)\,,$$

$$\varpi_{n-1} = \tfrac{1}{2} \sum_{i=1}^{n} \omega_i - \omega_n$$

$$\varpi_n = \tfrac{1}{2} \sum_{i=1}^{n} \omega_i\,;$$

on a

$$\varpi_k = \sum_{i=1}^{k} i\, \alpha_i + k \sum_{i=k+1}^{n-2} \alpha_i + \tfrac{1}{2}\, k\, (\alpha_{n-1} + \alpha_n) \quad (1 \leq k \leq n-2)$$

$$\varpi_{n-1} = \tfrac{1}{2} \sum_{i=1}^{n-2} i\, \alpha_i + \tfrac{1}{4}\, n\, \alpha_{n-1} + \tfrac{1}{4}(n-2)\, \alpha_n$$

$$\varpi_n = \tfrac{1}{2} \sum_{i=1}^{n-2} i\, \alpha_i + \tfrac{1}{4}(n-2)\, \alpha_{n-1} + \tfrac{1}{4}\, n\, \alpha_n\,.$$

V. *Type* E_6. La dimension de groupe est 78. Il existe une base $(\omega_1, \ldots, \omega_6)$ de l'espace V telle que

$$\alpha_i = \omega_i - \omega_{i+1} \quad (1 \leq i \leq 5)\,, \qquad \alpha_6 = \omega_4 + \omega_5 + \omega_6 - s$$

où l'on a posé $s = \frac{1}{3} \sum_{i=1}^{6} \omega_i$. Si $1 \leq i \leq 5$, w_i échange ω_i et ω_{i+1} et laisse ω_j fixe si $j \neq i, i+1$; l'opération w_6 laisse ω_i fixe si $i \leq 3$ et change ω_i en $\omega_i - \alpha_6$ si $i \geq 4$, et donc s en $s - \alpha_6$. Les racines sont les

$$\omega_i - \omega_j \ (i \neq j), \quad \pm(\omega_i + \omega_j + \omega_k - s) \ (i, j, k \text{ distincts}), \ \pm s\,.$$

On peut munir l'espace V d'une forme quadratique définie positive invariante par W telle que l'on ait $(\omega_i \mid \omega_i) = 4/3$, $(\omega_i \mid \omega_j) = 1/3$ si $i \neq j$, d'où

$(\omega_i \mid s) = 1$, $(s \mid s) = 2$, $(\alpha \mid \alpha) = 2$ pour toute racine α. Les racines orthogonales à s sont les $\omega_i - \omega_j$ $(i \neq j)$; elles forment un système isomorphe au système de racines d'un diagramme de type A_5. Les opérations de W qui permutent entre elles les racines $\omega_i - \omega_j$ forment un groupe W' qui contient le groupe W'' engendré par les réflexions par rapport aux $\omega_i - \omega_j$ et aussi la réflexion par rapport à s ; on déduit facilement du fait qu'un diagramme de Dynkin de type A_5 n'admet que deux automorphismes que W'' est d'indice 2 ou 4 dans W'. Si cet indice était 4, W' contiendrait l'opération w' qui transforme s en s et $\omega_i - \omega_j$ en $\omega_{7-j} - \omega_{7-i}$; or w' permute $\alpha_1, \ldots, \alpha_6$ entre elles de manière non triviale[3] et n'appartient par suite pas à W'. Donc W'' est d'indice 2 dans W'. Comme W'' est d'ordre 6!, W' est d'ordre $2 \cdot 6!$. Par ailleurs, les seules racines qui sont orthogonales à toutes les $\omega_i - \omega_j$ sont s et $-s$; on en déduit tout de suite[4] que l'ordre de W est $\frac{1}{2} \cdot 72 \cdot 2 \cdot 6! = 72 \cdot 6!$. Les poids fondamentaux sont

$$\varpi_1 = \omega_1 = \tfrac{1}{3}(4\alpha_1 + 5\alpha_2 + 6\alpha_3 + 4\alpha_4 + 2\alpha_5) + \alpha_6$$

$$\varpi_2 = \omega_1 + \omega_2 = \tfrac{1}{3}(5\alpha_1 + 10\alpha_2 + 12\alpha_3 + 8\alpha_4 + 4\alpha_5) + 2\alpha_6$$

$$\varpi_3 = \omega_1 + \omega_2 + \omega_3 = 2\alpha_1 + 4\alpha_2 + 6\alpha_3 + 4\alpha_4 + 2\alpha_5 + 3\alpha_6$$

$$\varpi_4 = \omega_1 + \omega_2 + \omega_3 + \omega_4 - s = \tfrac{1}{3}(4\alpha_1 + 8\alpha_2 + 12\alpha_3 + 10\alpha_4 + 5\alpha_5) + 2\alpha_6$$

$$\varpi_5 = \omega_1 + \omega_2 + \omega_3 + \omega_4 + \omega_5 - 2s = \tfrac{1}{3}(2\alpha_1 + 4\alpha_2 + 6\alpha_3 + 5\alpha_4 + 4\alpha_5) + \alpha_6$$

$$\varpi_6 = s = \alpha_1 + 2\alpha_2 + 3\alpha_3 + 2\alpha_4 + \alpha_5 + 2\alpha_6\,.$$

Les transformés de $\varpi_1 = \omega_1$ par les opérations de W sont les

$$\omega_i\,,\ \omega_i - s\,,\ s - (\omega_i + \omega_j) \qquad (i \neq j)\ ;$$

le nombre de ces transformés est 27 ; parmi eux ne figure pas $-\omega_1$, ce qui montre que l'automorphisme $\omega \to -\omega$ de V n'appartient pas au groupe de Weyl.

VI. *Type* E_7. La dimension de groupe est 133. Il existe une base $(\omega_1, \ldots, \omega_7)$ de l'espace V telle que l'on ait

$$\alpha_i = \omega_i - \omega_{i+1} \quad (1 \leq i \leq 6)\,, \qquad \alpha_7 = \omega_5 + \omega_6 + \omega_7 - s$$

où $s = \frac{1}{3} \sum_{i=1}^{7} \omega_i$. Si $i \leq 6$, w_i échange ω_i et ω_{i+1} et laisse ω_j fixe si $j \neq i$, $i+1$. L'opération w_7 transforme ω_i en lui-même si $i \leq 4$ et en $\omega_i - \alpha_7$ si $i \geq 5$. Les racines sont les

$$\omega_i - \omega_j\ (i \neq j), \quad \pm(\omega_i + \omega_j + \omega_k - s)\ (i, j, k \text{ distincts}) \text{ et } \pm\,(s - \omega_i)\,.$$

[3] En envoyant α_i sur α_{6-i} pour $1 \leq i \leq 5$ et α_6 sur α_6.

[4] En effet, W'' est le stabilisateur de s dans W, et W opère transitivement sur l'ensemble des racines (au nombre de 72).

On peut munir l'espace V d'une forme quadratique définie positive invariante par W en posant $(\omega_i \mid \omega_i) = 3/2$, $(\omega_i \mid \omega_j) = 1/2$ si $i \neq j$; on a $(\omega_i \mid s) = 3/2$, $(s \mid s) = 7/2$, $(\alpha \mid \alpha) = 2$ pour toute racine α. Les racines α telles que $(\omega_1 \mid \alpha) = 0$ sont toutes celles qui sont combinaisons linéaires de $\alpha_2, \ldots, \alpha_7$; leur ensemble est isomorphe à l'ensemble des racines d'un diagramme de type E_6. Les opérations de W qui permutent ces racines entre elles forment un groupe W' qui contient le groupe W'' engendré par les réflexions par rapport aux racines $\alpha_2, \ldots, \alpha_7$; ce dernier est isomorphe au groupe de Weyl d'un diagramme de type E_6. On déduit du fait qu'un diagramme de type E_6 n'admet que deux automorphismes que l'indice de W'' dans W' est 1, 2 ou 4. Par ailleurs, l'homothétie w_0 de rapport -1 de V permute entre elles les racines ; on en déduit qu'il existe une opération w_0' de W telle que $w_0' w_0$ permute entre elles les α_i $(1 \leq i \leq 7)$; comme un diagramme de type E_7 n'admet aucun automorphisme distinct de l'identité, $w_0' w_0$ est l'identité, d'où $w_0 \in W$. Or nous avons vu dans l'étude du type E_6 que w_0 ne peut appartenir à W'' ; de plus, on voit facilement qu'il n'y a aucune opération de W qui change ω_1 en $-\omega_1$ et qui conserve $\alpha_2, \ldots, \alpha_7$; W'' est donc d'indice 2 dans W'. Les transformés de ω_1 par les opérations du groupe de Weyl sont les $\pm\omega_i$, $\pm(s - \omega_i - \omega_j)$ $(i \neq j)$; leur nombre est 56, et, parmi eux, les seuls qui soient orthogonaux à $\alpha_2, \ldots, \alpha_7$ sont $\pm\omega_1$. On en conclut que l'indice de W' dans W est $\frac{1}{2} \cdot 56$ et que l'ordre de W est $56 \cdot 72 \cdot 6!$

Les poids fondamentaux sont

$$\varpi_1 = \omega_1 = \tfrac{1}{2}(3\alpha_1 + 4\alpha_2 + 5\alpha_3 + 6\alpha_4 + 4\alpha_5 + 2\alpha_6 + 3\alpha_7)$$

$$\varpi_2 = \omega_1 + \omega_2 = 2\alpha_1 + 4\alpha_2 + 5\alpha_3 + 6\alpha_4 + 4\alpha_5 + 2\alpha_6 + 3\alpha_7$$

$$\varpi_3 = \omega_1 + \omega_2 + \omega_3 = \tfrac{1}{2}(5\alpha_1 + 10\alpha_2 + 15\alpha_3 + 18\alpha_4 + 12\alpha_5 + 6\alpha_6 + 9\alpha_7)$$

$$\varpi_4 = \omega_1 + \omega_2 + \omega_3 + \omega_4 = 3\alpha_1 + 6\alpha_2 + 9\alpha_3 + 12\alpha_4 + 8\alpha_5 + 4\alpha_6 + 6\alpha_7$$

$$\varpi_5 = \omega_1 + \omega_2 + \omega_3 + \omega_4 + \omega_5 - s = 2\alpha_1 + 4\alpha_2 + 6\alpha_3 + 8\alpha_4 + 6\alpha_5 + 3\alpha_6 + 4\alpha_7$$

$$\varpi_6 = s - \omega_7 = \alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 3\alpha_5 + 2\alpha_6 + 2\alpha_7$$

$$\varpi_7 = s = \tfrac{1}{2}(3\alpha_1 + 6\alpha_2 + 9\alpha_3 + 12\alpha_4 + 8\alpha_5 + 4\alpha_6 + 7\alpha_7)\,.$$

VII. *Type* E_8. La dimension de groupe est 248. L'espace V est engendré par 9 éléments ω_i $(1 \leq i \leq 9)$ dont la somme est nulle tels que

$$\alpha_i = \omega_i - \omega_{i+1} \quad (1 \leq i \leq 7)\,, \qquad \alpha_8 = \omega_6 + \omega_7 + \omega_8\,.$$

Si $i \leq 7$, w_i échange ω_i et ω_{i+1} et laisse ω_j fixe si $j \neq i$, $i+1$. L'opération w_8 transforme ω_i en $\omega_i + \frac{1}{3}\alpha_8$ si $i \neq 6, 7, 8$, en $\omega_i - \frac{2}{3}\alpha_8$ si $i = 6, 7$ ou 8. Les racines sont les

$$\omega_i - \omega_j,\ (i \neq j), \quad \pm(\omega_i + \omega_j + \omega_k)\ (i, j, k \text{ distincts})\,.$$

On peut munir l'espace V d'une forme quadratique définie positive invariante par W en posant $(\omega_i \mid \omega_i) = 8/9$, $(\omega_i \mid \omega_j) = -1/9$ si $i \neq j$; on a

$(\alpha \mid \alpha) = 2$ pour toute racine α. Les racines orthogonales à $\omega_1 - \omega_9$ sont celles qui expriment comme combinaisons linéaires de $\alpha_2, \dots, \alpha_8$; elles forment un système de racines isomorphe à l'ensemble des racines d'un diagramme de type E_7. Les opérations de W qui permutent ces racines entre elles forment un groupe W' ; comme le groupe de Weyl d'un diagramme de type E_7 n'admet aucun automorphisme distinct de l'identité, W' contient le groupe engendré par les réflexions par rapport à $\alpha_2, \dots, \alpha_8$ comme sous-groupe d'indice 2. Il en résulte[5] que l'ordre de W est $240 \cdot 56 \cdot 72 \cdot 6!$. Les poids fondamentaux sont

$$\varpi_1 = \omega_1 - \omega_9 = 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 5\alpha_4 + 6\alpha_5 + 4\alpha_6 + 2\alpha_7 + 3\alpha_8$$

$$\varpi_2 = \omega_1 + \omega_2 - 2\omega_9 = 3\alpha_1 + 6\alpha_2 + 8\alpha_3 + 10\alpha_4 + 12\alpha_5 + 8\alpha_6 + 4\alpha_7 + 6\alpha_8$$

$$\varpi_3 = \omega_1 + \omega_2 + \omega_3 - 3\omega_9 = 4\alpha_1 + 8\alpha_2 + 12\alpha_3 + 15\alpha_4 + 18\alpha_5 + 12\alpha_6 + 6\alpha_7 + 9\alpha_8$$

$$\begin{aligned}\varpi_4 &= \omega_1 + \omega_2 + \omega_3 + \omega_4 - 4\omega_9 \\ &= 5\alpha_1 + 10\alpha_2 + 15\alpha_3 + 20\alpha_4 + 24\alpha_5 + 16\alpha_6 + 8\alpha_7 + 12\alpha_8\end{aligned}$$

$$\begin{aligned}\varpi_5 &= \omega_1 + \omega_2 + \omega_3 + \omega_4 + \omega_5 - 5\omega_9 \\ &= 6\alpha_1 + 12\alpha_2 + 18\alpha_3 + 24\alpha_4 + 30\alpha_5 + 20\alpha_6 + 10\alpha_7 + 15\alpha_8\end{aligned}$$

$$\varpi_6 = -\omega_7 - \omega_8 - 4\omega_9 = 4\alpha_1 + 8\alpha_2 + 12\alpha_3 + 16\alpha_4 + 20\alpha_5 + 14\alpha_6 + 7\alpha_7 + 10\alpha_8$$

$$\varpi_7 = -\omega_8 - 2\omega_9 = 2\alpha_1 + 4\alpha_2 + 6\alpha_3 + 8\alpha_4 + 10\alpha_5 + 7\alpha_6 + 4\alpha_7 + 5\alpha_8$$

$$\varpi_8 = -3\omega_9 = 3\alpha_1 + 6\alpha_2 + 9\alpha_3 + 12\alpha_4 + 15\alpha_5 + 10\alpha_6 + 5\alpha_7 + 8\alpha_8\,.$$

VIII. *Type* F_4. La dimension de groupe est 52. L'espace V a une base $(\omega_1, \dots, \omega_4)$ telle que

$$\alpha_1 = \omega_1 - \omega_2\,, \qquad \alpha_2 = \omega_2 - \omega_3\,, \qquad \alpha_3 = \omega_3$$

$$\alpha_4 = \tfrac{1}{2}(\omega_4 - \omega_1 - \omega_2 - \omega_3)\,.$$

Si $i = 1$ ou 2, w_i échange ω_i et ω_{i+1} et laisse ω_j fixe si $j \neq i, i+1$; l'opération w_3 change ω_3 en $-\omega_3$ et laisse ω_i fixe si $i \neq 3$. L'opération w_4 change ω_i en $\omega_i + \alpha_4$ si $i = 1$, 2 ou 3 et change ω_4 en $\omega_4 - \alpha_4$. Les racines sont les

$$\omega_i - \omega_j \ (i \neq j), \quad \pm\omega_i, \ \pm(\omega_i + \omega_j) \ (i \neq j) \text{ et } \tfrac{1}{2} \textstyle\sum_{i=1}^{4} e(i)\,\omega_i\,,$$

où les $e(i)$ sont des entiers égaux à ± 1. On peut munir l'espace V d'une forme quadratique définie positive invariante par W en posant $(\omega_i \mid \omega_i) = 1$, $(\omega_i \mid \omega_j) = 0$ si $i \neq j$. Les seules racines α telles que $(\alpha \mid \alpha) = 2$ sont les $\omega_i - \omega_j$, $\pm(\omega_i + \omega_j)$; ces racines sont donc permutées entre elles par les opérations de W. Elles forment un système de racines isomorphe à l'ensemble des racines d'un diagramme de type D_4. Soit W' le groupe engendré par les

[5] Car W opère transitivement sur l'ensemble des 240 racines, et le stabilisateur W' de la racine $\omega_1 - \omega_9$ est isomorphe au groupe de Weyl de type E_7, d'ordre $56 \times 72 \times 6$!.

réflexions par rapport à ces racines ; comme le groupe des automorphismes d'un diagramme de type D_4 est d'ordre 6, l'indice de W' dans W est un diviseur de 6. Or la réflexion par rapport à ω_4 conserve $\omega_1 - \omega_2$ et $\omega_2 - \omega_3$ et échange $\omega_3 - \omega_4$ avec $\omega_3 + \omega_4$; par ailleurs, la réflexion par rapport à la racine $\frac{1}{2}(\omega_1 - \omega_2 - \omega_3 + \omega_4)$ conserve $\omega_2 - \omega_3$ et $\omega_3 + \omega_4$ et échange $\omega_1 - \omega_2$ avec $\omega_3 - \omega_4$. Il en résulte facilement que W' est d'indice 6 dans W, donc que W est d'ordre $6 \cdot 2^3 \cdot 4!$. Les poids fondamentaux sont

$$\varpi_1 = \omega_1 + \omega_4 = 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 2\alpha_4$$

$$\varpi_2 = \omega_1 + \omega_2 + 2\omega_4 = 3\alpha_1 + 6\alpha_2 + 8\alpha_3 + 4\alpha_4$$

$$\varpi_3 = \tfrac{1}{2}(\omega_1 + \omega_2 + \omega_3 + 3\omega_4) = 2\alpha_1 + 4\alpha_2 + 6\alpha_3 + 3\alpha_4$$

$$\varpi_4 = \omega_4 = \alpha_1 + 2\alpha_2 + 3\alpha_3 + 2\alpha_4 \,.$$

IX. *Type* G_2. La dimension de groupe est 14. L'espace V est engendré par 3 éléments ω_0, ω_1, ω_2 de somme nulle tels que

$$\alpha_1 = \omega_0 \,, \qquad \alpha_2 = \omega_1 - \omega_0 \,.$$

L'opération w_1 change ω_0 en $-\omega_0$ et ω_1 en $\omega_1 + \omega_0$; l'opération w_2 change ω_0 en ω_1, ω_1 en ω_0. Les racines sont les

$$\pm\omega_i, \ \omega_i - \omega_j \ (i \neq j) \,.$$

On définit une forme quadratique définie positive invariante par le groupe de Weyl en posant $(\omega_i \mid \omega_i) = 1$, $(\omega_i \mid \omega_j) = -1/2$ si $i \neq j$. Les opérations de W sont les automorphismes w définis par $w \cdot \omega_i = e\,\omega_{\pi(i)}$, où π est une permutation de $\{0, 1, 2\}$ et $e = \pm 1$; W est donc d'ordre 12. Les poids fondamentaux sont

$$\varpi_1 = \omega_0 + \omega_1 = 2\alpha_1 + \alpha_2$$

$$\varpi_2 = \omega_1 - \omega_2 = 3\alpha_1 + 2\alpha_2 \,.$$

20. Les groupes de type A_n [1]

20.1 Le groupe SL(V)

Soit V un espace vectoriel de dimension finie sur K ; nous supposerons V de dimension $n+1 > 1$. Soit $\mathrm{SL}(V)$ le groupe des automorphismes de déterminant 1 de V. Le groupe $\mathrm{GL}(V)$ est, comme on le voit facilement, produit semi-direct de $\mathrm{SL}(V)$ et d'un groupe de dimension 1 ; comme $\mathrm{GL}(V)$ est connexe, on voit que $\mathrm{SL}(V)$ *est connexe. Montrons qu'il est semi-simple.* Il est bien connu que l'injection canonique $\mathrm{SL}(V) \to \mathrm{GL}(V)$ est une représentation simple de $\mathrm{SL}(V)$ et que le centre de $\mathrm{SL}(V)$ est fini ; notre assertion résultera donc du

Lemme 1. – *Soient V un espace vectoriel de dimension finie sur K et G un sous-groupe fermé connexe de* $\mathrm{GL}(V)$ *; si l'injection canonique $G \to \mathrm{GL}(V)$ est une représentation semi-simple de G, le radical de G est un tore qui est la composante neutre dans le centre de G.*

Soient R le radical de G et R^u l'ensemble des éléments unipotents de R. Représentons V comme somme directe de sous-espaces V_k stables par G qui fournissent des représentations simples de G. Pour chaque k, il existe un élément $x_k \neq 0$ de V_k qui est laissé fixe par les éléments de R^u (n° 6.2, théorème 2). Or il est clair que R^u est un sous-groupe invariant de G ; les éléments de V_k invariants par R^u forment donc un sous-espace stable par G et par suite identique à V_k. Ceci étant vrai pour tout k, R^u se réduit à son élément neutre. Il en résulte que R est un tore (n° 6.4, théorème 4) ; R étant invariant dans G, il est dans le centre de G (n° 4.3, corollaire de la proposition 2) ; le lemme 1 résulte immédiatement de là.

Soit $(x_1, \ldots, x_{n+1})$ une base de V. Les éléments s de $\mathrm{SL}(V)$ qui admettent chacun des x_i comme vecteur propre forment un groupe T ; si on pose $t \cdot x_i = \omega_i(t) x_i$ $(t \in T)$, on a $\prod_{i=1}^{n} \omega_i(t) = 1$, et, si $a_1, \ldots, a_{n+1}$ sont des éléments quelconques de K de produit égal à 1, il existe un élément $t \in T$ tel que $\omega_i(t) = a_i$ $(1 \leq i \leq n+1)$; si on choisit les a_i de manière qu'ils soient tous distincts, ce qui est manifestement possible, le centralisateur de l'élément t est T. Il résulte de là que T est un tore maximal de $\mathrm{SL}(V)$ et que le groupe $X(T)$ des caractères rationnels de T est engendré par les ω_i ; on a (en notation additive) $\sum_{i=1}^{n+1} \omega_i = 0$, et tout ensemble composé de n des éléments ω_i est une

[1] Exposé de C. Chevalley, le 16.12.1957

base du groupe $X(T)$. Soient i et j des indices distincts entre 1 et $n+1$; si $\xi \in K$, les formules

$$\tau_{ij}(\xi) \cdot x_i = x_i + \xi\, x_j\ ,$$

$$\tau_{ij}(\xi) \cdot x_k = x_k \quad \text{si} \quad k \neq i$$

définissent un élément $\tau_{ij}(\xi)$ de $\mathrm{SL}(V)$, et τ_{ij} est un isomorphisme du groupe additif K sur un sous-groupe de $\mathrm{SL}(V)$; on a si $t \in T$,

$$t\,\tau_{ij}(\xi)t^{-1} = \tau_{ij}(\omega_j(t)\,\omega_i^{-1}(t)\xi)\ ;$$

il s'ensuit que $\omega_j - \omega_i$ est une racine de $\mathrm{SL}(V)$ par rapport à T. Il est clair que l'on obtient ainsi $n(n+1)$ racines distinctes de $\mathrm{SL}(V)$; comme $\mathrm{SL}(V)$ est de dimension $(n+1)^2 - 1$ et T de dimension n, on a obtenu toutes les racines de $\mathrm{SL}(V)$ (n° 19.3, lemme 1). Il est clair que les racines $\alpha_i = \omega_i - \omega_{i+1}$ $(1 \leq i \leq n)$ forment un système fondamental, et que le diagramme de Dynkin correspondant est de type A_n. Le normalisateur de T dans $\mathrm{SL}(V)$ se compose des automorphismes $x_i \to b_i\, x_{\pi(i)}$ où π est une permutation de $\{1, \ldots, n+1\}$ et où les b_i ont pour produit la signature de π. Les éléments de $\mathrm{SL}(V)$ qui transforment en eux-mêmes tous les sous-espaces $\sum_{j=i}^{n+1} Kx_j$ de V $(1 \leq i \leq n+1)$ forment un groupe de Borel.

Soit f l'application canonique de $\mathrm{GL}(V)$ sur le groupe projectif $\mathrm{PL}(V)$ de l'espace V. C'est une isogénie dont les exposants radiciels sont tous égaux à 1 (n° 18.3, proposition 4) ; il résulte immédiatement de là que $\mathrm{PL}(V)$ est aussi de type A_n. Si $T' = f(T)$, et si φ est l'isomorphisme du groupe $X(T')$ des caractères rationnels de T' sur un sous-groupe de $X(T)$ qui est attaché à f, l'image de $X(T')$ par φ est engendrée par les rapports mutuels (en notation additive, les différences mutuelles) des ω_i ; le groupe $X(T')$ est donc engendré par les racines de $\mathrm{PL}(V)$.

Soit q une puissance de l'exposant caractéristique de K ; soit H le groupe algébrique qui a les mêmes éléments que $\mathrm{SL}(V)$ mais tel que les fonctions numériques sur H soient les puissances q-ièmes des fonctions numériques sur $\mathrm{SL}(V)$. Pour tout $s \in \mathrm{SL}(V)$, soit $M(s)$ la matrice qui représente s par rapport à la base $(x_1, \ldots, x_{n+1})$; l'application de $\mathrm{SL}(V)$ qui fait correspondre à tout s l'élément s' tel que les éléments de $M(s')$ soient les puissances q-ièmes de ceux de $M(s)$ est un isomorphisme[2] de $\mathrm{SL}(V)$ sur H.

20.2 Poids dominants minimaux

Soient G un groupe algébrique semi-simple, T un tore maximal de G et $(\alpha_1, \ldots, \alpha_n)$ un système fondamental de racines de G par rapport à T. On

[2] Souvent appelé *transformation de Frobenius*.

appelle *poids dominants* de G les poids dominants des représentations projectives simples de G. Désignant par $X(T)$ le groupe des caractères rationnels de T, on peut ordonner l'espace vectoriel $X^{\mathbf{Q}}(T)$ en convenant que les éléments positifs sont les combinaisons linéaires à coefficients tous positifs des α_i ; on appelle alors *poids dominants minimaux* les éléments minimaux de l'ensemble des poids dominants $\neq 0$ relativement à cette relation d'ordre.

Lemme 2. – *Introduisons une forme quadratique définie positive invariante par le groupe de Weyl W sur l'espace $X^{\mathbf{Q}}(T)$. Tout élément λ de $X^{\mathbf{Q}}(T)$ tel que l'on ait*[3] $(\lambda \mid \alpha_i) \geq 0$ *$(1 \leq i \leq n)$ est positif relativement à notre relation d'ordre.*

Ecrivons en effet : $\lambda = \sum_{i \in I'} c_i \alpha_i - \sum_{i \in I''} c_i \alpha_i$ où I' et I'' sont des ensembles disjoints et où les c_i sont ≥ 0. Tenant compte des relations $(\alpha_i \mid \alpha_j) \leq 0$ si $i \neq j$, on voit tout de suite que $\Big(\sum_{i \in I''} c_i \alpha_i \mid \alpha_j\Big) \leq 0$ pour tout $j \in I''$; il en résulte que $\Big(\sum_{i \in I''} c_i \alpha_i \mid \sum_{i \in I''} c_i \alpha_i\Big) \leq 0$, d'où $\sum_{i \in I''} c_i \alpha_i = 0$, ce qui démontre notre assertion. Si ϖ est un poids dominant et w_i la réflexion par rapport à α_i, on a $w_i(\varpi) = \varpi - e_i \alpha_i$ avec $e_i \geq 0$; il en résulte que $(\varpi \mid \alpha_i) \geq 0$, donc que ϖ est ≥ 0.

Corollaire. – *Les poids dominants minimaux sont des poids dominants fondamentaux*[4] *(mais, en général, les poids dominants fondamentaux ne sont pas tous minimaux).*

Lemme 3. – *Si λ est un élément quelconque de $X^{\mathbf{Q}}(T)$, il existe une opération w du groupe de Weyl tel que l'on ait*[3] $(w(\lambda) \mid \alpha_i) \geq 0$ *pour tout i, d'où $w(\lambda) \geq 0$.*

En effet, soit λ' un élément maximal (relativement à notre relation d'ordre) dans l'ensemble des transformés de λ par les opérations de W ; comme w_i est la réflexion par rapport à α_i, on a $w_i(\lambda') = \lambda' - m_i \alpha_i$, m_i étant un nombre rationnel ; il résulte du caractère maximal de λ' que les m_i sont tous ≥ 0, d'où $(\lambda' \mid \alpha_i) \geq 0$, ce qui démontre notre assertion.

Proposition 1. – *Soit ρ une représentation projective simple de G dont le poids dominant ϖ soit minimal. Les poids $\neq 0$ de ρ sont alors les transformés de ϖ par les opérations du groupe de Weyl W; ils sont tous de multiplicité* 1.

Soit en effet ϖ' un poids de ρ ; il existe une opération w de W telle que l'on ait $(w(\varpi') \mid \alpha_i) \geq 0$ $(1 \leq i \leq n)$ (lemme 3) ; on a donc $w_i(w(\varpi')) = w(\varpi') - e_i \alpha_i$, les e_i étant des nombres rationnels ≥ 0. Mais tout transformé

[3] L'ensemble $\mathcal{C}$ des λ dans $X^{\mathbf{Q}}(T)$ tels que l'on ait $(\lambda \mid \alpha_i) > 0$ pour $1 \leq i \leq n$ est une *chambre*. Les inégalités $(\lambda \mid \alpha_i) \geq 0$ $(1 \leq i \leq n)$ caractérisent donc l'adhérence $\overline{\mathcal{C}}$ de $\mathcal{C}$.

[4] Rappelons (fin du n° 16.3) que les poids dominants sont les combinaisons linéaires à coefficients entiers positifs des poids dominants fondamentaux.

de ϖ' par une opération de W est encore un poids de ρ, et les différences mutuelles des poids de ρ sont des combinaisons linéaires à coefficients entiers des racines (n° 16.2, propositions 1 et 2) ; les e_i sont donc entiers.

Il en résulte que, si $\varpi' \neq 0$, $w(\varpi')$ est un poids dominant ; comme $\varpi - w(\varpi')$ est ≥ 0 (*loc. cit.*), il résulte du caractère minimal de ϖ que $w(\varpi') = \varpi$. Il est clair que deux poids de ρ qui se déduisent l'un de l'autre par une opération de W ont même multiplicité ; comme ϖ est de multiplicité 1, il en est de même de ϖ'.

Corollaire. – *Les notations étant celles de la proposition* 1*, si l'on suppose de plus que ϖ n'est pas combinaison linéaire à coefficients entiers de $\alpha_1, \ldots, \alpha_n$, 0 n'est pas un poids de ρ et le degré de ρ est le nombre des transformés distincts de ϖ par les opérations de W.*

Cela résulte de ce que la différence entre deux poids de ρ est une combinaison linéaire à coefficients entiers des α_i (*loc. cit.*).

[On notera que nous appelons degré d'une représentation projective opérant dans l'espace projectif $P(V)$ associé à un espace vectoriel V la dimension de l'espace V et non pas celle de l'espace $P(V)$.]

Appliquons ceci aux divers types de diagrammes de Dynkin connexes. Nous utiliserons les notations[5] de l'exposé 19.

I. *Type A_n.* On reconnaît facilement que tous les poids dominants fondamentaux sont minimaux. Les transformés du k-ième poids dominant fondamental ϖ_k par les opérations de W sont tous les éléments $\omega_{i_1} + \ldots + \omega_{i_k}$ où $i_1, \ldots, i_k$ sont des indices distincts entre 1 et $n+1$. Aucun des poids ϖ_k n'est combinaison linéaire à coefficients entiers des racines ; si donc G est de type A_n, le degré de la représentation projective simple de poids dominant ϖ_k est le coefficient binomial $\binom{n+1}{k}$.

II. *Type B_n.* Les seuls poids dominants minimaux sont ϖ_1 et ϖ_n. Le poids ϖ_1 est combinaison linéaire à coefficients entiers des racines, mais il n'en est pas ainsi de ϖ_n. Les transformés de ϖ_n par les opérations de W sont les $\frac{1}{2} \sum_{i=1}^{n} e(i)\,\omega_i$, $e(i) = \pm 1$. Si donc G est de type B_n, la représentation projective simple de poids dominant ϖ_n de G est de degré 2^n.

III. *Type C_n.* Le seul poids dominant minimal est ϖ_1, qui n'est pas combinaison linéaire à coefficients entiers des racines. Ses transformés par les opérations de W sont les $\pm\omega_i$ $(1 \leq i \leq n)$. Si donc G est de type C_n, la représentation projective simple de poids dominant ϖ_1 de G est de degré $2n$.

IV. *Type D_n.* Les seuls poids dominants minimaux sont ϖ_1, ϖ_{n-1} et ϖ_n ; ϖ_1 n'est pas combinaison linéaire à coefficients entiers des racines ; ses transformés par les opérations de W sont les $\pm\omega_i$ $(1 \leq i \leq n)$. Donc, si G est de type D_n, la représentation projective simple de poids dominant ϖ_1 de G est

[5] Les poids dominants minimaux qui ne sont pas combinaisons linéaires à coefficients entiers de racines sont appelés "poids minuscules" par Bourbaki.

de degré $2n$; on voit facilement de la même manière que les représentations projectives simples de poids dominants ϖ_{n-1} et ϖ_n sont de degré 2^{n-1}.

V. *Type* E_6. Le poids ϖ_1 est minimal ; il n'est pas combinaison linéaire à coefficients entiers des racines et ses transformés par les opérations de W sont les ω_i, $\omega_i - s$, $s - (\omega_i + \omega_j)$ $(i \neq j)$; on en conclut que, si G est de type E_6, la représentation projective simple de poids dominant ϖ_1 de G est de degré 27. De la même manière, on voit que ϖ_5 est minimal, n'est pas combinaison linéaire à coefficients entiers des racines, et qu'il est le poids dominant d'une représentation projective simple de degré 27.

VI. *Type* E_7. Le poids ϖ_1 est le seul poids dominant minimal ; il n'est pas combinaison linéaire à coefficients entiers des racines ; ses transformés par les opérations de W sont les $\pm\omega_i$, $\pm(s-(\omega_i+\omega_j))$ $(i \neq j)$. On en conclut que, si G est de type E_7, la représentation projective simple de poids dominant ϖ_1 de G est de degré 56.

Dans le cas des types E_8, F_4, G_2, tous les poids dominants sont des combinaisons linéaires à coefficients entiers des racines.

20.3 Classification des groupes de type A_n

Lemme 4. – *Soit f un homomorphisme d'un groupe algébrique semi-simple G dans un groupe algébrique semi-simple G_1 ; soient T un tore maximal de G et T_1 un tore maximal de G_1 contenant $f(T)$. Soit φ l'application linéaire de $X^{\mathbf{Q}}(T_1)$ dans $X^{\mathbf{Q}}(T)$ qui fait correspondre à tout $\theta_1 \in X(T_1)$ le caractère rationnel $t \to \theta_1(f(t))$ de T. Soit σ une représentation linéaire ou projective de G_1 ; les poids de la représentation $\sigma \circ f$ de G sont alors les images par φ des poids de σ.*

L'homomorphisme σ (resp. $\sigma \circ f$) de G_1 (resp. G) dans $\sigma(G_1)$ définit une application linéaire ψ_1 (resp. ψ) de $X^{\mathbf{Q}}(\sigma(T_1))$ dans $X^{\mathbf{Q}}(T_1)$ (resp. $X^{\mathbf{Q}}(T)$) telle que l'on ait $(\psi_1(\overline{\theta}_1))(t_1) = \overline{\theta}_1(\sigma(t_1))$ (resp. $(\psi(\overline{\theta}_1))(t) = \overline{\theta}_1(\sigma(f(t)))$) pour tout $\overline{\theta}_1 \in X(\sigma(T_1))$ et tout $t_1 \in T_1$ (resp. $t \in T$) ; il est clair que $\psi = \varphi \circ \psi_1$. Dans le cas où σ est linéaire (resp. projective), elle opère dans un espace vectoriel V (resp. dans l'espace projectif $P(V)$ associé à un espace vectoriel V), et l'application identique de $\sigma(G_1)$ dans $\mathrm{GL}(V)$ (resp. $\mathrm{PL}(V)$) est une représentation linéaire (resp. projective) τ de $\sigma(G_1)$. Les poids de σ (resp. $\sigma \circ f$) sont par définition les images par ψ_1 (resp. ψ) de ceux de τ, ce qui démontre le lemme.

Corollaire. – *Les notations étant celles du lemme* 4, *supposons de plus que f soit une isogénie et que $\sigma \circ f$ soit une représentation (projective ou linéaire) simple de G dont le poids dominant (relativement à un système fondamental $(\alpha_1, \ldots, \alpha_n)$ de racines de G par rapport à T) soit le k-ième poids dominant fondamental ϖ_k* (i.e. *celui associé à la racine α_k). La racine α_k est alors l'image par φ d'une racine de G_1.*

En effet, il existe des racines α'_i de G_1 telles que $\varphi(\alpha'_i) = q_i\,\alpha_i$, les q_i étant des entiers > 0 ; ces racines forment un système fondamental de racines de G_1. Soient w_k et w'_k les réflexions par rapport à α_k et α'_k respectivement ; soit ϖ'_k l'élément de $X^{\mathbf{Q}}(T_1)$ tel que $\varphi(\varpi'_k) = \varpi_k$. On a donc $w_k(\varpi_k) = \varpi_k - \alpha_k$. Par ailleurs, on a $w_k \circ \varphi = \varphi \circ w'_k$ (n° 18.3, proposition 5) ; il en résulte que $w'_k(\varpi'_k) = \varpi'_k - q_k^{-1}\,\alpha'_k$. Par ailleurs, il résulte du lemme 4 que ϖ'_k est un poids d'une représentation (linéaire ou projective) de G_1 ; l'élément $\varpi'_k - w'_k(\varpi'_k)$, différence de deux poids d'une même représentation simple de G_1, est donc une combinaison linéaire à coefficients entiers des α'_i (n° 16.2, proposition 1). On en conclut $q_k = 1$, ce qui démontre le corollaire.

Soit n un entier > 0 ; nous désignerons par $(\overline{x}_1, \ldots, \overline{x}_{n+1})$ la base canonique de K^{n+1} et par $\overline{T}$ le tore maximal de $\mathrm{PL}(K^{n+1})$ composé des opérations qui laissent fixes les points $K\,\overline{x}_i$ de l'espace projectif $P(K^{n+1})$. A chaque $\overline{x}_i$ correspond un poids $\overline{\omega}_i$ de la représentation identique de $\mathrm{PL}(K^{n+1})$ sur lui-même ; si l'on pose $\overline{\alpha}_i = \overline{\omega}_i - \overline{\omega}_{i+1}$ $(1 \leq i \leq n)$, les $\overline{\alpha}_i$ forment un système fondamental de racines de $\mathrm{PL}(K^{n+1})$ par rapport à $\overline{T}$.

Soit G un groupe algébrique semi-simple de type A_n, et soit T un tore maximal de G ; soit $(\alpha_1, \ldots, \alpha_n)$ un système fondamental de racines de G par rapport à T tel que, dans le diagramme de Dynkin correspondant, les sommets correspondants à α_i et α_{i+1} (où $1 \leq i < n$) soient liés par une arête. Soient $\omega_1, \ldots, \omega_{n+1}$ des éléments de somme nulle de $X^{\mathbf{Q}}(T)$ tels que $\alpha_i = \omega_i - \omega_{i+1}$ $(1 \leq i \leq n)$; ω_1 est alors le poids dominant ϖ_1 d'une représentation projective simple ρ de G, opérant sur l'espace projectif $P(V)$ associé à un espace vectoriel V. On a vu au n° 20.2 que V est de dimension $n+1$ et que les poids de ρ sont les ω_i $(1 \leq i \leq n+1)$; soit x_i un point de V qui donne lieu au poids ω_i ; les éléments $x_1, \ldots, x_{n+1}$ forment alors une base de V. Par ailleurs, la dimension de G est $(n+1)^2 - 1$ (n° 19.3, lemme 1). Comme G est presque simple, ρ est une isogénie, d'où $\dim \rho(G) = \dim G = (n+1)^2 - 1 = \dim \mathrm{PL}(V)$; comme $\rho(G) \subset \mathrm{PL}(V)$, on a $\rho(G) = \mathrm{PL}(V)$. Le groupe $T' = \rho(T)$ est le groupe des opérations de $\mathrm{PL}(V)$ qui laissent fixe chacun des points $K\,x_i$; chaque x_i donne lieu à un poids ω'_i de la représentation de $\mathrm{PL}(V)$ constituée par son application identique sur lui-même. Soit φ' l'isomorphisme spécial de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(T)$ attaché à l'isogénie ρ ; on a alors $\varphi'(\omega'_i) = \omega_i$ (*cf.* la démonstration du lemme 4). Il existe un isomorphisme de V sur K^{n+1} qui applique x_i sur $\overline{x}_i$ $(1 \leq i \leq n+1)$; cet isomorphisme définit un isomorphisme h de $\mathrm{PL}(V)$ sur $\mathrm{PL}(K^{n+1})$, et $h \circ \rho$ est une isogénie f de G sur $\mathrm{PL}(K^{n+1})$. Si φ est l'isomorphisme spécial de $X^{\mathbf{Q}}(\overline{T})$ sur $X^{\mathbf{Q}}(T)$ attaché à f, il est clair que $\varphi(\overline{\omega}_i) = \omega_i$ $(1 \leq i \leq n+1)$, d'où $\varphi(\overline{\alpha}_i) = \alpha_i$ $(1 \leq i \leq n)$. Soit q une puissance de l'exposant caractéristique de K ; l'isogénie des puissances q-ièmes applique G sur un groupe $\widetilde{G}$. Faisant usage de l'isogénie de $\widetilde{G}$ sur $\mathrm{PL}(K^{n+1})$ qu'on vient de construire, on voit qu'il existe une isogénie de G sur $\mathrm{PL}(K^{n+1})$ telle que l'isomorphisme de $X^{\mathbf{Q}}(\overline{T})$ sur $X^{\mathbf{Q}}(T)$ attaché à cette isogénie applique $\overline{\alpha}_i$ sur $q\,\alpha_i$ $(1 \leq i \leq n)$.

Théorème 1. – *Soient G et G' des groupes algébriques semi-simples, T et T' des tores maximaux de G et G', $X(T)$ et $X(T')$ les groupes des caractères rationnels de G et G' et φ un isomorphisme spécial de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(T)$. Si l'un au moins des groupes G, G' est de type A_n, il en est de même de l'autre, et φ est attaché à une isogénie de G sur G'.*

Comme toutes les racines d'un groupe de type A_n se déduisent les unes des autres par les opérations du groupe de Weyl, tous les exposants radiciels de φ sont égaux entre eux ; soit q leur valeur commune. Il y a donc une bijection ψ de l'ensemble des racines de G sur l'ensemble des racines de G' telle que $\varphi(\psi(\alpha)) = q\,\alpha$ pour toute racine α de G ; il en résulte immédiatement que G et G' sont de même type, donc sont tous deux de type A_n. Soit $(\alpha_1, \ldots, \alpha_n)$ un système fondamental de racines de G par rapport à T tel que, dans le diagramme de Dynkin correspondant, les sommets relatifs à α_i et α_{i+1} soient liés par une arête $(1 \leq i < n)$; si α'_i est la racine de G' telle que $\varphi(\alpha'_i) = q\,\alpha_i$, les α'_i forment un système fondamental de racines de G' par rapport à T', et, dans le diagramme de Dynkin correspondant, les sommets relatifs à α'_i et α'_{i+1} sont liés par une arête $(1 \leq i < n)$. Utilisons les mêmes notations que plus haut en ce qui concerne le groupe $\mathrm{PL}(K^{n+1})$; il résulte de ce que nous avons dit qu'il existe une isogénie g' de G' sur $\mathrm{PL}(K^{n+1})$ qui applique T' sur $\overline{T}$ et qui est telle que l'isomorphisme spécial γ' qui lui est attaché applique $\overline{\omega}_i$ sur ω'_i $(1 \leq i \leq n+1)$. Posons $\gamma = \varphi \circ \gamma'$; c'est un isomorphisme de $X^{\mathbf{Q}}(\overline{T})$ sur $X^{\mathbf{Q}}(T)$ qui applique $\overline{\alpha}_i$ sur $q\,\alpha_i$; il résulte de ce qui a été dit plus haut que γ est associé à une isogénie g de G sur $\mathrm{PL}(K^{n+1})$ qui applique T sur $\overline{T}$. L'existence des isogénies g, g' démontre le théorème 1, compte tenu de la proposition 7 du n° 18.4. C.Q.F.D.

Soit G un groupe algébrique semi-simple de type A_n, et soit T un tore maximal de G. Soient P et Q respectivement le groupe des poids et le groupe des racines de G par rapport à T ; on a donc

$$Q \subset X(T) \subset P\,.$$

Il résulte immédiatement de l'étude que nous avons faite des diagrammes de type A_n (n° 19.4, I) que P/Q est un groupe cyclique d'ordre $n+1$, engendré par la classe modulo Q de $\omega_1 = \varpi_1$. Le groupe $X(T)/Q$ est donc un groupe cyclique dont l'ordre d divise $n+1$; nous dirons que d est l'*invariant numérique*[6] *de* G. Nous allons prouver qu'il existe des groupes de type A_n admettant pour invariant numérique un diviseur donné quelconque de $n+1$. Partons pour cela du groupe $\mathrm{SL}(V)$, où V est un espace vectoriel de dimension $n+1$. Si $1 \leq k \leq n$, soit V_k la puissance extérieure k-ième de l'espace V ; si $s \in \mathrm{SL}(V)$, soit $\rho_k(s)$ la puissance extérieure k-ième de s ; ρ_k est donc une

[6] De manière générale, le centre d'un groupe algébrique semi-simple G est isomorphe au groupe dual $\mathrm{Hom}(X(T)/Q, K^*)$ du groupe $X(T)/Q$. Donc si G est un groupe de type A_n et d'invariant numérique d, le centre de G est isomorphe au groupe $\mu_d(K)$ des racines d-ièmes de l'unité dans K.

représentation rationnelle de $\mathrm{SL}(V)$. Soit $(x_1, \ldots, x_{n+1})$ une base de V et soit T le tore maximal de $\mathrm{SL}(V)$ composé des opérations qui admettent chacun des x_i comme vecteur propre ; soit $t \cdot x_i = \omega_i(t)x_i$ $(t \in T)$. Soit $(i_1, \ldots, i_k)$ une suite strictement croissante d'indices entre 1 et $n+1$; désignons par $y(i_1, \ldots, i_k)$ le produit extérieur des éléments $x_{i_1}, \ldots, x_{i_k}$. On a alors

$$\rho_k(t) \cdot y(i_1, \ldots, i_k) = \omega_{i_1}(t) \ldots \omega_{i_k}(t) y(i_1, \ldots, i_k)\,.$$

Les poids de la représentation ρ_k sont donc, en notation additive, les $\omega_{i_1} + \ldots + \omega_{i_k}$ pour toutes les suites strictement croissantes de k indices. Ces poids sont tous transformés les uns des autres par les opérations du groupe de Weyl ; il en résulte tout de suite que ρ_k est une représentation simple dont le poids dominant est le k-ième poids dominant fondamental ϖ_k relativement au système fondamental de racines formé des $\alpha_i = \omega_i - \omega_{i+1}$. Soit

$$G_k = \rho_k(\mathrm{SL}(V))\,,\ T_k = \rho_k(T)\ ;$$

soit φ_k l'isomorphisme de $X^{\mathbf{Q}}(T_k)$ sur $X^{\mathbf{Q}}(T)$ attaché à ρ_k. Les exposants radiciels de φ_k, qui sont tous égaux, sont égaux à 1 (corollaire au lemme 4). Il en résulte tout de suite que φ_k applique le groupe Q_k des racines de G_k sur Q ; il applique par ailleurs $X(T_k)$ sur le groupe engendré par les $\omega_{i_1} + \ldots + \omega_{i_k}$, donc aussi sur le groupe engendré par Q et ϖ_k. Or, il résulte immédiatement de l'expression explicite de ϖ_k donnée au n° 19.4, I que l'on a $\varpi_k \equiv k\varpi_1 \pmod{Q}$ et que le groupe engendré par Q et ϖ_k contient Q comme sous-groupe d'indice $m^{-1}(n+1)$, où m est le p.g.c.d. de k et $n+1$; il en résulte que, si d est un diviseur $\neq 1$ de $n+1$, l'invariant numérique de G_k est d si l'on prend $k = d^{-1}(n+1)$. Par ailleurs, il résulte de ce qui a été dit plus haut que $\mathrm{PL}(V)$ est un groupe d'invariant numérique 1.

Théorème 2. – *Soit n un entier > 0 ; si d est un diviseur de $n+1$, il existe un groupe algébrique semi-simple de type A_n et d'invariant numérique d ; tous les groupes satisfaisant à ces conditions sont isomorphes entre eux.*

La première assertion a déjà été établie. Soient G et G' des groupes de type A_n ayant même invariant numérique, T et T' des tores maximaux de G et G' respectivement. Comme un groupe cyclique n'a qu'un seul sous-groupe d'ordre donné, il est clair qu'il existe un isomorphisme φ de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(T)$ qui applique les racines de G' sur celles de G et qui applique $X(T')$ sur $X(T)$; l'isomorphisme φ est attaché à une isogénie f de G sur G' (théorème 1), et f est un isomorphisme en vertu de la proposition 7 du n° 18.4.

Corollaire. – *Tout groupe algébrique semi-simple de rang* 1 *est isomorphe soit à* $\mathrm{SL}(K^2)$*, soit à* $\mathrm{PL}(K^2)$*.*

Un pareil groupe est en effet de type A_1.

Reprenons maintenant les représentations ρ_k considérées plus haut. Elles donnent naissance à des représentations projectives $\widetilde{\rho}_k$ de $\mathrm{PL}(V)$, opérant

dans les espaces $\mathrm{PL}(V_k)$. Soient H un groupe algébrique et σ une représentation linéaire (resp. projective) de H opérant dans V (resp. $P(V)$) ; $\rho_k \circ \sigma$ (resp. $\widetilde{\rho}_k \circ \sigma$) est alors une représentation linéaire (resp. projective) de H opérant dans V_k (resp. $P(V_k)$) et qu'on appelle la *puissance extérieure k-ième* de σ. Considérons en particulier le cas où $k = n$; la représentation ρ_n de $\mathrm{SL}(V)$ est évidemment équivalente à la représentation contragrédiente[7] de ρ_1, qui fait correspondre à tout élément $s \in \mathrm{SL}(V)$ l'automorphisme ${}^t s^{-1}$ du dual V^* de V. Par ailleurs, il résulte de la formule $\omega_1 + \ldots + \omega_{n+1} = 0$ que ses poids sont les $-\omega_i$ $(1 \leq i \leq n+1)$. Si σ est une représentation linéaire de H, $\rho_n \circ \sigma$ est équivalente à la représentation contragrédiente de σ, qui opère dans le dual de V et associe à tout $z \in H$ l'automorphisme ${}^t\sigma(z^{-1})$. De même, si σ est projective, $\widetilde{\rho}_n \circ \sigma$ est équivalente à la *représentation projective contragrédiente à σ* qui opère dans l'espace projectif $P(V^*)$ associé au dual de V, qu'on peut identifier à l'espace des hyperplans de l'espace $P(V)$; si $z \in H$, la contragrédiente de σ fait correspondre à z l'automorphisme qui transforme tout hyperplan M de $P(V)$ en $z(M)$. Nous avons donc le résultat suivant :

Proposition 2. – *Soit σ une représentation linéaire ou projective d'un groupe algébrique G. Les poids de la représentation contragrédiente de σ sont alors les opposés des poids de σ.*

Corollaire. – *Soit G un groupe algébrique semi-simple, et soit T un tore maximal de G. Si l'automorphisme $\theta \to -\theta$ de $X^{\mathbf{Q}}(T)$ appartient au groupe de Weyl de G (ce qui se produit dans le cas où G est de l'un des types B_n, C_n, D_n (n pair), E_7, E_8, F_4 ou G_2), toute représentation linéaire ou projective simple ρ de G est équivalente à sa contragrédiente. Si V est l'espace d'une représentation linéaire simple ρ de G, il existe une forme bilinéaire β non-dégénérée sur $V \times V$, et une seule à un facteur constant près, qui est invariante par $\rho(G)$; la forme β est soit symétrique, soit antisymétrique.*

Comme les opérations du groupe de Weyl permutent entre eux les poids de ρ, on voit que l'opposé de tout poids de ρ est un poids de ρ, donc que ρ a les mêmes poids que sa contragrédiente ρ^*. En particulier, ρ a le même poids dominant que ρ^*, donc lui est équivalente. Supposons ρ linéaire ; il résulte alors du fait que ρ est équivalente à sa contragrédiente que les opérations de $\rho(G)$ laissent invariante au moins une forme bilinéaire non dégénérée sur $V \times V$. Soit β une forme bilinéaire $\neq 0$ sur $V \times V$ invariante par $\rho(G)$; l'espace des vecteurs x tels que $\beta(x, y) = 0$ pour tout $y \in V$ est $\neq V$ et stable par $\rho(G)$; comme ρ est simple, cet espace est donc $\{0\}$, ce qui montre que β n'est pas dégénérée. Si β' est une forme bilinéaire quelconque sur $V \times V$ invariante

[7] Si V est un espace vectoriel de dimension $m = n + 1$, la puissance extérieure $\Lambda^n V = V_n$ est canoniquement isomorphe au dual V^* de V, l'isomorphisme η dépendant du choix d'une forme multilinéaire alternée ε de m variables dans V. Mais ε est invariante par $\mathrm{SL}(V)$, donc η définit une équivalence de représentations de $\mathrm{SL}(V)$.

par $\rho(G)$, il en est de même de $c\beta + c'\beta$ (où c, c' sont dans K) ; or, K étant algébriquement clos, on peut toujours choisir c, c' non nuls tous deux tels que $c\beta + c'\beta'$ soit dégénérée ; cette forme est alors nulle, et β' est proportionnelle à β. Appliquons ceci au cas où β' est définie par $\beta'(y,x) = \beta(x,y)$: il existe $m \in K$ tel que $\beta' = m\beta$. Il est clair que $m^2 = 1$; β est donc symétrique ou antisymétrique.

Remarque. – Supposons le corps K de caractéristique 2. On a $1 = -1$ dans K, et il y a identité entre formes bilinéaires symétriques et antisymétriques. Soit ρ une représentation linéaire simple d'un groupe G dans l'espace V, admettant une forme bilinéaire invariante β. On a vu que β est non dégénérée et symétrique. Mais alors $x \to \beta(x,x)$ est le carré d'une forme linéaire f sur V invariante par $\rho(G)$. Comme ρ est simple, on a donc $f = 0$, d'où $\beta(x,x) = 0$ ($x \in V$). Donc β est *alternée*, et l'on sait que ceci n'est possible que si la dimension de V est *paire*.

20.4 Les représentations simples d'un groupe de rang 1

Soit V un espace vectoriel de dimension 2 sur K, et soit (x,y) une base de V. Nous nous proposons de rechercher les représentations simples du groupe $\mathrm{SL}(V)$.

Etablissons d'abord le résultat suivant :

Proposition 3. – *Soient φ et φ' des représentations linéaires d'un groupe G telles que les représentations projectives déduites de ρ et ρ' soient équivalentes. Si G est son propre groupe dérivé (en particulier, si G est un groupe algébrique semi-simple), ρ et ρ' sont équivalentes.*

Soient V et V' les espaces de ρ et ρ' respectivement ; soient $\widetilde{\rho}$ et $\widetilde{\rho}'$ les représentations projectives déduites de ρ et ρ' ; elles opèrent sur les espaces projectifs $P(V)$ et $P(V')$ associés à V et V' respectivement. Il existe par hypothèse un isomorphisme $\widetilde{\mu}$ d'espaces projectifs de $P(V)$ sur $P(V')$ tel que

$$\widetilde{\mu} \circ \widetilde{\rho}(s) = \widetilde{\rho}'(s) \circ \widetilde{\mu} \quad \text{pour tout} \quad s \in G\,.$$

L'isomorphisme $\widetilde{\mu}$ provient par définition d'un isomorphisme μ de V sur V' ; si $s \in G$, $\mu \circ \rho(s)$ et $\rho'(s) \circ \mu$ sont des isomorphismes de V sur V' qui définissent le même isomorphisme de $P(V)$ sur $P(V')$. Or il est bien connu que les seuls automorphismes d'un espace vectoriel V qui définissent l'automorphisme identique de $P(V)$ sont les homothéties de V de rapports $\neq 0$; il existe donc une application χ de G dans l'ensemble K^* des éléments $\neq 0$ de K telle que l'on ait $\mu \circ \rho(s) = \chi(s)(\rho'(s) \circ \mu)$ pour tout $s \in G$. Comme ρ et ρ' sont des représentations, il en résulte que l'on a $\chi(st) = \chi(s)\,\chi(t)$ pour $s, t \in G$. Si G est son propre groupe dérivé, il résulte de là que $\chi(s) = 1$ pour tout $s \in G$, donc que ρ et ρ' sont équivalentes.

Corollaire. – *Deux représentations linéaires simples d'un groupe algébrique semi-simple G qui ont même poids dominant (relativement à un tore maximal T de G et à un système fondamental de racines de G par rapport à T) sont équivalentes.*

Ceci dit, revenons au problème de la détermination des représentations linéaires simples de $\mathrm{SL}(V)$. Nous désignerons par T le tore maximal de $\mathrm{SL}(V)$ composé des éléments t qui admettent x et y comme vecteurs propres ; nous posons, si $t \in T$, $t \cdot x = \omega(t)x$, d'où $t \cdot y = \omega^{-1}(t)\, y$. Les racines de G par rapport à T sont 2ω et -2ω (en notation additive) ; nous posons $2\omega = \alpha$, et nous considérons α comme racine fondamentale. Les poids dominants sont les $e\omega$, e entier ≥ 0. Pour tout $n \geq 0$, soit V_n l'espace des éléments homogènes de degré n de l'algèbre symétrique sur V ; il se compose des formes de degré n en x et y. L'espace V_n est l'espace d'une représentation σ_n de $\mathrm{SL}(V)$: si $s \in \mathrm{SL}(V)$, $\sigma_n(s)$ est la puissance symétrique n-ième de s.

Proposition 4. – *Soit W_n le sous-espace de V_n engendré par les puissances n-ièmes des éléments de V ; il est stable par $\sigma_n(\mathrm{SL}(V))$; soit ζ_n la représentation d'espace W_n induite par σ_n. La représentation linéaire ζ_n de $\mathrm{SL}(V)$ est simple, de poids dominant $n\omega$.*

Désignons par W'_n un sous-espace de V_n stable par ζ_n et $\neq \{0\}$. Soit B le groupe des éléments $s \in \mathrm{SL}(V)$ qui laissent invariant le sous-espace Kx de V ; c'est un groupe de Borel. L'espace W'_n contient donc un élément $z \neq 0$ tel que l'espace Kz soit stable par les opérations de B. Si l'on désigne par $\tau(\xi)$ $(\xi \in K)$ l'automorphisme de V qui laisse x invariant et change y en $y + \xi x$, $\tau(\xi)$ est un élément unipotent de B, de sorte que $\zeta_n(\tau(\xi))$ laisse z invariant. Ecrivant $z = F(x, y)$, où F est une forme de degré n, on voit que $F(x, y) = F(x, y + \xi x)$ pour tout $\xi \in K$, ce qui n'est possible que si $F(x, y) = cx^n$ $(c \in K)$. On a donc $x^n \in W'_n$; si x' est un vecteur $\neq 0$ quelconque de V, il existe une opération de $\mathrm{SL}(V)$ qui transforme x en x' , d'où $x'^n \in W'_n$ et par suite $W'_n \supset W_n$. On a donc prouvé que W_n est contenu dans tout sous-espace $\neq \{0\}$ de V_n stable par les opérations de $\sigma_n(\mathrm{SL}(V))$ et, en particulier, que la représentation d'espace W_n est simple.

Les poids de la représentation σ_n sont (en notation additive) les $k\omega$ pour $-n \leq k \leq n$, et $n\omega$ est un poids de ζ_n ; c'est donc le poids dominant de ζ_n.

Corollaire. – *Toute représentation linéaire simple de $\mathrm{SL}(V)$ est équivalente à une et une seule des représentations ζ_n.*

Si K est de caractéristique 0, il est bien connu que $W_n = V_n$ pour tout n. Supposons maintenant que K soit de caractéristique $p > 0$. Posons, pour $\xi, \xi' \in K$,

$$(\xi x + \xi' y)^n = \sum_{k=0}^{n} c_k\, \xi^k\, \xi'^{n-k}\, x^k\, y^{n-k} \qquad (c_k \in K)\ ;$$

on voit alors facilement que W_n est engendré par les $x^k\, y^{n-k}$ pour les k tels que $c_k \neq 0$, *i.e.* pour les k tels que le coefficient binomial $\binom{n}{k}$ ne soit pas divisible par p. Ecrivons n dans le système de numération de base p : $n = \sum_{r=0}^{h} a_r\, p^r$ avec $0 \leq a_r < p$. On a alors

$$(\xi x + \xi' y)^n = \prod_{r=0}^{h} (\xi^{p^r}\, x^{p^r} + \xi'^{p^r}\, y^{p^r})^{a_r}\,.$$

On en conclut facilement que les nombres k sont ceux qui peuvent se mettre sous la forme $\sum_{r=0}^{h} b_r\, p^r$ avec $0 \leq b_r \leq a_r$ pour tout r. On a donc prouvé la :

Proposition 5. – *Si K est de caractéristique 0, la représentation ζ_n de poids dominant $n\omega$ est de degré $n+1$. Si K est de caractéristique $p > 0$, et si $n = \sum_{r=0}^{h} a_r\, p^r$, avec $0 \leq a_r < p$, la représentation ζ_n de poids $n\omega$ est de degré $\prod_{r=0}^{h} (a_r + 1)$.*

De plus, on notera qu'il résulte de ce que nous avons dit que la représentation σ_n, puissance symétrique n-ième de l'application identique $\mathrm{SL}(V) \to \mathrm{GL}(V)$, n'est semi-simple (dans le cas où K est de caractéristique $p > 0$) que si ou bien $n < p$ ou bien n est de la forme $p^s - 1$. Enfin, supposant toujours K de caractéristique p et $n = \sum_{r=0}^{h} a_r\, p^r$, $0 \leq a_r < p$, ζ_n est équivalente au produit tensoriel des représentations simples de poids dominants $a_0\, \omega$, $a_1\, p\omega, \ldots, a_h\, p^h\omega$. La représentation simple de poids dominant $p^h\omega$ de $\mathrm{SL}(V)$ est de degré 2 et admet $p^h\omega$ et $-p^h\omega$ comme seuls poids.

21. Les groupes de type G_2 [1]

21.1 Deux lemmes

Soient G un groupe algébrique semi-simple, T un tore maximal de G, α une racine de G par rapport à T, et Z le sous-groupe de dimension 3 de G correspondant à la racine α (*i.e.* le centralisateur de la composante neutre dans l'ensemble des $t \in T$ tels que $\alpha(t) = 1$). Soient τ_+ et τ_- des isomorphismes de K sur des sous-groupes de Z tels que l'on ait, pour $\xi \in K$, $t \in T$,

$$t\,\tau_+(\xi)\,t^{-1} = \tau_+(\alpha(t)\xi)$$

$$t\,\tau_-(\xi)\,t^{-1} = \tau_-((\alpha(t))^{-1}\xi)\,.$$

Soit enfin ρ une représentation linéaire[2] de G opérant dans un espace vectoriel V ; si ϖ est un poids de ρ, on dit qu'un vecteur $x \in V$ appartient au poids ϖ si $x \neq 0$ et si l'on a, pour $t \in T$, $t \cdot x = \varpi(t)x$.

Nous poserons

$$\zeta_+(\xi) = \rho(\tau_+(\xi))\,,\ \zeta_-(\xi) = \rho(\tau_-(\xi))\,.$$

Lemme 1. – *Soit x un vecteur de V appartenant à un poids ϖ. Alors, pour tout $\xi \in K$, $\tau_+(\xi) \cdot x$ est une combinaison linéaire de vecteurs de V appartenant à des poids de la forme $\varpi + k\,\alpha$, k entier ≥ 0.*

En effet, $\rho \circ \tau_+$ est une application polynôme de K dans $\mathrm{GL}(V)$; on peut donc écrire $\tau_+(\xi) \cdot x = x + \sum_{k=1}^{m} \xi^k\, x_k$, les x_k étant des vecteurs de V. On a $t\,\tau_+(\xi) \cdot x = t \cdot x + \sum_{k=1}^{m} \xi^k\, t \cdot x_k$; mais ceci est encore égal à

$$\tau_+(\alpha(t)\xi) \cdot (t \cdot x)\,,$$

donc à

$$\omega(t)\,\tau_+(\alpha(t)\xi) \cdot x = \omega(t)x + \sum_{k=1}^{m} \omega(t)(\alpha(t))^k\,\xi^k\, x_k\ ;$$

[1] Exposé de C. Chevalley, le 6.1.1958

[2] On note, de manière générale, $g \cdot x$ le transformé d'un élément x de V par $\rho(g)$ (pour $g \in G$).

on a donc $t \cdot x_k = \omega(t)(\alpha(t))^k\, x_k$, et x_k appartient au poids $\varpi + k\alpha$. Ceci démontre le lemme.

Corollaire. – *Le sous-espace de V engendré par les vecteurs qui appartiennent à des poids de la forme $\varpi + r\alpha$, où r est un entier, est transformé en lui-même par les opérations de $\rho(Z)$.*

Cet espace est évidemment transformé en lui-même par les opérations de $\rho(T)$; il résulte du lemme 1 qu'il est transformé en lui-même par les opérations $\tau_+(\xi)$, $\tau_-(\xi)$ $(\xi \in K)$. Le corollaire résulte alors du fait que Z est engendré par la réunion des ensembles $Z \cap T$, $\tau_+(K)$ et $\tau_-(K)$.

Lemme 2. – *Soit $\widetilde{\rho}$ une représentation projective de noyau fini d'un groupe algébrique semi-simple G, et soit T un tore maximal de G. Supposons que les poids de $\widetilde{\rho}$ par rapport à T appartiennent au groupe $X(T)$ des caractères rationnels de T. Il existe alors une représentation linéaire ρ de G telle que $\widetilde{\rho}$ soit la représentation projective déduite de ρ.*

Posons $\overline{G} = \widetilde{\rho}(G)$, $\overline{T} = \widetilde{\rho}(T)$. L'application $\widetilde{\rho}$ est une isogénie de G sur $\overline{G}$; il lui correspond un isomorphisme spécial $\widetilde{\varphi}$ de $X^{\mathbf{Q}}(\overline{T})$ sur $X^{\mathbf{Q}}(T)$. La représentation $\widetilde{\rho}$ opère dans l'espace projectif $P(V)$ associé à un espace vectoriel V ; soit G' le groupe linéaire associé à $\widetilde{\rho}$; c'est un sous-groupe de $\mathrm{SL}(V)$. Soient g' l'application canonique de G' sur $\overline{G}$ et T' le tore maximal de G' tel que $g'(T') = \overline{T}'$. Il correspond à l'isogénie g' un isomorphisme spécial γ' de $X^{\mathbf{Q}}(\overline{T})$ sur $X^{\mathbf{Q}}(T')$. Soit φ l'isomorphisme de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(T)$ tel que $\widetilde{\varphi} = \varphi \circ \gamma'$. Nous allons montrer que φ est un isomorphisme spécial. Soit α' une racine de G' par rapport à T' ; on sait que les exposants radiciels de γ' sont égaux à 1 (n° 18.3, proposition 4) ; il existe donc une racine $\overline{\alpha}$ de $\overline{G}$ telle que $\gamma'(\overline{\alpha}) = \alpha'$. Il existe une racine α de G et une puissance q de l'exposant caractéristique de K telles que $\widetilde{\varphi}(\overline{\alpha}) = q\alpha$, d'où $\varphi(\alpha') = q\alpha$. Par ailleurs, l'application identique de G' dans $\mathrm{GL}(V)$ est une représentation τ de G', et les poids de $\widetilde{\rho}$ sont par définition les images par φ de ceux de τ ; comme $X(T')$ est engendré par les poids de τ, il résulte du fait que les poids de $\widetilde{\rho}$ appartiennent à $X(T)$ que $\varphi(X(T')) \subset X(T)$; φ est donc bien spécial. On en conclut (n° 18, proposition 7) qu'il existe une isogénie ρ de G sur G' telle que $\widetilde{\rho} = g' \circ \rho$, ce qui démontre le lemme 2.

Rappelons que l'on a $Q \subset X(T) \subset P$, où Q est le sous-groupe de $X(T)$ engendré par l'ensemble R des racines, et où P est le groupe des poids (n° 16.3).

Définition 1. – *On dit que le groupe algébrique semi-simple G est* adjoint (resp. simplement connexe) *si l'on a $X(T) = Q$* (resp. $X(T) = P$).

D'après le lemme 2, le groupe G est simplement connexe si et seulement si toute représentation projective de noyau fini de G se relève en une représentation linéaire.

21.2 Etude d'un groupe de type G_2

Soit G un groupe algébrique semi-simple de type G_2. Soit T un tore maximal de G, et soit $X(T)$ le groupe des caractères rationnels de T. Soit (α_1, α_2) un système fondamental de racines de G par rapport à T tel que le diagramme de Dynkin correspondant soit

le sommet S_i correspondant à α_i $(i = 1, 2)$. L'espace $X^{\mathbf{Q}}(T)$ est donc engendré par les éléments ω_0, ω_1, ω_2 de somme nulle tels que $\alpha_1 = \omega_0$, $\alpha_2 = \omega_1 - \omega_0$; les poids dominants fondamentaux sont $\varpi_1 = -\omega_2 = 2\alpha_1 + \alpha_2$, $\varpi_2 = \omega_1 - \omega_2 = 3\alpha_1 + 2\alpha_2$ (*cf.* n° 19.4, IX) ; comme ils sont combinaisons linéaires à coefficients entiers des racines, *il existe donc une représentation linéaire simple ρ de G de poids dominant ϖ_1* (lemme 2). Posons $G' = \rho(G)$, $T' = \rho(T)$, et soit φ l'isomorphisme spécial de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(T)$ attaché à ρ. Il existe un système fondamental de racines (α'_1, α'_2) de G' par rapport à T' tel que $\varphi(\alpha'_i) = q_i\,\alpha_i$ $(i = 1, 2)$, et on a $q_1 = 1$ en vertu du corollaire au lemme 4 du n° 20.3. Soient w_i et w'_i les réflexions par rapport aux racines α_i de G et α'_i de G' ; on a $w_1(\alpha_2) = \alpha_2 + 3\alpha_1$ et $\varphi \circ w'_1 = w_1 \circ \varphi$ (n° 18.3, proposition 5) ; on en conclut que $w'_1(\alpha'_2) = \alpha'_2 + 3\,q_2\,\alpha'_1$. Comme les entiers de Cartan d'un groupe semi-simple sont < 4 en valeur absolue, on a $q_2 = 1$. Il en résulte que G' est de type G_2 et que le diagramme de Dynkin associé au système fondamental (α'_1, α'_2) est le même que celui associé au système (α_1, α_2), le sommet S_i correspondant à α'_i. La représentation ρ opère dans un espace vectoriel V ; l'application identique de G' dans $\mathrm{GL}(V)$ est une représentation simple τ de G' dont le poids dominant ϖ' est l'élément de $X(T')$ dont l'image par φ est ϖ_1, c'est à dire $2\alpha'_1 + \alpha'_2$. Comme ρ induit un isomorphisme de $X(T')$ sur $X(T)$, ρ est un isomorphisme de G sur G' (n° 18.4, proposition 6). Remplaçant G par G', nous supposerons désormais que G est un groupe d'automorphismes d'un espace vectoriel V et que ρ est l'application identique de G dans $\mathrm{GL}(V)$. Il est immédiat que ϖ_1 est un poids dominant minimal. Les poids $\neq 0$ de ρ sont donc les transformés $\pm\omega_i$ du poids dominant par les opérations du groupe de Weyl (n° 20.2, proposition 1) ; ils sont de multiplicité 1.

Lemme 3. – *Si* 0 *est un poids de ρ, ce poids est de multiplicité* 1.

Nous désignerons par x_i (resp. y_i) un vecteur de V de poids ω_i (resp. $-\omega_i$), et par Z_i le sous-groupe de dimension 3 de G correspondant à la racine α_i. Soit z un vecteur de V appartenant au poids 0. Comme il n'existe aucun multiple entier $\neq 0$ de α_2 qui soit poids de ρ, l'espace Kz est transformé en lui-même par les opérations de Z_2 (corollaire au lemme 1), d'où il résulte que z est invariant par les opérations de Z_2 puisque Z_2 est son propre groupe dérivé. Par ailleurs, G est engendré par Z_1 et Z_2 (n° 13.3, proposition 5) ;

il est donc impossible que z soit stable par les opérations de Z_1. Soit τ_1 un isomorphisme de K sur un sous-groupe de Z_1 associé à la racine α_1 ; montrons que z ne peut être invariant par les opérations de $\tau_1(K)$. Supposons en effet le contraire ; il existe un groupe de Borel B_1 de Z_1 qui est engendré par $\tau_1(K)$ et par un tore maximal T_1 de Z_1 contenu dans T ; z serait alors invariant par B_1, et son orbite $Z_1\, z$ relativement à Z_1 serait l'image de la variété complète Z_1/B_1 par un morphisme de cette variété dans V ; cette image, étant une sous-variété complète de l'espace vectoriel V, se réduirait à point, et z serait invariant par les opérations de Z_1, ce qui n'est pas. Il n'y a qu'un seul poids de ρ qui soit de la forme $k\,\alpha_1$ avec $k > 0$: ce poids est ω_0. Il résulte alors du lemme 1 que l'on a $\tau_1(\xi) \cdot z = z + c\,\xi\, x_0$ avec $c \in K$, $c \neq 0$. Ceci dit, soit z' un vecteur quelconque appartenant au poids 0 ; on a $\tau_1(\xi) \cdot z' = z' + c'\,\xi\, x_0$, $c' \neq 0$. Il en résulte que $c'z - cz'$ est invariant par les opérations de $\tau_1(K)$; si ce vecteur était $\neq 0$, il appartiendrait au poids 0, ce que nous avons vu être impossible. On a donc $z' = c^{-1}\, c'z$, ce qui montre que, si 0 est un poids de ρ, ce poids est de multiplicité 1. C.Q.F.D.

Lemme 4. – 0 *n'appartient pas aux poids de* ρ *si et seulement si le corps* K *est de caractéristique* 2.

Supposons d'abord que 0 ne soit pas un poids de ρ. L'espace M_0 engendré par x_0 et y_0 est alors stable par les opérations de Z_1. Soit T_1 le tore maximal de Z_1 contenu dans T ; les racines de Z_1 par rapport à T_1 sont les restrictions $\overline{\alpha}_1$ et $-\overline{\alpha}_1$ de α_1 et $-\alpha_1$ à T_1 ; les poids par rapport à T_1 de la représentation de Z_1 sur l'espace M_0 sont donc $\overline{\alpha}_1$ et $-\overline{\alpha}_1$. Il en résulte aussitôt que la représentation de Z_1 sur l'espace M_0 est simple et de poids dominant $\overline{\alpha}_1$. Mais, si K est de caractéristique $\neq 2$, la représentation de Z_1 de poids dominant $\overline{\alpha}_1$ est de dimension 3 ; donc, si 0 n'est pas un poids de ρ, K est de caractéristique 2.

Réciproquement, supposons K de caractéristique 2. D'après le corollaire à la proposition 2 du n° 20.3, et la remarque qui la suit, l'espace V de ρ est de dimension *paire*. Si 0 était un poids de ρ, il existerait 7 poids 0, $\pm\omega_0$, $\pm\omega_1$, $\pm\omega_2$ tous de multiplicité 1, d'où $\dim V = 7$ dans ce cas. Donc 0 n'est pas un poids de ρ. C.Q.F.D.

Ceci étant, *supposons que* K *ne soit pas de caractéristique* 2. On désignera par z_0 un vecteur appartenant au poids 0. L'espace V est donc de dimension 7. Faisons usage de la forme bilinéaire β déjà mentionnée ci-dessus. Exprimant qu'elle est invariante par les opérations de T, on trouve tout de suite que l'on a

$$\beta(x_i, x_j) = \beta(y_i, y_j) = 0 \qquad \text{quels que soient } i \text{ et } j\,,$$

$$\beta(z_0, x_i) = \beta(z_0, y_i) = 0 \quad \text{et} \quad \beta(x_i, y_j) = 0 \quad \text{si} \quad i \neq j\,.$$

On peut donc supposer x_1, x_2, y_1, y_2 normalisés de telle manière que $\beta(x_1, y_1) = \beta(x_2, y_2) = 1$. Faisant usage du corollaire au lemme 1, on voit tout

de suite que les espaces $M_1 = Kx_1 + Ky_2$, $M_2 = Kx_2 + Ky_1$ sont invariants par les opérations de Z_1. Les poids de la représentation de Z_1 sur l'espace M_2 sont les restrictions de ω_2 et $-\omega_1$ à T_1. Déterminons ces restrictions. Soit $\overline{w}_1$ la réflexion par rapport à la racine α_1 de Z_1 ; il est clair que, si w_1 est la réflexion par rapport à α_1, et si ω est un élément quelconque de $X(T)$, $\overline{w}_1$ change la restriction $\overline{\omega}$ de ω à T_1 en la restriction de $w_1(\omega)$, ce qui montre que $\overline{\omega} = 0$ si $w_1(\omega) = \omega$ (car $\overline{w}_1$ change tout élément de $X(T_1)$ en son opposé). Or on a $w_1(\omega_1) = \omega_1 + \omega_0$, $w_1(\omega_2) = \omega_2 + \omega_0$; la restriction de $\omega_1 - \omega_2$ à T_1 est donc nulle ; comme il est de même de celle de $\omega_0 + \omega_1 + \omega_2$ et comme la restriction de ω_0 est $\overline{\alpha}_1$, on voit que les restrictions de ω_1 et ω_2 sont égales à $-\frac{1}{2}\overline{\alpha}_1$. Comme $-\frac{1}{2}\overline{\alpha}_1$ appartient à $X(T_1)$, Z_1 est isomorphe à $\mathrm{SL}(K^2)$. Introduisons un espace vectoriel W de dimension 2 sur K et une base (w_1, w_2) de W. Soit f_1 l'isomorphisme de W sur M_1 qui applique w_1 sur x_1 et w_2 sur y_2 ; cet isomorphisme définit un isomorphisme F_1 de $\mathrm{SL}(W)$ sur $\mathrm{SL}(M_1)$ qui est l'ensemble des restrictions à M_1 des opérations de Z_1. Soit W^* le dual de W, et soit (w_1^*, w_2^*) la base de W^* duale de la base (w_1, w_2) ; soit f_1^* l'isomorphisme de W^* sur M_2 qui applique w_1^* sur y_1 et w_2^* sur x_2 ; cet isomorphisme définit un isomorphisme F_1^* de $\mathrm{SL}(W^*)$ sur $\mathrm{SL}(M_2)$. Il résulte du fait que β est invariante par les opérations de G que, si $s \in Z_1$ et si u est l'élément de $\mathrm{SL}(W)$ tel que s coïncide avec $F_1(u)$ sur M_1, alors s coïncide avec $F_1^*({}^t u^{-1})$ sur M_2. Par ailleurs, comme l'application qui fait correspondre à tout $s \in Z_1$ sa restriction à M_1 est une représentation simple de poids dominant $\frac{1}{2}\overline{\alpha}_1$ de Z_1, c'est un isomorphisme de Z_1 sur $\mathrm{SL}(M_1)$, d'où il résulte qu'il existe un isomorphisme F de $\mathrm{SL}(W)$ sur Z_1 tel que, pour tout $u \in \mathrm{SL}(W)$, $F_1(u)$ soit la restriction de $F(u)$ à M_1. Soit W_2 l'espace des éléments homogènes de degré 2 de l'algèbre symétrique sur W ; c'est l'espace d'une représentation σ_2 de $\mathrm{SL}(W)$. Si $s \in Z_1$, soit $\zeta_0(s)$ la restriction de s à l'espace M_0 engendré par x_0, y_0 et par le vecteur z_0 de poids 0 : c'est une représentation simple de poids dominant $\overline{\alpha}_1$ de Z_1. Par ailleurs, $\sigma_2 \circ F^{-1}$ est aussi une représentation simple de poids dominant $\overline{\alpha}_1$ de Z_1. Les représentations ζ_0 et $\sigma_2 \circ F^{-1}$ sont donc équivalentes, et il existe un isomorphisme f_2 de W_2 sur M_0 tel que l'on ait $f_2 \circ (\sigma_2 \circ F^{-1})(s) = \zeta_0(s) \circ f_2$ pour tout $s \in Z_1$. L'espace W_2 admet une base composée des éléments w_1^2, w_2^2, $w_1 w_2$. Soit τ_1 un isomorphisme de K sur un sous-groupe de Z_1 associé à la racine α_1 ; comme $\omega_0 - \omega_2$ n'est pas un poids de ρ, les opérations de $\tau_1(K)$ laissent y_2 fixe ; les opérations de $(F^{-1} \circ \tau_1)(K)$ laissent donc w_2 fixe, et leurs images par σ_2 laissent w_2^2 fixe. Par ailleurs, les points de M_0 qui sont invariants par les opérations de $\tau_1(K)$ sont les points de l'espace Kx_0 ; on en conclut que f_2 applique w_2^2 sur un multiple scalaire de x_0. On verrait de même que f_2 applique w_1^2 sur un multiple scalaire de y_0. Nous poserons $x_0' = f_2(w_2^2)$, $y_0' = f_2(w_1^2)$. Comme β n'est pas dégénérée et comme $\beta(z_0, x_i) = \beta(z_0, y_i) = 0$ $(i = 0, 1, 2)$, on a $\beta(x_0', y_0') \neq 0$. Or on peut remplacer f_2 par un isomorphisme de la forme cf_2, où c est un élément $\neq 0$ quelconque de K, sans que l'on cesse d'avoir $f_2 \circ (\sigma_2 \circ F^{-1})(s) = \zeta_0(s) \circ f_2$ pour tout $s \in Z_1$. On peut choisir c de telle

manière que $\beta(x'_0, y'_0) = 1$. Comme x_0 et y_0 n'ont encore été déterminés qu'à des facteurs constants près, on peut supposer que $x_0 = x'_0$ et $y_0 = y'_0$. Enfin, on peut supposer que $f_2(w_1 w_2) = z_0$. On voit donc que l'espace V admet une base composée d'éléments z_0, x_i, y_i $(i = 0, 1, 2)$ qui possèdent les propriétés suivantes : il existe des isomorphismes f_1, f_1^*, f_2 de W, W^* et W_2 sur les espaces $M_1 = Kx_1 + Ky_2$, $M_2 = Kx_2 + Ky_1$ et $M_0 = Kx_0 + Ky_0 + Kz_0$ respectivement tels que $f_1(w_1) = x_1$, $f_1(w_2) = y_2$, $f_1^*(w_1^*) = y_1$, $f_1^*(w_2^*) = x_2$, $f_2(w_1^2) = y_0$, $f_2(w_2^2) = x_0$, $f_2(w_1 w_2) = z_0$; si F_1, F_1^*, F_2 sont les isomorphismes de $\mathrm{SL}(W)$ sur $\mathrm{SL}(M_1)$, $\mathrm{SL}(W^*)$ sur $\mathrm{SL}(M_2)$ et $\mathrm{SL}(W_2)$ sur $\mathrm{SL}(M_0)$ définis par f_1, f_1^* et f_2 respectivement, les opérations de Z_1 sont les automorphismes s de V pour lesquels il existe un $u \in \mathrm{SL}(W)$ tel que les restrictions de s à M_1, M_2 et M_0 soient $F_1(u)$, $F_1^*({}^t u^{-1})$ et $F_2(\sigma_2(u))$ respectivement ($\sigma_2(u)$ étant la puissance symétrique seconde de u) ; les opérations de G laissent invariante une forme bilinéaire non dégénérée β telle que

$$\beta(x_i, y_i) = 1 \qquad (i = 0, 1, 2)\,,$$

$$\beta(z_0, x_i) = \beta(z_0, y_i) = \beta(x_i, x_j) = \beta(y_i, y_j) = 0 \quad (i, j = 0, 1, 2)\,,$$

$$\beta(x_i, y_j) = 0 \qquad \text{si} \quad i \neq j \ ;$$

enfin z_0 appartient au poids 0, x_i au poids ω_i et y_i au poids $-\omega_i$.

Considérons maintenant les opérations de Z_2. Il résulte du corollaire au lemme 1 que les espaces $Kx_0 + Kx_1$, $Ky_0 + Ky_1$, Kz_0, Kx_2, Ky_2 sont stables par les opérations de Z_2. Comme Z_2 est son propre groupe dérivé, les points z_0, x_2, y_2 sont invariants par les opérations de Z_2. Par ailleurs, les restrictions des opérations de Z_2 à $Kx_0 + Kx_1$ sont évidemment tous les automorphismes de déterminant 1 de cet espace. Les espaces $Kx_0 + Kx_1$ et $Ky_0 + Ky_1$ sont mis en dualité par la restriction de β au produit de ces deux espaces ; si $s \in Z_2$, les restrictions de s à $Kx_0 + Kx_1$ et $Ky_0 + Ky_1$ sont contragrédientes l'une à l'autre par rapport à cette restriction ; ces restrictions se déterminent donc mutuellement.

Ceci étant, construisons un groupe $\overline{G}$ comme suit. Ce sera un groupe d'automorphismes de l'espace vectoriel $W \times W^* \times W_2$; nous identifierons W, W^*, W_2 à leurs images dans $W \times W^* \times W_2$, qui sera donc identifié à la somme directe des espaces W, W^*, W_2. Le groupe $\overline{G}$ sera engendré par deux groupes $\overline{Z}_1$ et $\overline{Z}_2$ décrits comme suit. Le groupe $\overline{Z}_1$ se compose des automorphismes dont les restrictions à W, W^*, W_2 sont de la forme u, ${}^t u^{-1}$, $\sigma_2(u)$ pour $u \in \mathrm{SL}(W)$. Les opérations de $\overline{Z}_2$ laissent fixes les points $w_1 w_2$, w_2, w_2^* et les espaces $N = Kw_2^2 + Kw_1$, $N^* = Kw_1^2 + Kw_1^*$; leurs restrictions à N sont tous les automorphismes de déterminant 1 de cet espace ; enfin les restrictions d'une opération de $\overline{Z}_2$ à N et N^* sont contragrédientes l'une à l'autre par rapport à la forme bilinéaire γ sur $N \times N^*$ définie par $\gamma(w_2^2, w_1^2) = \gamma(w_1, w_1^*) = 1$, $\gamma(w_2^2, w_1^*) = \gamma(w_1, w_1^2) = 0$. Ceci étant, il résulte de ce que nous avons dit que le groupe G est isomorphe à $\overline{G}$.

On a des résultats entièrement analogues dans le cas où K est de caractéristique 2 ; il faut seulement remplacer l'espace W_2 par le sous-espace W_2' engendré par w_1^2 et w_2^2 et remplacer la représentation σ_2 de $\mathrm{SL}(W)$ par la représentation σ_2' telle que $\sigma_2'(u)$ soit la restriction de $\sigma_2(u)$ à W_2' ($u \in \mathrm{SL}(W)$). Nous avons donc établi le

Théorème 1. – *Tous les groupes algébriques semi-simples de type G_2 (relatifs à un même corps de base K) sont isomorphes entre eux.*

21.3 Sur l'algèbre de Lie d'un groupe semi-simple

Soient G un groupe algébrique semi-simple et $\mathfrak{g}$ son algèbre de Lie. Désignons par T un tore maximal de G, et par $\mathfrak{t}$ son algèbre de Lie, qui est une sous-algèbre de $\mathfrak{g}$. Pour toute racine α de G par rapport à T, soit τ_α un isomorphisme du groupe K sur un sous-groupe de G associé à α ; alors la formule $X_\alpha = [d\,\tau_\alpha(\xi)/d\xi]_{\xi=0}$ définit un élément X_α de $\mathfrak{g}$ ($\mathfrak{g}$ étant identifié à l'espace tangent à G en son élément neutre). Il résulte de ce qui a été dit au n° 15.1, lemme 2, que $\mathfrak{g}$ est la somme directe de $\mathfrak{t}$ et des espaces KX_α pour toutes les racines α. Soit γ un groupe multiplicatif à un paramètre contenu dans T ; alors la formule $\gamma^K = (d\gamma(\theta)/d\theta)_{\theta=1}$ définit un élément γ^K de $\mathfrak{t}$. On sait que la dérivée en (e,e) (où e est l'élément neutre de G) de l'application $(s,t) \to st$ de $G \times G$ dans G applique (L,M) sur $L+M$ (L et M étant des vecteurs tangents à G en e ; l'espace tangent à $G \times G$ en (e,e) est identifié au produit par lui-même de l'espace tangent à G en e) ; il en résulte que, si γ, γ' sont des éléments du groupe $\Gamma(T)$ des groupes à un paramètre de T (écrit en notation additive), on a

$$(\gamma+\gamma')^K = \gamma^K + \gamma'^K \ ;$$

on en déduit une application linéaire $K \otimes_{\mathbf{Z}} \Gamma(T) \to \mathfrak{t}$. Cette application est un isomorphisme d'espaces vectoriels, comme il résulte tout de suite du fait que $\Gamma(T)$ a une base $(\gamma_1, \ldots, \gamma_n)$ telle que l'application

$$(\theta_1, \ldots, \theta_n) \to \prod_{i=1}^{n} \gamma_i(\theta_i)$$

soit un isomorphisme de K^{*n} sur T. Le dual du $\mathbf{Z}$-module $\Gamma(T)$ s'identifie au groupe $X(T)$ des caractères rationnels de T ; on en déduit un isomorphisme de l'espace vectoriel $X^K(T) = K \otimes_{\mathbf{Z}} X(T)$ sur le dual $\mathfrak{t}^*$ de $\mathfrak{t}$; nous désignerons par ω^K l'image dans cet isomorphisme d'un élément ω de $X(T)$. Si α est une racine, nous dirons que α^K est la *racine infinitésimale* associée à α. On sait que, pour toute racine α, il existe un élément γ_α et un seul de $\Gamma(T)$ qui est changé en son opposé par la symétrie par rapport à α et qui est tel que $\langle \gamma_\alpha, \alpha \rangle = 2$; le groupe à un paramètre γ_α est contenu dans le groupe Z_α de dimension 3 associé à la racine α. Nous poserons

$$H_\alpha = \gamma_\alpha^K$$

d'où

$$\alpha^K(H_\alpha) = 2\,.$$

L'espace $\mathfrak{g}$ est l'espace de la représentation adjointe $s \to \operatorname{Ad} s$ de G : $\operatorname{Ad} s$ est la dérivée en e de l'application $t \to sts^{-1}$ de G sur lui-même. Si $t \in T$, la formule $t\,\tau_\alpha(\xi)t^{-1} = \tau_\alpha(\alpha(t)\xi)$ donne

$$\operatorname{Ad} t \cdot X_\alpha = \alpha(t)X_\alpha \ ;$$

par ailleurs, T étant commutatif, on a $\operatorname{Ad} t \cdot T = T$ pour tout $t \in \mathfrak{t}$. Les poids de la représentation adjointe de G sont d'une part les racines (qui sont des poids de multiplicité 1) et d'autre part 0, de multiplicité égale à $\dim \mathfrak{t}$, donc au rang de G.

Tout homomorphisme f de G dans un groupe algébrique G' définit un homomorphisme de $\mathfrak{g}$ dans l'algèbre de Lie de G' (à savoir la dérivée de f en l'élément neutre). En particulier, supposons que f soit une représentation linéaire ρ, donc que $G' = \mathrm{GL}(V)$, V étant un espace vectoriel ; l'algèbre de Lie de $\mathrm{GL}(V)$ s'identifie canoniquement à l'espace E des endomorphismes de V ; l'homomorphisme $\mathfrak{g} \to E$ défini par ρ s'appelle la *représentation infinitésimale* associée à ρ ; nous la désignerons par ρ_i. La représentation adjointe de $\mathrm{GL}(V)$ fait correspondre à tout $s \in \mathrm{GL}(V)$ l'automorphisme $X \to sXs^{-1}$ de E ; les opérations de $\operatorname{Ad}(\mathrm{GL}(V))$ laissent donc invariante la forme bilinéaire $(X, Y) \to \operatorname{Tr} XY$ sur $E \times E$. Il en résulte que, si $\mathfrak{g}$ est l'algèbre de Lie de G, et ρ une représentation linéaire de $\mathfrak{g}$, la forme bilinéaire $(X, Y) \to \operatorname{Tr} \rho_i(X)\,\rho_i(Y)$ sur $\mathfrak{g}$ est invariante par les opérations de $\operatorname{Ad} G$. Soit B_ρ cette forme, que nous appellerons la *forme de Killing* de la représentation ρ. Exprimant l'invariance de cette forme par les opérations $\operatorname{Ad} t$, $t \in T$, il vient

$$\begin{array}{l} B_\rho(X_\alpha, X_\beta) = 0 \text{ si } \alpha, \beta \text{ sont des racines, } \alpha \neq -\beta \\ B_\rho(H, X_\alpha) = 0 \text{ si } \alpha \text{ est une racine, } H \in \mathfrak{t}\,. \end{array} \tag{1}$$

Supposons maintenant que G soit de rang 1. Dans ce cas, G est isomorphe soit à $\mathrm{SL}(K^2)$ soit à $\mathrm{PL}(K^2)$. Supposons d'abord que G soit $\mathrm{SL}(K^2)$, c'est-à-dire le groupe des matrices de degré 2 et de déterminant 1. On a alors, en prenant comme tore maximal T le groupe des matrices diagonales contenues dans G, et en choisissant convenablement la racine α,

$$\tau_{-\alpha}(\xi) = \begin{pmatrix} 1 & 0 \\ c_2\,\xi & 1 \end{pmatrix} \qquad \tau_\alpha(\xi) = \begin{pmatrix} 1 & c_1\,\xi \\ 0 & 1 \end{pmatrix}$$

$$\gamma_\alpha(\theta) = \begin{pmatrix} \theta & 0 \\ 0 & \theta^{-1} \end{pmatrix}$$

où c_1, c_2 sont des éléments $\neq 0$ de K. Il en résulte que l'on a alors $[X_\alpha, X_{-\alpha}] = c\,H_\alpha$, avec $c = c_1\,c_2 \neq 0$. On vérifie facilement qu'il en est encore ainsi dans

le cas où G est isomorphe à $\mathrm{PL}(K^2)$ (mais il convient d'observer que dans ce cas, si K est de caractéristique 2, on a $H_\alpha = 0$). Soit ρ une représentation linéaire de G ; exprimant l'invariance de B_ρ, on trouve facilement la relation $B_\rho([X_\alpha, H_\alpha], X_{-\alpha}) + B_\rho(H_\alpha, [X_\alpha, X_{-\alpha}]) = 0$, et par suite

$$cB_\rho(H_\alpha, H_\alpha) = 2\, B_\rho(X_\alpha, X_{-\alpha})\,.$$

Revenons maintenant au cas d'un groupe G semi-simple quelconque. A toute racine α correspond un sous-groupe Z_α de dimension 3 de G qui admet un tore maximal T_α contenu dans T ; X_α et $X_{-\alpha}$ sont des éléments de l'algèbre de Lie de Z_α ; le groupe à un paramètre γ_α est un groupe à un paramètre de T_α ; la restriction $\overline{\alpha}$ de α à T_α est une racine de Z_α et l'on a $\overline{\alpha}\,(H_\alpha) = 2$. On en déduit que, pour toute représentation linéaire ρ de G, on a $[X_\alpha, X_{-\alpha}] = c_\alpha\, H_\alpha$ avec une constante $c_\alpha \neq 0$, et

$$c_\alpha B_\rho(H_\alpha, H_\alpha) = 2\, B_\rho(X_\alpha, X_{-\alpha})\,. \tag{2}$$

21.4 Algèbre de Lie d'un groupe de type G_2

Nous allons appliquer ceci au cas où G est le groupe de type G_2 considéré au n° 21.2, dont nous utiliserons les notations ; en particulier, ρ sera l'application identique de G dans $\mathrm{GL}(V)$. *Nous supposerons de plus que K est de caractéristique* 3. Considérons un élément H de $\mathfrak{t}$; on a $\rho_i(H) \cdot x_i = \omega_i^K(H) \cdot x_i$, $\rho_i(H) \cdot y_i = -\omega_i^K(H) \cdot y_i$, $\rho_i(H) \cdot z_0 = 0$, d'où

$$B_\rho(H, H) = 2 \sum_{i=0}^{2} (\omega_i^K(H))^2\,.$$

Soit γ_i (resp. H_i) l'élément γ_α (resp. H_α) relatif à $\alpha = \alpha_i$. En exprimant que γ_i est changé en son opposé par la réflexion w_i par rapport à α_i et en tenant compte de ce que $\langle \gamma_i, \alpha_i \rangle = 2$, $w_1(\alpha_2) = 3\alpha_1 + \alpha_2$, $w_2(\alpha_1) = \alpha_1 + \alpha_2$, il vient $\langle \gamma_2, \alpha_1 \rangle = -1$, $\langle \gamma_1, \alpha_2 \rangle = -3$. Il en résulte que $\langle \gamma_1, \omega_0 \rangle = 2$, $\langle \gamma_1, \omega_1 \rangle = -1$, $\langle \gamma_1, \omega_2 \rangle = -1$, $\langle \gamma_2, \omega_0 \rangle = -1$, $\langle \gamma_2, \omega_1 \rangle = 1$, $\langle \gamma_2, \omega_2 \rangle = 0$. Les éléments $\omega_i^K(H_j)$ se déduisent des formules que l'on vient d'écrire ; on voit tout de suite que H_1 et H_2 sont linéairement indépendants, donc forment une base de $\mathfrak{t}$, et que pour $H = a_1 H_1 + a_2 H_2$ on a

$$B_\rho(H, H) = 2[6\, a_1^2 - 6\, a_1\, a_2 + 2\, a_2^2] = a_2^2\,.$$

Tenant compte des formules (1), (2), on en conclut que H_1 et X_{α_1} appartiennent au *sous-espace* $\mathfrak{g}_0$ *de* $\mathfrak{g}$ *composé des* X *tels que* $B_\rho(X, Y) = 0$ *pour tout* $Y \in \mathfrak{g}$, mais que ni H_2 ni X_{α_2} n'appartiennent à cet espace. Il résulte de l'invariance de B_ρ par la représentation adjointe que $\mathfrak{g}_0$ est stable pour la représentation adjointe. Or, soit s un élément du normalisateur de T ; il

définit une opération w du groupe de Weyl. Posons, si $t \in T$ et si α est une racine, $sts^{-1} = t'$, $s\,\tau_\alpha(\xi)s^{-1} = \tau'(\xi)$; il vient alors

$$t'\,\tau'(\xi)t'^{-1} = \tau'(\alpha(t)\xi)\,.$$

Or, si $w(\alpha)$ est la transformée de la racine α par w, on a

$$(w(\alpha))(t) = \alpha(s^{-1}\,ts)\ ;$$

la formule précédente montre alors que τ' est un isomorphisme associé à la racine $w(\alpha)$, d'où l'on déduit que Ad s transforme X_α en un multiple scalaire $\neq 0$ de $X_{w(\alpha)}$. La relation $X_{\alpha_1} \in \mathfrak{g}_0$ entraîne donc $X_\alpha \in \mathfrak{g}_0$ pour toute racine α transformée de α_1 par une opération du groupe de Weyl W ; ces racines sont $\pm\alpha_1$, $\pm(\alpha_2+\alpha_1)$, $\pm(\alpha_2+2\,\alpha_1)$. On en conclut que $\mathfrak{g}_0$ est de dimension ≥ 7.

L'espace $\mathfrak{g}/\mathfrak{g}_0$ est l'espace d'une représentation linéaire σ de G. Désignant par X^* la classe modulo $\mathfrak{g}_0$ d'un élément $X \in \mathfrak{g}$, on a $X^*_{\alpha_2} \neq 0$ et $\sigma(t)\cdot X^*_{\alpha_2} = \alpha_2(t)X^*_{\alpha_2}$ si $t \in T$. On en conclut que α_2 est un poids de σ. Il est de même des transformées de α_2 par les opérations de W, *i.e.* des racines $\pm\alpha_2$, $\pm(\alpha_2+3\alpha_1)$, $\pm(2\alpha_2+3\alpha_1)$. De plus, on a $H_2^* \neq 0$, et H_2^* est invariant par les opérations de $\sigma(T)$, ce qui montre que 0 est un poids de σ ; σ est donc de degré ≥ 7. Comme $\mathfrak{g}/\mathfrak{g}_0$ est de dimension ≤ 7, on en conclut que cet espace est de dimension 7.

Nous allons maintenant montrer que cette représentation σ est simple. Observons d'abord que, si X, $Y \in \mathfrak{g}$, $B_\rho(X,Y)$ ne dépend que de X^* et Y^* ; B_ρ définit donc, par passage aux quotients, une forme bilinéaire B^* sur $(\mathfrak{g}/\mathfrak{g}_0)\times(\mathfrak{g}/\mathfrak{g}_0)$ qui est un invariant de la représentation σ. Ceci dit, soit M un sous-espace $\neq \{0\}$ de $\mathfrak{g}/\mathfrak{g}_0$ stable pour $\sigma(G)$. Comme les poids de σ sont tous de multiplicité 1, M est engendré par des vecteurs de $\mathfrak{g}/\mathfrak{g}_0$ qui appartiennent à des poids. Soit σ_M la représentation sur l'espace M ; comme les transformés d'un poids de σ_M par les opérations de W sont encore des poids de σ_M, on voit qu'il n'y a que trois possibilités :

a) on a $M = \mathfrak{g}/\mathfrak{g}_0$;

b) M est engendré par les X^*_α pour toutes les racines $\alpha = \pm\alpha_2$, $\pm(\alpha_2+3\,\alpha_1)$, $\pm(2\,\alpha_2+3\,\alpha_1)$;

c) M est engendré par H_2^*.

De plus, le complémentaire orthogonal de M relativement à la forme bilinéaire B^*, soit M^*, est encore stable par $\sigma(G)$; si donc on était dans le cas b), l'espace KH_2^* serait également stable par $\sigma(G)$. Tout revient donc à établir que KH_2^* n'est pas stable par $\sigma(G)$. Or, supposons pour un moment qu'il en soit ainsi ; comme G est son propre groupe des commutateurs, H_2^* est alors invariant par les opérations de $\sigma(G)$, ce qui signifie que $(\mathrm{Ad}\,s)(H_2) - H_2 \in \mathfrak{g}_0$ pour tout $s \in G$. Or on sait que la représentation $(\mathrm{Ad}\,s)_i$ de $\mathfrak{g}$ déduite de la représentation adjointe de G n'est autre que la représentation adjointe de $\mathfrak{g}$; on en déduit alors que $[X, H_2] \in \mathfrak{g}_0$ pour tout $X \in \mathfrak{g}$. Or il est impossible

qu'il en soit ainsi, car $[H_2, X_{\alpha_2}] = \alpha_2^K(H_2)X_{\alpha_2} = 2X_{\alpha_2}$ n'est pas dans $\mathfrak{g}_0$. Nous avons donc bien établi que la représentation σ est simple. *Son poids dominant est manifestement la racine* $2\alpha_2 + 3\alpha_1$ *qui est le poids dominant* ϖ_2 *relatif à la racine* α_2.

La représentation σ est une isogénie de G sur le groupe $G' = \sigma(G)$; posons $T' = \sigma(T)$, et désignons par φ l'isomorphisme spécial de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(T)$ défini par σ. Son exposant radiciel relatif à la racine α_2 est 1 (n° 20.3, corollaire au lemme 4) ; son exposant radiciel q relatif à la racine α_1 est une puissance de 3. Soient α'_1, α'_2 les racines de $\sigma(G)$ telles que $\varphi(\alpha'_1) = q\alpha'_1$, $\varphi(\alpha'_2) = \alpha_2$. Tenant compte de la proposition 5 du n° 18.3, on voit facilement qu'il n'y a que deux possibilités : ou bien $q = 1$, et les entiers de Cartan relatifs au système fondamental (α'_1, α'_2) sont les mêmes que ceux relatifs au système fondamental (α_1, α_2), ou bien $q = 3$ et les entiers de Cartan relatifs à (α'_1, α'_2) sont les mêmes que ceux relatifs à (α_2, α_1). Nous allons voir que c'est la seconde possibilité qui se réalise. Considérons pour cela la représentation $\overline{\sigma}$ de Z_1 induite par σ. Les sous-espaces $KX^*_{\alpha_2} + KX^*_{\alpha_2+3\alpha_1} = N_1$, $KX^*_{-\alpha_2} + KX^*_{-(\alpha_2+3\alpha_1)} = N_2$, $KX^*_{2\alpha_2+3\alpha_1} = N_3$, $KX^*_{-(2\alpha_2+3\alpha_1)} = N_4$, $KH_2^* = N_5$ sont stables par $\overline{\sigma}(Z_1)$. Les représentations sur N_3, N_4, N_5 sont triviales. Si l'on désigne par $\overline{\alpha}_1$ la restriction de α_1 à T_1, celle de $\overline{\alpha}_2$ est $-\frac{3}{2}\overline{\alpha}_1$ (comme il résulte de la formule $\langle\gamma_1, \alpha_2\rangle = -3$). Les poids de la représentation sur l'un ou l'autre des espaces N_1, N_2 sont donc $\pm\frac{3}{2}\overline{\alpha}_1$; chacune de ces représentations est donc équivalente à la représentation simple de poids dominant $\frac{3}{2}\overline{\alpha}_1$. Comme on est en caractéristique 3, il en résulte que, si $\overline{\sigma}_1$ et $\overline{\sigma}_2$ sont les représentations sur N_1 et N_2 restriction de $\overline{\sigma}$, les coefficients de la matrice qui représente $\overline{\sigma}_i(\tau_1(\xi))$ $(s \in Z_1)$ relativement à une base de N_i sont des polynômes en ξ^3. Tenant compte de la définition des exposants radiciels, on en conclut que l'exposant radiciel de φ relatif à α_1 est 3. Nous avons donc prouvé la :

Proposition 1. – *Si K est de caractéristique 3, et si G est un groupe de type G_2, T un tore maximal de G et (α_1, α_2) un système fondamental de racines de G par rapport à T tel que*[3] *la réflexion par rapport à α_1 transforme α_2 en $\alpha_2 + 3\alpha_1$, il existe une isogénie de G dont les exposants radiciels par rapport à α_1 et α_2 sont 3 et 1 respectivement.*

21.5 Isogénies d'un groupe de type G_2

Théorème 2. – *Soit G un groupe algébrique semi-simple de type G_2, et soit T un tore maximal de G. Soient G' un groupe algébrique semi-simple, T' un tore maximal de G' et φ un isomorphisme spécial de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(T)$. Alors G' est de type G_2 et φ est l'isomorphisme attaché à une isogénie de G sur G' qui applique T sur T'.*

[3] Autrement dit, l'entier de Cartan $c(1,2)$ est égal à 3, puisque l'on a $w_1(\alpha_2) = \alpha_2 + c(1,2)\alpha_1$.

Soit (α_1, α_2) un système fondamental de racines de G par rapport à T tel que l'entier de Cartan $c(1,2)$ relatif à ce système de racines soit 3. Soit (α'_1, α'_2) le système fondamental de racines de G' tel que $\varphi(\alpha'_i) = q_i\,\alpha_i$, q_i étant une puissance de l'exposant caractéristique de K. Soit $c'(1,2)$ l'entier de Cartan relatif à ce système fondamental. On a $3\,q_2 = c'(1,2)\,q_1$ d'après la proposition 5 du n° 18.3 ; comme $c'(1,2)$ ne peut prendre que les valeurs 0, 1, 2 ou 3, on voit que l'on a ou bien $q_1 = q_2$, $c'(1,2) = 3$ ou bien $q_1 = 3q_2$, $c'(1,2) = 1$; ce dernier cas n'est possible que si K est de caractéristique 3 ; de plus, si $q_1 = 3q_2$, on a $c'(2,1) = 3$; G' est donc bien en tous cas de type G_2.

Posons dans tous les cas $q = q_2$; l'isogénie des puissances q-ièmes applique G sur un groupe $\overline{G}$ de type G_2. Soit $\overline{T}$ l'image de T, et soit γ l'isomorphisme correspondant de $X^{\mathbf{Q}}(\overline{T})$ sur $X^{\mathbf{Q}}(T)$. Il existe alors un système fondamental de racines $(\overline{\alpha}_1, \overline{\alpha}_2)$ de $\overline{G}$ par rapport à $\overline{T}$ tel que $\gamma(\overline{\alpha}_i) = q\alpha_i$ $(i = 1, 2)$. L'isomorphisme φ se met sous la forme $\gamma \circ \overline{\varphi}$, où $\overline{\varphi}$ est un isomorphisme de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(T)$ qui applique α'_2 sur α_2 et α'_1 sur α_1 ou $3\alpha_1$ suivant que $q_1 = q_2 = q$ ou que $q_1 = 3q$.

Supposons d'abord $q_1 = q_2$. Il résulte alors de ce qui a été démontré plus haut qu'il existe des représentations simples $\overline{\rho}$, ρ' de $\overline{G}$, G' respectivement qui possèdent les propriétés suivantes : $\overline{\rho}$ (resp. ρ') est de poids dominant $\overline{\alpha}_2 + 2\,\overline{\alpha}_1$ (resp. $\alpha'_2 + 2\alpha'_1$) ; on a $\overline{\rho}(\overline{G}) = \rho'(G')$, $\overline{\rho}(\overline{T}) = \rho'(T')$; si $T^* = \overline{\rho}(\overline{T})$, les exposants radiciels des isomorphismes spéciaux ζ et ζ' de $X^{\mathbf{Q}}(T^*)$ sur $X^{\mathbf{Q}}(\overline{T})$ et $X^{\mathbf{Q}}(T')$ attachés à $\overline{\rho}$ et ρ' sont égaux à 1. Il en résulte que $\overline{\varphi} \circ \zeta' = \zeta$. Par ailleurs, les groupes $X(\overline{T})$ et $X(T')$ sont engendrés par les racines ; il en résulte que $\overline{\varphi}$ est spécial. Faisant usage de la proposition 7 du n° 18.4, on en conclut que $\overline{\varphi}$ est attaché à un isomorphisme de $\overline{G}$ sur G', ce qui démontre le théorème dans ce cas.

Supposons maintenant $q_1 = 3q_2$; la caractéristique de K est alors 3, et nous avons vu au n° 21.4 qu'il existe une isogénie γ_1 de $\overline{G}$ sur un groupe $\overline{\overline{G}}$ qui applique $\overline{T}$ sur un tore maximal $\overline{\overline{T}}$ de $\overline{\overline{G}}$ telle que les exposants radiciels relatifs à $\overline{\alpha}_1$ et $\overline{\alpha}_2$ de l'isomorphisme spécial ζ_1 attaché à cette isogénie soient 3 et 1 respectivement. On peut alors écrire $\overline{\varphi} = \zeta_1 \circ \overline{\overline{\varphi}}$, où $\overline{\overline{\varphi}}$ est un isomorphisme spécial de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(\overline{\overline{T}})$ dont les exposants radiciels sont égaux à 1. On conclut comme plus haut que $\overline{\overline{\varphi}}$ est attaché à un isomorphisme de $\overline{\overline{G}}$ sur G' qui applique $\overline{\overline{T}}$ sur T', ce qui achève la démonstration du théorème.

22. Les groupes de type C_n [1]

22.1 Le groupe Sp n

Soit β la forme bilinéaire sur $K^{2n} \times K^{2n}$ définie par

$$\beta(x,y) = \sum_{i=1}^{n} (\xi_i \, \eta_{i+n} - \xi_{i+n} \, \eta_i)$$

si $x = (\xi_1, \ldots, \xi_{2n})$, $y = (\eta_1, \ldots, \eta_{2n})$. Nous désignerons par $\mathrm{Sp}\, n$ le groupe des automorphismes de K^{2n} qui laissent la forme β invariante. On montre facilement que, si (x,y) et (x',y') sont deux éléments de $K^{2n} \times K^{2n}$ tels que $\beta(x,y) = \beta(x',y') = 1$, il existe une opération de $\mathrm{Sp}\, n$ qui transforme x en x' et y en y' (cela résulte immédiatement de la théorie de la réduction des formes bilinéaires alternées). Soit $(e_1, \ldots, e_{2n})$ la base canonique de K^{2n}. Les opérations de $\mathrm{Sp}\, n$ qui laissent fixes les points e_n, e_{2n} forment un sous-groupe G isomorphe à $\mathrm{Sp}\,(n-1)$, et on a une bijection naturelle de l'espace homogène $\mathrm{Sp}\, n/G$ sur l'ensemble des points (x,y) de $K^{2n} \times K^{2n}$ tels que $\beta(x,y) = 1$, ensemble qui est évidemment une hypersurface quadrique irréductible. Comme $\mathrm{Sp}\, 1 = \mathrm{SL}(K^2)$ est connexe, on en déduit par récurrence sur n que $\mathrm{Sp}\, n$ est connexe. Comme $\mathrm{Sp}\, n$ opère transitivement sur l'ensemble des éléments $\neq 0$ de K^{2n}, son application identique dans $\mathrm{GL}\,(K^{2n})$ est une représentation simple. Soit T l'ensemble des matrices diagonales appartenant à $\mathrm{Sp}\, n$; pour qu'une matrice diagonale $\mathrm{diag}\,(a_1, \ldots, a_{2n})$ appartienne à T, il faut et il suffit que l'on ait $a_i \, a_{i+n} = 1$ $(1 \leq i \leq n)$. Il en résulte que T contient une matrice $t_0 = \mathrm{diag}\,(a_1, \ldots, a_{2n})$ telle que les a_i soient tous distincts ; le centralisateur de t_0 dans $\mathrm{GL}\,(K^{2n})$ étant le groupe des matrices inversibles diagonales, on voit que T est son propre centralisateur dans $\mathrm{Sp}\, n$, donc est un tore maximal de $\mathrm{Sp}\, n$. Il résulte du lemme de Schur qu'une matrice z_0 du centre de $\mathrm{Sp}\, n$ est de la forme cI, $c \in K$, I étant la matrice unité ; exprimant que $cI \in \mathrm{Sp}\, n$, il vient $c = \pm 1$; le centre de $\mathrm{Sp}\, n$ est donc d'ordre 2 ou 1 suivant que la caractéristique de K est $\neq 2$ ou $= 2$. Ce centre étant fini, $\mathrm{Sp}\, n$ est semi-simple (n° 20.1, lemme 1). Posons, pour $t \in T$, $t \cdot e_i = \omega_i(t) e_i$; il est clair que l'on a (en notation additive) $\omega_{i+n} = -\omega_i$ et que $\omega_1, \ldots, \omega_n$ forment une base du groupe $X(T)$ des caractères rationnels de T.

[1] Exposé de C. Chevalley, le 13.1.1958

Soient i et j des indices distincts entre 1 et n ; si $\xi \in K$, les formules

$$\begin{aligned}
&\tau_{ij}(\xi)\cdot e_i = e_i + \xi e_j\\
&\tau_{ij}(\xi)\cdot e_{j+n} = e_{j+n} - \xi e_{i+n}\\
&\tau_{ij}(\xi)\cdot e_k = e_k \qquad \text{si } k \neq i, j+n
\end{aligned}$$

$$\begin{aligned}
&\tau'_{ij}(\xi)\cdot e_{i+n} = e_{i+n} + \xi e_j\\
&\tau'_{ij}(\xi)\cdot e_{j+n} = e_{j+n} + \xi e_i\\
&\tau'_{ij}(\xi)\cdot e_k = e_k \qquad \text{si } k \neq i+n, j+n
\end{aligned}$$

$$\begin{aligned}
&\tau''_{ij}(\xi)\cdot e_i = e_i + \xi e_{j+n}\\
&\tau''_{ij}(\xi)\cdot e_j = e_j + \xi e_{i+n}\\
&\tau''_{ij}(\xi)\cdot e_k = e_k \qquad \text{si } k \neq i, j
\end{aligned}$$

$$\begin{aligned}
&\tau_i(\xi)\cdot e_{i+n} = e_{i+n} + \xi e_i\\
&\tau_i(\xi)\cdot e_k = e_k \qquad \text{si } k \neq i+n
\end{aligned}$$

$$\begin{aligned}
&\tau'_i(\xi)\cdot e_i = e_i + \xi e_{i+n}\\
&\tau'_i(\xi)\cdot e_k = e_k \qquad \text{si } k \neq i
\end{aligned}$$

définissent des automorphismes $\tau_{ij}(\xi)$, $\tau'_{ij}(\xi)$, $\tau''_{ij}(\xi)$, $\tau_i(\xi)$, $\tau'_i(\xi)$ de K^{2n}. On vérifie facilement que ces automorphismes appartiennent à $\mathrm{Sp}\, n$, et que les applications $\xi \to \tau_{ij}(\xi)$, $\xi \to \tau'_{ij}(\xi)$, $\xi \to \tau''_{ij}(\xi)$, $\xi \to \tau_i(\xi)$, $\xi \to \tau'_i(\xi)$ sont des isomorphismes de K sur des sous-groupes de $\mathrm{Sp}\, n$. De plus, on a, si $t \in T$,

$$\begin{aligned}
&t\,\tau_{ij}(\xi)\,t^{-1} = \tau_{ij}(\omega_j(t)(\omega_i(t))^{-1}\,\xi)\\
&t\,\tau'_{ij}(\xi)\,t^{-1} = \tau'_{ij}(\omega_i(t)\,\omega_j(t)\,\xi)\\
&t\,\tau''_{ij}(\xi)\,t^{-1} = \tau''_{ij}((\omega_i(t)\,\omega_j(t))^{-1}\,\xi)\\
&t\,\tau_i(\xi)\,t^{-1} = \tau_i((\omega_i(t))^2\,\xi)\\
&t\,\tau'_i(\xi)\,t^{-1} = \tau'_i((\omega_i(t))^{-2}\,\xi)\,.
\end{aligned}$$

Il en résulte que $\omega_i - \omega_j$, $\pm(\omega_i + \omega_j)$, $\pm 2\omega_i$ sont des racines de $\mathrm{Sp}\, n$. Or il résulte de ce qui a été dit plus haut que l'on a, pour $n > 1$,

$$\dim \mathrm{Sp}\, n = \dim \mathrm{Sp}\,(n-1) + 4n - 1\ ;$$

comme $\dim \mathrm{Sp}\, 1 = 3$, on a $\dim \mathrm{Sp}\, n = n(2n+1)$. Comme on a $\dim T = n$, il en résulte que le nombre des racines de $\mathrm{Sp}\, n$ est $2n^2 = 2n(n-1) + 2n$, donc que les racines que nous avons déjà trouvées sont toutes les racines. Il est clair que $\omega_1 - \omega_2, \ldots, \omega_{n-1} - \omega_n$, $2\omega_n$ forment un système fondamental de racines et que le diagramme de Dynkin correspondant est de type C_n. De plus, on sait que le groupe des poids est engendré par les ω_i ; le groupe $\mathrm{Sp}\, n$ est donc un groupe simplement connexe de type C_n (si $n > 1$).

Le groupe projectif associé à $\mathrm{Sp}\, n$ s'appelle le *groupe symplectique projectif*, et se note $\mathrm{PSp}\, n$. Soit f l'application canonique de $\mathrm{Sp}\, n$ sur $\mathrm{PSp}\, n$, et soit $f(T) = T'$. L'isogénie f définit un isomorphisme spécial φ de $X^{\mathbf{Q}}(T')$

sur $X^{\mathfrak{Q}}(T)$; on sait (proposition 4 du n° 18.3) que les exposants radiciels de φ sont tous égaux à 1, d'où il résulte que $\mathrm{PSp}\, n$ est encore de type C_n. De plus, $\varphi(X(T'))$ est engendré par les différences mutuelles des éléments $\pm\omega_i$ de $X(T)$; ce groupe n'est donc autre que le groupe des racines. Il en résulte que, dans le cas de $\mathrm{PSp}\, n$, $X(T')$ est engendré par les racines.

22.2 Le groupe SO(2n + 1)

Désignons par $e_0, \ldots, e_{2n}$ la base canonique de K^{2n+1} et par $\mathrm{SO}(2n+1)$ le groupe des automorphismes de déterminant 1 de K^{2n+1} qui conservent la forme quadratique Q définie par

$$Q\Big(\sum_{i=0}^{2n} \xi_i\, e_i\Big) = \xi_0^2 + \sum_{i=1}^{n} \xi_i\, \xi_{i+n}\,.$$

Supposons d'abord que K ne soit pas de caractéristique 2. Dans ce cas, la forme quadratique Q est non dégénérée ; désignons par β le forme bilinéaire associée à cette forme quadratique. Il résulte du théorème de Witt que, si $n > 0$, les opérations de $\mathrm{SO}(2n+1)$ permutent transitivement entre eux les couples (x, y) de points de K^{2n+1} tels que $Q(x) = 1$, $Q(y) = -1$, $\beta(x, y) = 0$; ces couples forment une variété irréductible de dimension $4n-1$ dans $K^{2n+1} \times K^{2n+1}$. Par ailleurs, les opérations de $\mathrm{SO}(2n+1)$ qui laissent fixes les deux points $x_0 = e_n + e_{2n}$, $y_0 = e_n - e_{2n}$ forment un groupe qui est manifestement isomorphe à $\mathrm{SO}(2n-1)$. On en conclut, en procédant par récurrence sur n, que $\mathrm{SO}(2n+1)$ est un groupe connexe de dimension $n(2n+1)$. Procédant comme dans le cas de $\mathrm{Sp}\, n$, on voit que les matrices diagonales

$$t = (a_0, a_1, \ldots, a_{2n})$$

contenues dans $\mathrm{SO}(2n+1)$ sont celles pour lesquelles on a $a_0 = 1$, $a_i\, a_{i+n} = 1$ $(1 \leq i \leq n)$; elles forment un tore maximal T, et le groupe des caractères rationnels de T est engendré par $\omega_1, \ldots, \omega_n$ si $t \cdot e_i = \omega_i(t) e_i$ $(0 \leq i \leq 2n)$. *Montrons que l'application identique de* $\mathrm{SO}(2n+1)$ *dans* $\mathrm{GL}(K^{2n+1})$ *est une représentation simple.* Soit V un sous-espace $\neq \{0\}$ de K^{2n+1} stable par les opérations de $\mathrm{SO}(2n+1)$; V est stable par les opérations de T ; comme les fonctions 1, ω_i, ω_i^{-1} sur T sont toutes distinctes, il en résulte que V est engendré par ceux des vecteurs $e_0, e_1, \ldots, e_{2n}$ qu'il contient. Or, si $n > 0$, les opérations de $\mathrm{SO}(2n+1)$ permutent transitivement les vecteurs x non nuls tels que $Q(x) = 1$; si donc $e_0 \in V$, V contient aussi les vecteurs $e_0 + e_i$ $(1 \leq i \leq 2n)$, d'où $V = K^{2n+1}$. Par ailleurs, les opérations de $\mathrm{SO}(2n+1)$ permutent aussi transitivement entre eux les vecteurs x non nuls tels que $Q(x) = 0$; si donc $e_i \in V$ pour un $i > 0$, V contient aussi e_{i+n}, donc contient $e_i + e_{i+n}$ et par suite aussi e_0, ce qui achève de montrer que $V = K^{2n+1}$. Comme tout élément du centre de $\mathrm{SO}(2n+1)$ est une matrice scalaire, on

voit tout de suite que le centre de $\mathrm{SO}(2n+1)$ se réduit à son élément neutre. Il en résulte que $\mathrm{SO}(2n+1)$ *est un groupe semi-simple* (lemme 1 du n° 20.1).

Si K est de caractéristique 2, la forme bilinéaire β associée à Q est dégénérée ; l'espace des vecteurs x tels que $\beta(x,y) = 0$ pour tout $y \in K^{2n+1}$ est Ke_0. On en déduit l'existence d'une *représentation linéaire ω de* $\mathrm{SO}(2n+1)$ *opérant dans* K^{2n+1}/Ke_0. Cette représentation est injective. Soit en effet s un élément de $\mathrm{SO}(2n+1)$ tel que $\omega(s)$ soit l'identité ; on a donc

$$s \cdot x = x + u(x)e_0$$

pour tout $x \in K^{2n+1}$; on a $Q(x) = Q(s \cdot x) = Q(x) + u(x)^2$, d'où $u(x) = 0$, ce qui démontre notre assertion. Par ailleurs, $\beta(x,y)$ ne dépend que des classes de x, y modulo Ke_0, de sorte que β définit une forme bilinéaire $\overline{\beta}$ sur $(K^{2n+1}/Ke_0) \times (K^{2n+1}/Ke_0)$, évidemment invariante par les opérations de $\omega(\mathrm{SO}(2n+1))$. On a $\beta(x,x) = 2Q(x) = 0$, ce qui montre que $\overline{\beta}$ est alternée. La restriction de Q à l'espace engendré par $e_1, \ldots, e_{2n}$ étant une forme quadratique non dégénérée sur cet espace, la forme bilinéaire $\overline{\beta}$ est non dégénérée. Montrons que tout automorphisme $\overline{s}$ de K^{2n+1}/Ke_0 qui laisse la forme $\overline{\beta}$ invariante appartient à $\omega(\mathrm{SO}(2n+1))$. Soit r l'application canonique de K^{2n+1} sur K^{2n+1}/Ke_0, et soit W l'espace engendré par $e_1, \ldots, e_{2n}$; il y a un automorphisme s^* de K^{2n+1} qui laisse e_0 fixe, qui transforme W en lui-même et qui est tel que $r \circ s^* = \overline{s} \circ r$. Il est clair que s^* laisse invariante la forme bilinéaire β ; si donc on pose $Q_1(x) = Q(s^* \cdot x) - Q(x)$, Q_1 est une forme quadratique dont la forme bilinéaire associée est nulle. Comme K est algébriquement clos, Q_1 est le carré d'une forme linéaire u ; on a $u(e_0) = 0$. Posons $s \cdot x = s^* \cdot x + u(x)e_0$; on a encore $r \circ s = \overline{s} \circ r$, $s(e_0) = e_0$, de sorte que s est un automorphisme ; son déterminant est égal à celui de $\overline{s}$, donc à 1. On a $Q(s \cdot x) = Q(s^* \cdot x) + u(x)^2$, ce qui montre que $s \in \mathrm{SO}(2n+1)$; il est clair que $\omega(s) = \overline{s}$. *Le groupe $\omega(\mathrm{SO}(2n+1))$ est donc isomorphe à* $\mathrm{Sp}\, n$ *; ω étant une isogénie, on voit que* $\mathrm{SO}(2n+1)$ *est encore semi-simple dans ce cas.* De plus, le groupe T des matrices diagonales contenues dans $\mathrm{SO}(2n+1)$ est encore un tore maximal ; nous définirons les ω_i comme plus haut. On notera que $\dim \mathrm{SO}(2n+1) = \dim \mathrm{Sp}\, n = n(2n+1)$.

Revenons au cas général. Si i et j sont des indices distincts entre 1 et n, les formules

$$\begin{aligned}
&\tau_{ij}(\xi) \cdot e_i = e_i + \xi e_j \\
&\tau_{ij}(\xi) \cdot e_{j+n} = e_{j+n} - \xi e_{i+n} \\
&\tau_{ij}(\xi) \cdot e_k = e_k \qquad \text{si } k \neq i, j+n
\end{aligned}$$

$$\begin{aligned}
&\tau'_{ij}(\xi) \cdot e_{i+n} = e_{i+n} + \xi e_j \\
&\tau'_{ij}(\xi) \cdot e_{j+n} = e_{j+n} - \xi e_i \\
&\tau'_{ij}(\xi) \cdot e_k = e_k \qquad \text{si } k \neq i+n, j+n
\end{aligned}$$

$$\begin{aligned}
&\tau''_{ij}(\xi) \cdot e_i = e_i + \xi e_{j+n} \\
&\tau''_{ij}(\xi) \cdot e_j = e_j - \xi e_{i+n} \\
&\tau''_{ij}(\xi) \cdot e_k = e_k \qquad \text{si } k \neq i, j
\end{aligned}$$

$$\begin{aligned}
&\tau_i(\xi)\cdot e_{i+n} = e_{i+n} + \xi e_0 - \xi^2\, e_i\\
&\tau_i(\xi)\cdot e_0 = e_0 - 2\xi\, e_i\\
&\tau_i(\xi)\cdot e_k = e_k \qquad \text{si } k \neq 0, i+n
\end{aligned}$$

$$\begin{aligned}
&\tau'_i(\xi)\cdot e_i = e_i + \xi e_0 - \xi^2\, e_{i+n}\\
&\tau'_i(\xi)\cdot e_0 = e_0 - 2\xi\, e_{i+n}\\
&\tau'_i(\xi)\cdot e_k = e_k \qquad \text{si } k \neq 0, i
\end{aligned}$$

définissent des automorphismes de K^{2n+1} ; on vérifie facilement que ces automorphismes appartiennent à $\mathrm{SO}(2n+1)$ et que les applications $\xi \to \tau_{ij}(\xi)$, $\xi \to \tau'_{ij}(\xi)$, $\xi \to \tau''_{ij}(\xi)$, $\xi \to \tau_i(\xi)$, $\xi \to \tau'_i(\xi)$ sont des isomorphismes de K sur des sous-groupes de $\mathrm{SO}(2n+1)$. De plus on a, si $t \in T$,

$$\begin{aligned}
&t\,\tau_{ij}(\xi)\,t^{-1} = \tau_{ij}(\omega_j(t)(\omega_i(t))^{-1}\,\xi)\\
&t\,\tau'_{ij}(\xi)\,t^{-1} = \tau'_{ij}(\omega_i(t)\,\omega_j(t)\,\xi)\\
&t\,\tau''_{ij}(\xi)\,t^{-1} = \tau''_{ij}((\omega_i(t)\,\omega_j(t))^{-1}\,\xi)\\
&t\,\tau_i(\xi)\,t^{-1} = \tau_i(\omega_i(t)\,\xi)\\
&t\,\tau'_i(\xi)\,t^{-1} = \tau'_i((\omega_i(t))^{-1}\,\xi)\,.
\end{aligned}$$

Procédant comme dans le cas de $\mathrm{Sp}\,n$, on voit que $\mathrm{SO}(2n+1)$ *est de type* B_n (en convenant que $B_1 = A_1$, $B_2 = C_2$).

On notera que, si K est de caractéristique 2, et si ω désigne l'isogénie construite ci-dessus, $\omega \circ \tau_{ij}$, $\omega \circ \tau'_{ij}$, $\omega \circ \tau''_{ij}$ sont des isomorphismes de K sur des sous-groupes de $\omega(\mathrm{SO}(2n+1))$, tandis que $(\omega \circ \tau_i)(\xi) = \overline{\tau}_i(\xi^2)$, $(\omega \circ \tau'_i)(\xi) = \overline{\tau}'_i(\xi^2)$, $\overline{\tau}_i$ et $\overline{\tau}'_i$ étant des isomorphismes de K sur des sous-groupes de $\omega(\mathrm{SO}(2n+1))$.

22.3 Les groupes de type C_n

Soit G un groupe algébrique semi-simple de type C_n. Soient T un tore maximal de G et $\omega_1, \ldots, \omega_n$ des éléments de $X^{\mathbf{Q}}(T)$ tels que les racines soient les $\pm(\omega_i \pm \omega_j)$ $(i < j)$, $\pm 2\omega_i$. Posons

$$\alpha_1 = \omega_1 - \omega_2, \ldots, \alpha_{n-1} = \omega_{n-1} - \omega_n\,,\ \alpha_n = 2\omega_n\ ;$$

les α_i forment alors un système fondamental de racines. Le poids dominant fondamental ϖ_1 qui correspond à α_1 est ω_1 ; soit ρ une représentation projective simple admettant ω_1 comme poids dominant. Le poids ω_1 est un poids dominant minimal et n'est pas combinaison linéaire à coefficients entiers des racines ; les poids de ρ sont donc les transformés $\pm\omega_i$ $(1 \leq i \leq n)$ de ω_1 par les opérations du groupe de Weyl et sont de multiplicité 1 (n° 20.2, proposition 1 et son corollaire). La représentation ρ est donc de degré $2n$; elle opère sur l'espace projectif $P(V)$ associé à un espace vectoriel V de dimension $2n$. De plus, l'automorphisme de $X^{\mathbf{Q}}(T)$ qui change tout élément en son opposé appartient au groupe de Weyl ; toute représentation projective

de G est donc équivalente à sa contragrédiente (corollaire à la proposition 2 du n° 20.3). On en conclut que, si G' est le groupe linéaire associé à ρ, les opérations de G' laissent invariante une forme bilinéaire non dégénérée β sur $V \times V$, symétrique ou alternée. Nous allons montrer que β est alternée. Posons $Q(x) = \beta(x, x)$; c'est une forme quadratique sur V, invariante par les opérations de G' ; les opérations de G' laissent invariante la forme bilinéaire β' associée à Q. Comme l'application identique de G' dans $\mathrm{GL}(V)$ est une représentation simple, β' est ou bien nulle ou bien non dégénérée ; dans le second cas, Q est non dégénérée. Or, on a

$$\dim G' = \dim \rho(G) = \dim G = n(2n+1)\,,$$

et l'on sait que le groupe orthogonal d'une forme quadratique non dégénérée sur un espace de dimension $2n$ est de dimension $n(2n-1)$. Il est donc impossible que $\beta' \neq 0$. Si K est de caractéristique $\neq 2$, il en résulte que $Q = 0$; si K est de caractéristique 2, il en résulte que Q est le carré d'une forme linéaire ; mais cette dernière, étant invariante par G', est nulle. On a donc bien $Q = 0$ dans tous les cas, et β est alternée. Or le groupe de tous les automorphismes de V qui invarient la forme β est de dimension $n(2n+1)$ égale à celle de G', et lui est par suite identique ; il en résulte que ce groupe est G', donc que G' est isomorphe à $\mathrm{Sp}\, n$ et que $\rho(G)$ est isomorphe à $\mathrm{PSp}\, n$. Nous allons maintenant déterminer les exposants radiciels de l'isomorphisme spécial attaché à ρ.

Plus généralement, on a la

Proposition 1. – *Soit G un groupe algébrique semi-simple de type C_n et soit $f : G \to \overline{G}$ une isogénie. On a deux possibilités :*

a) *Le corps K est de caractéristique 2, le groupe $\overline{G}$ est semi-simple de type B_n, et les exposants radiciels de l'isomorphisme spécial attaché à f sont $q, \ldots, q, 2q$ (où q est une puissance de 2).*

b) *Le groupe $\overline{G}$ est semi-simple de type C_n et les exposants radiciels de l'isomorphisme spécial attaché à f sont tous égaux.*

Posons $\overline{T} = f(T)$, et soit φ l'isomorphisme spécial de $X^{\mathbf{Q}}(\overline{T})$ sur $X^{\mathbf{Q}}(T)$ attaché à f. Soit $\overline{\alpha}_i$ la racine de $\overline{G}$ telle que $\varphi(\overline{\alpha}_i) = q_i\, \alpha_i$, q_i étant une puissance de l'exposant caractéristique de K. Les racines $\alpha_1, \ldots, \alpha_{n-1}$ sont les transformées les unes des autres par des opérations du groupe de Weyl ; les nombres $q_1, \ldots, q_{n-1}$ sont donc égaux entre eux (n° 18.3, proposition 5) ; soit q' leur valeur commune, et soit $q'' = q_n$. Soient $c(i,j)$ (resp. $\overline{c}(i,j)$) les entiers de Cartan du système fondamental $(\alpha_1, \ldots, \alpha_n)$ (resp. du système fondamental $(\overline{\alpha}_1, \ldots, \overline{\alpha}_n)$) ; on sait que l'on a

$$c(i,j) = \overline{c}(i,j)\, q_i\, q_j^{-1}$$

(n° 18.3, proposition 5). On en conclut que $c(i, i+1) = 1$ si $1 \leq i \leq n-2$, $2 = \overline{c}(n-1, n)\, q'\, q''^{-1}$. Comme $\overline{c}(n-1, n)$ ne peut prendre que les valeurs

1, 2 ou 3, on a ou bien $\overline{c}(n-1,n) = 1$, $q' = 2q''$ ou bien $\overline{c}(n-1,n) = 2$, $q' = q''$. Dans le premier cas, K est nécessairement de caractéristique 2 et l'on a $\overline{c}(n, n-1) = 2$, de sorte que $\overline{G}$ est de type B_n. Dans le second cas, $\overline{G}$ est de type C_n. C.Q.F.D.

Revenons maintenant au cas où f est la représentation projective ρ considérée ci-dessus ; on sait que l'on a alors $q_1 = 1$ (n° 20.3, corollaire au lemme 4), de sorte qu'on se trouve dans le second cas (cela résulte d'ailleurs aussi de ce que $\rho(G)$, étant isomorphe à $\mathrm{PSp}\, n$, est de type C_n). Les exposants radiciels de ρ sont donc tous égaux à 1. Nous avons donc prouvé que *tout groupe semi-simple G de type C_n admet une isogénie sur* $\mathrm{PSp}\, n$ *dont tous les exposants radiciels sont égaux à* 1.

Soit G^* un autre groupe de type C_n, et soit T^* un tore maximal de G^*. Soit $(\alpha_1^*, \ldots, \alpha_n^*)$ un système fondamental de racines de G^* tel que le diagramme de Dynkin correspondant soit

Il existe un isomorphisme de $X^{\mathbf{Q}}(T^*)$ sur $X^{\mathbf{Q}}(T)$ qui applique α_i^* sur α_i $(1 \leq i \leq n)$. Si cet isomorphisme applique $X(T^*)$ sur $X(T)$, les groupes G et G^* sont isomorphes (n° 18.4, proposition 7). Par ailleurs, dans le cas d'un groupe de type C_n, le groupe des poids contient le groupe des racines comme sous-groupe d'indice 2. On en conclut que, si l'indice dans $X(T^*)$ du groupe des racines de G^* est égal à l'indice dans $X(T)$ du groupe des racines de G, G et G^* sont isomorphes. Nous arrivons donc au résultat suivant :

Théorème 1. – *Tout groupe algébrique semi-simple de type C_n est isomorphe à l'un ou l'autre des groupes* $\mathrm{Sp}\, n$ *ou* $\mathrm{PSp}\, n$.

22.4 Isogénies d'un groupe de type C_2

Nous nous proposons de démontrer le théorème suivant :

Théorème 2. – *Soit G un groupe algébrique semi-simple de type C_2 ; soit T un tore maximal de G. Soient G' un groupe algébrique semi-simple et T' un tore maximal de G'. Supposons qu'il existe un isomorphisme spécial φ de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(T)$; φ est alors attaché à une isogénie de G sur G' qui applique T sur T'.*

On sait déjà qu'il existe[2] un groupe simplement connexe G_0 de type C_2 et une isogénie f_0 de G_0 sur G ; si T_0 est le tore maximal de G_0 tel que $f(T_0) = T$, f_0 définit un isomorphisme spécial φ_0 de $X^{\mathbf{Q}}(T)$ sur $X^{\mathbf{Q}}(T_0)$. L'application $\varphi_0 \circ \varphi$ est un isomorphisme spécial de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(T_0)$; s'il

[2] Le groupe $\mathrm{Sp}\, 2$ est simplement connexe, de type C_2, et l'on utilise le théorème 1 !

est attaché à une isogénie de G_0 sur G', le théorème sera établi en vertu de la proposition 6 du n° 18.4. On peut donc supposer G simplement connexe[3]. Soit (α_1, α_2) un système fondamental de racines de G tel que le diagramme de Dynkin correspondant soit

Soient q_1 et q_2 les exposants radiciels de φ relativement à α_1 et α_2 ; d'après la proposition 1, on a ou bien $q_1 = q_2$ ou bien $q_1 = 2q_2$. L'isogénie des puissances q_2-ièmes applique G sur un groupe $\overline{G}$ et T sur un tore $\overline{T}$; il lui correspond un isomorphisme spécial $\overline{\varphi}$ de $X^{\mathbf{Q}}(\overline{T})$ sur $X^{\mathbf{Q}}(T)$ dont les exposants radiciels sont égaux à q_2. Comme $\overline{\varphi}$ applique $X(\overline{T})$ sur $q_2\, X(T)$, il est clair que $\overline{G}$ est encore simplement connexe. L'isomorphisme φ se met sous la forme $\overline{\varphi} \circ \varphi_1$, où φ_1 est un isomorphisme de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(\overline{T})$, qui applique le groupe des racines de G' dans celui de $\overline{G}$. Comme $\overline{G}$ est simplement connexe, φ_1 est spécial. Si φ_1 est attaché à une isogénie de $\overline{G}$ sur G', φ est attaché à une isogénie de G sur G'. Nous pouvons donc nous ramener au cas où G est simplement connexe et $q_2 = 1$. Supposons désormais qu'il en soit ainsi.

Considérons d'abord le cas où l'on a aussi $q_1 = 1$. Soit T'' un tore maximal de $\mathrm{PSp}\,2$ et soit (α_1'', α_2'') un système fondamental de racines de $\mathrm{PSp}\,2$ par rapport à T'' tel que le diagramme de Dynkin correspondant soit

Nous savons qu'il existe des isogénies g et g' de G et G' sur $\mathrm{PSp}\,2$ telles que $g(T) = g'(T') = T''$ et que les isomorphismes spéciaux γ, γ' attachés à g et g' appliquent α_i'' sur α_i et α_i' respectivement, α_i' étant la racine de G' telle que $\varphi(\alpha_i') = \alpha_i$. On a $\gamma = \varphi \circ \gamma'$; il en résulte que φ est attaché à une isogénie de G sur G' (n° 18.4, proposition 7).

Considérons maintenant le cas où $q_1 = 2$; K est alors de caractéristique 2. Posons $G^* = \mathrm{SO}(5)$, $G^{**} = \mathrm{Sp}\,2$; nous avons vu au n° 22.2 qu'il existe une isogénie ω de G^* sur G^{**}, des tores maximaux T^* et T^{**} de G^* et G^{**} respectivement tels que $\omega(T^*) = T^{**}$ et des systèmes fondamentaux de racines (α_1^*, α_2^*) et $(\alpha_1^{**}, \alpha_2^{**})$ de G^* et G^{**} qui possèdent les propriétés suivantes : les diagrammes de Dynkin associés à ces systèmes fondamentaux sont tous deux le diagramme

et les exposants radiciels de l'isomorphisme spécial θ de $X^{\mathbf{Q}}(T^{**})$ sur $X^{\mathbf{Q}}(T^*)$ attaché à ω sont 2 et 1 respectivement[4]. Par ailleurs, $\mathrm{SO}(5)$ est de type

[3] C'est-à-dire isomorphe à $\mathrm{Sp}\,2$.

[4] Prendre garde que l'on a $2\,\alpha_1^* = \theta(\alpha_2^{**})$ et $\alpha_2^* = \theta(\alpha_1^{**})$!

$B_2 = C_2$ et $\mathrm{Sp}\,2$ est simplement connexe de type C_2 ; comme G est simplement connexe de même type que $\mathrm{SO}(5)$, il existe donc des isogénies g de G sur $\mathrm{SO}(5)$ et g' de $\mathrm{Sp}\,2$ sur G' telles que $g(T) = T^*$, $g'(T^{**}) = T'$ et que les exposants radiciels des isomorphismes spéciaux γ et γ' attachés à g et g' soient égaux à 1. On a alors $\varphi = \gamma \circ \theta \circ \gamma'$; il en résulte que φ est attaché à l'isogénie $g' \circ \omega \circ g$ de G sur G', ce qui achève la démonstration du théorème.

22.5 Isogénies d'un groupe de type $A_1 + A_1$

Théorème 3. – *Soient G un groupe algébrique semi-simple de type $A_1 + A_1$ et T un tore maximal de G. Soient G' un groupe algébrique semi-simple et T' un tore maximal de G'. Supposons qu'il existe un isomorphisme spécial φ de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(T)$; G' est alors de type $A_1 + A_1$ et φ est attaché à une isogénie de G sur G' qui applique T sur T'.*

Il résulte immédiatement de la proposition 5 du n° 18.3 que G' est de type $A_1 + A_1$. Soit $\overline{G}$ le groupe $\mathrm{SL}(K^2) \times \mathrm{SL}(K^2)$, et soit $\overline{T}$ un tore maximal de $\overline{G}$. Le groupe $\overline{G}$ est manifestement simplement connexe. On voit facilement qu'il existe des isomorphismes spéciaux γ et γ' de $X^{\mathbf{Q}}(T)$ et $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(\overline{T})$ tels que $\gamma' = \gamma \circ \varphi$. Tenant compte de la proposition 6 du n° 18.4, on voit qu'il suffit de démontrer le théorème 3 dans le cas où $G = \mathrm{SL}(K^2) \times \mathrm{SL}(K^2)$. Soit (α_1, α_2) un système fondamental de racines de G par rapport à T ; soient α'_1 et α'_2 les racines de G' par rapport à T' telles que $\varphi(\alpha'_i) = q_i\,\alpha_i$ $(i = 1, 2)$, les q_i étant des puissances de l'exposant caractéristique de K. Si $i = 1$ ou 2, les racines α_i, $-\alpha_i$ (resp. α'_i, $-\alpha'_i$) forment un système fermé de racines de G (resp. G') ; il lui correspond un sous-groupe G_i (resp. G'_i) de G (resp. G') ; G_i est isomorphe à $\mathrm{SL}(K^2)$; on a $G = G_1\,G_2$, $G' = G'_1\,G'_2$ et tout élément de G_1 (resp. G'_1) commute à tout élément de G_2 (resp. G'_2). Le groupe G_i (resp. G'_i) possède un tore maximal T_i (resp. T'_i) contenu dans T (resp. T') et l'on a $T = T_1\,T_2$, $T' = T'_1\,T'_2$. La restriction $\overline{\alpha}_i$ (resp. $\overline{\alpha}'_i$) de α_i (resp. α'_i) à T_i (resp. T'_i) est une racine de G_i (resp. G'_i)[5]. Comme G_i est isomorphe à $\mathrm{SL}(K^2)$, il existe une isogénie f_i de G_i sur G'_i qui applique T_i sur T'_i telle que l'isomorphisme spécial φ_i de $X^{\mathbf{Q}}(T'_i)$ sur $X^{\mathbf{Q}}(T_i)$ attaché à f_i applique α'_i sur $q_i\,\alpha_i$. Comme l'application $(s_1, s_2) \to s_1\,s_2$ est un isomorphisme de $G_1 \times G_2$ sur G, il existe une isogénie f de G sur G' telle que $f(s_1\,s_2) = f_1(s_1)\,f_2(s_2)$ si $s_i \in G_i$ $(i = 1, 2)$. Il est clair que f applique T sur T' et que l'isomorphisme spécial de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(T)$ attaché à f est φ, ce qui démontre le théorème.

[5] Pour toutes ces affirmations, voir le théorème 1 du n° 17.2, le corollaire de la proposition 1 du n° 17.3 et le théorème 2 du n° 17.4.

23. Existence d'isogénies [1]

23.1 Existence de groupes simplement connexes

Proposition 1. – *Soit G un groupe algébrique semi-simple. Il existe alors une isogénie h d'un groupe algébrique semi-simple simplement connexe G' sur G. De plus, T étant un tore maximal de G et T' le tore maximal de G' tel que $h(T') = T$, on peut supposer que les exposants radiciels de l'isomorphisme spécial η de $X^{\mathbf{Q}}(T)$ sur $X^{\mathbf{Q}}(T')$ attaché à h sont tous égaux à 1.*

Soit $(\alpha_1, \ldots, \alpha_n)$ un système fondamental de racines de G par rapport à T ; soit ϖ_i le poids dominant fondamental relatif à α_i et soit ρ_i une représentation projective simple de poids dominant ϖ_i de G (proposition 5 du n° 15.3). Nous désignerons par G_i le groupe linéaire associé à la représentation ρ_i et par f_i l'application naturelle de G_i sur $\rho_i(G)$. Soit G' la composante neutre dans le groupe des $(s_1, \ldots, s_n, s) \in G_1 \times \ldots \times G_n \times G$ tels que l'on ait $\rho_i(s) = f_i(s_i)$ $(1 \leq i \leq n)$; les projections de $G_1 \times \ldots \times G_n \times G$ sur ses différents facteurs définissent des homomorphismes $h_1, \ldots, h_n, h$ de G' dans $G_1, \ldots, G_n, G$; on a $f_i \circ h_i = \rho_i \circ h$. Les noyaux des f_i étant finis, il en est de même de celui de h. Pour tout $s \in G$, il existe des $s_i \in G_i$ tels que $f_i(s_i) = \rho_i(s)$, d'où on déduit que $\dim G' \geq \dim G$; h est par suite une isogénie. Soit T' le tore maximal de G' tel que $h(T') = T$, et soit η l'isomorphisme de $X^{\mathbf{Q}}(T)$ sur $X^{\mathbf{Q}}(T')$ attaché à h. Posons $\eta(\alpha_i) = q_i\, \alpha'_i$, q_i étant une puissance de l'exposant caractéristique de K et α'_i une racine de G'. Soit τ'_i un isomorphisme de K sur un sous-groupe de G' associé à la racine α'_i ; si $\eta(\alpha_i) = q_i\, \alpha'_i$, on a $h(\tau'_i(\xi)) = \tau_i(\xi^{q_i})$ (pour $\xi \in K$), où τ_i est un isomorphisme de K sur un sous-groupe de G associé à la racine α_i ; nous voulons montrer que $q_i = 1$. Or $\rho_i \circ \tau_i$ est un homomorphisme de K sur un sous-groupe de $\rho_i(G)$ formé d'éléments unipotents. Il en résulte (n° 18.3, proposition 4) qu'il existe un homomorphisme $\widetilde{\tau}_i$ de K dans G_i tel que $f_i \circ \widetilde{\tau}_i = \rho_i \circ \tau_i$. On a donc, pour tout $\xi \in K$,

$$(f_i \circ \widetilde{\tau}_i)(\xi^{q_i}) = \rho_i(\tau_i(\xi^{q_i})) = (\rho_i \circ h)(\tau'_i(\xi)) = f_i((h_i \circ \tau'_i)(\xi)) \ ;$$

il en résulte immédiatement (le noyau de f_i étant composé d'éléments semi-simples) que $h_i(\tau'_i(\xi)) = \widetilde{\tau}_i(\xi^{q_i})$. Or on a

$$\tau'_i(\xi) = (h_1(\tau'_i(\xi)), \ldots, h_n(\tau'_i(\xi)),\ h(\tau'_i(\xi))) \ ;$$

[1] Exposés de C. Chevalley, les 20.1.1958 et 27.1.1958

il en résulte immédiatement que $q_i = 1$. Nous avons donc prouvé que les exposants radiciels de η sont tous égaux à 1 (ce qui montre incidemment que G' est du même type que G). Il en résulte que les $\varpi'_i = \eta(\varpi_i)$ sont les poids dominants fondamentaux de G' relatifs au système fondamental $(\alpha'_1, \ldots, \alpha'_n)$. Pour chaque i, $\rho_i \circ h$ est une représentation projective simple de poids dominant ϖ'_i de G'. Comme cette représentation s'écrit $f_i \circ h_i$, on voit que h_i est une représentation linéaire simple de poids dominant ϖ'_i de G', d'où $\varpi'_i \in X(T')$. Ceci étant vrai pour tout i, G' est simplement connexe.

Proposition 2. – *Soient G un groupe algébrique semi-simple simplement connexe et T un tore maximal de G. Pour toute racine α de G par rapport à T, soit Z_α le sous-groupe presque simple de dimension 3 de G associé à la racine α. Les groupes Z_α sont alors tous isomorphes à* $\mathrm{SL}(K^2)$.

Soit $(\alpha_1, \ldots, \alpha_n)$ un système fondamental de racines. Comme toute racine peut être transformée en l'une des α_i par une opération du groupe de Weyl, il suffit de faire la démonstration dans le cas où α est une racine fondamentale, soit $\alpha = \alpha_i$. Soit ϖ le poids dominant fondamental relatif à la racine α, et soit ρ une représentation linéaire simple de G de poids dominant ϖ (il en existe une puisque G est simplement connexe). La représentation ρ induit une représentation linéaire ρ^* de Z_α ; si T_α est le tore maximal de Z_α contenu dans T, la restriction ϖ^* de ϖ à T_α est un poids de ρ^*. Or, si w est la réflexion par rapport à α, on a $w(\varpi) = \varpi - \alpha$. Soit α^* la restriction de α à T_α, qui est l'une des racines de Z_α, et soit w^* la réflexion par rapport à cette racine, opérant dans $X(T_\alpha)$; on a $w^*(\varpi^*) = \varpi^* - \alpha^*$, mais aussi $w^*(\varpi^*) = -\varpi^*$; il en résulte que $\varpi^* = \frac{1}{2}\alpha^*$. Puisque $\frac{1}{2}\alpha^*$ appartient à $X(T_\alpha)$, Z_α est isomorphe à $\mathrm{SL}(K^2)$.

23.2 Isogénies attachées à un même isomorphisme spécial

Proposition 3. – *Soient G et G' des groupes algébriques semi-simples, T et T' des tores maximaux de G et G' respectivement, f et f_1 des isogénies de G sur G' telles que $f(T) = f_1(T) = T'$. Si les isomorphismes spéciaux de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(T)$ attachés à f et f_1 sont égaux*[2]*, on a $f_1 = f \circ g$, où g est un automorphisme intérieur de G produit par un élément de T.*

Faisant usage de la proposition 7 du n° 18.4, on voit qu'il existe une isogénie g de G sur lui-même qui applique T sur lui-même, et qui possède les propriétés suivantes : on a $f_1 = f \circ g$, et l'isomorphisme spécial de $X^{\mathbf{Q}}(T)$ sur lui-même attaché à g est l'automorphisme identique ; de plus, g est un automorphisme de G. Il est clair que g coïncide avec l'identité sur T. Il en résulte que g est un automorphisme intérieur produit par un élément de T (*cf.* la démonstration de la proposition 1 du n° 17.3).

[2] Cette hypothèse signifie évidemment que f et f_1 ont même restriction à T.

Proposition 4. – *Les notations étant celles de la proposition* 3*, soit de plus* $(\alpha_1, \ldots, \alpha_n)$ *un système fondamental de racines de* G *par rapport à* T *; pour chaque* i*, soient* Z_i *le sous-groupe presque simple de dimension* 3 *de* G *associé à* α_i*,* T_i *le tore maximal de* Z_i *contenu dans* T *et* s_i *un élément du normalisateur de* T_i *dans* Z_i *n'appartenant pas à* T_i*. Supposons que* G *et* G' *soient simplement connexes, que les isomorphismes spéciaux attachés à* f *et* f_1 *soient égaux*[3] *et que* $f(s_i) = f_1(s_i)$ *pour tout* i*. On a alors* $f = f_1$*.*

Comme $Z_1, \ldots, Z_n$ engendrent G (n° 13.3, proposition 5), il suffit de montrer que, pour tout i, les restrictions f_i et $f_{1,i}$ de f et f_1 à Z_i sont égales. D'après la proposition 3, on a $f_1 = f \circ g$, où g est un automorphisme intérieur de G produit par un élément de T, d'où $g(Z_i) = Z_i$ pour tout i ; on a donc $f_i(Z_i) = f_{1,i}(Z_i)$. Soit $T_i' = f_i(T_i) = f_{1,i}(T_i)$; comme f_i et $f_{1,i}$ coïncident sur T_i, les isomorphismes spéciaux de $X^{\mathbf{Q}}(T_i')$ sur $X^{\mathbf{Q}}(T_i)$ attachés à f_i et $f_{1,i}$ sont égaux ; il en résulte que $f_{1,i} = f_i \circ h_i$, où h_i est un automorphisme intérieur de Z_i produit par un élément t_i de T_i.

Par ailleurs, f_i est *bijective*. En effet, s'il n'en était pas ainsi, le centre de Z_i serait d'ordre 2, de sorte que la caractéristique de K serait $\neq 2$, et $Z_i' = f_i(Z_i)$ serait isomorphe à $\mathrm{PL}(K^2)$; mais Z_i' est le sous-groupe de dimension 3 de G' associé à une racine de G' par rapport à T' et est par suite isomorphe à $\mathrm{SL}(K^2)$ (proposition 2) puisque G' est simplement connexe.

L'égalité $f_i(s_i) = f_{1,i}(s_i)$ entraîne donc $h_i(s_i) = s_i$. Il nous suffira de montrer que ceci entraîne que h_i est l'identité. Or on a $s_i^{-1}\, t_i\, s_i = t_i^{-1}$, d'où $s_i = h_i(s_i) = t_i\, s_i\, t_i^{-1} = s_i\, t_i^{-2}$ et par suite $t_i^{-2} = e$ (l'élément neutre). Or, T_i est isomorphe au groupe multiplicatif K^* des éléments $\neq 0$ de K. Si K est de caractéristique 2, la relation $t_i^2 = e$ entraîne $t_i = e$. Sinon, T_i n'a qu'un seul élément d'ordre 2, et cet élément appartient au centre de Z_i, car Z_i, étant isomorphe à $\mathrm{SL}(K^2)$, a un centre d'ordre 2. Donc, dans tous les cas, t_i appartient au centre de Z_i, ce qui montre que h_i est l'identité.

Proposition 5. – *Soient* G *un groupe algébrique semi-simple,* T *un tore maximal de* G*,* $(\alpha_1, \ldots, \alpha_n)$ *un système fondamental de racines de* G *par rapport à* T*. Pour chaque* i*, soit* Z_i *le sous-groupe presque simple de dimension* 3 *de* G *associé à* α_i*,* T_i *le tore maximal de* Z_i *contenu dans* T *et* s_i*,* s_i' *des éléments du normalisateur de* T_i *dans* Z_i *n'appartenant pas à* T_i*. Il existe alors un élément* t *de* T *tel que* $t\, s_i\, t^{-1} = s_i'$ *(*$1 \leq i \leq n$*).*

On a $s_i' = t_i\, s_i$, où t_i est un élément de T_i. Observons maintenant que, pour tout $t \in T$, on a $t\, Z_i\, t^{-1} = Z_i$, $t\, T_i\, t^{-1} = T_i$; il en résulte que $t\, s_i\, t^{-1}\, s_i^{-1} \in T_i$. Soit f l'application

$$t \to (t\, s_1\, t^{-1}\, s_1^{-1}, \ldots, t\, s_n\, t^{-1}\, s_n^{-1})$$

de T dans $T_1 \times \ldots \times T_n$. Comme T est commutatif, f est un homomorphisme. Montrons qu'il est de noyau fini. Soit t un élément de ce noyau. L'opération

[3] Voir la note précédente. Noter le corollaire suivant de la proposition 4 : si f et f_1 coïncident sur le normalisateur $N(T)$ de T dans G, on a $f = f_1$.

du groupe de Weyl qui correspond à s_i est la réflexion par rapport à α_i ; on a donc $\alpha_i(s_i\, t'\, s_i^{-1}) = (\alpha_i(t'))^{-1}$ pour tout $t' \in T$, d'où $\alpha_i(t) = \pm 1$ $(1 \leq i \leq n)$, d'où notre assertion résulte immédiatement. On en conclut que

$$\dim f(T) = \dim T = n = \dim (T_1 \times \ldots \times T_n)\,;$$

comme les groupes algébriques T et $T_1 \times \cdots \times T_n$ sont connexes, on a donc $f(T) = T_1 \times \ldots \times T_n$, ce qui démontre la proposition 5.

23.3 Enoncé du théorème. Notations

Nous nous proposons de démontrer le théorème suivant :

Théorème 1. – *Soient G et G' des groupes algébriques semi-simples, T et T' des tores maximaux de G et G' respectivement et φ un isomorphisme spécial de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(T)$. Il existe alors une isogénie f de G sur G' appliquant T sur T' et telle que φ soit l'isomorphisme spécial attaché à f.*

Nous utiliserons les notations suivantes. Pour chaque racine α de G par rapport à T, nous désignerons par τ_α un isomorphisme de K sur un sous-groupe de G associé à α et par Z_α le sous-groupe presque simple de dimension 3 de G associé à α ; si α' est la racine de G' telle que $\varphi(\alpha') = q(\alpha)\,\alpha$, $q(\alpha)$ étant une puissance de l'exposant caractéristique de K, nous désignerons par τ'_α un isomorphisme de K sur un sous-groupe de G' associé à α' et par Z'_α le sous-groupe presque simple de dimension 3 de G' associé à α'. Si α et β sont des racines de G, nous désignerons par $Z_{\alpha\beta}$ le sous-groupe radiciel de G défini par l'ensemble des racines qui sont combinaisons linéaires à coefficients rationnels de α et β et par $Z'_{\alpha\beta}$ le sous-groupe radiciel de G' défini par l'ensemble des racines qui sont combinaisons linéaires à coefficients rationnels de α', β' ; $Z_{\alpha\beta}$ et $Z'_{\alpha\beta}$ sont donc des groupes semi-simples de rang 1 ou 2. Nous désignerons par T_α (resp. T'_α, $T_{\alpha\beta}$, $T'_{\alpha\beta}$) le tore maximal de Z_α (resp. Z'_α, $Z_{\alpha\beta}$, $Z'_{\alpha\beta}$) contenu dans T (resp. T', T, T'). Nous désignerons par $N(T)$ et $N(T')$ les normalisateurs de T et T' ; pour toute racine α, nous désignerons par s_α (resp. s'_α) un élément de $N(T) \cap Z_\alpha$ (resp. $N(T') \cap Z'_\alpha$) non contenu dans T (resp. T'). Nous désignerons par $(\alpha_1, \ldots, \alpha_n)$ un système fondamental de racines de G ; pour chaque i, nous désignerons par α'_i la racine de G' telle que $\varphi(\alpha'_i) = q_i\,\alpha_i$, q_i étant une puissance de l'exposant caractéristique de K ; $\alpha'_1, \ldots, \alpha'_n$ forment donc un système fondamental de racines de G'. Si $\alpha = \alpha_i$, nous écrirons τ_i, Z_i, T_i, s_i, τ'_i, Z'_i, T'_i, s'_i au lieu de τ_α, Z_α, T_α, s_α, τ'_α, Z'_α, T'_α, s'_α. Si $\alpha = \alpha_i$, $\beta = \alpha_j$, nous écrirons T_{ij}, Z_{ij}, T'_{ij}, Z'_{ij} au lieu de $T_{\alpha\beta}$, $Z_{\alpha\beta}$, $T'_{\alpha\beta}$, $Z'_{\alpha\beta}$.

23.4 Premières constructions

Comme on a $\varphi(X(T')) \subset X(T)$, il existe un homomorphisme f_T de T sur T' tel que $\chi'(f_T(t)) = (\varphi(\chi'))(t)$ pour tout $t \in T$ et tout caractère rationnel χ'

de T' ; si φ est attaché à une isogénie f de G sur G', f prolonge f_T. Si α, β sont des racines, f_T applique $T_{\alpha\beta}$ sur $T'_{\alpha\beta}$.

Proposition 6. – *Si φ est attaché à une isogénie f de G sur G', φ est aussi attaché à une isogénie f_1 de G sur G' telle que l'on ait $f_1(s_i) = s'_i$ $(1 \leq i \leq n)$.*

On a évidemment $f(Z_\alpha) = Z'_\alpha$, $f(N(T)) \subset N(T')$; $f(s_\alpha)$ est donc un élément de $Z'_\alpha \cap N(T')$. Comme on a $s_\alpha\, t\, s_\alpha^{-1} = t^{-1}$ pour tout $t \in T_\alpha$, on a $f(s_\alpha)\, t'\, f(s_\alpha^{-1}) = t'^{-1}$ pour tout $t' \in T'_\alpha$. Il résulte de là qu'on a

$$f(s_i) = t'_i\, s'_i \qquad (1 \leq i \leq n)$$

avec des $t'_i \in T'_i$. Il existe un automorphisme intérieur h' de G', produit par un élément de T', qui transforme $f(s_i)$ en s'_i $(1 \leq i \leq n)$ (proposition 5) ; posons $f_1 = h' \circ f$. L'application f_1 est encore une isogénie de G sur G' ; comme h' laisse fixes les éléments de T', on a $f_1(T) = T'$ et l'isomorphisme spécial de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(T)$ attaché à f_1 est encore φ, ce qui démontre la proposition 6.

Soient α et β des racines de G par rapport à T ; la restriction de f_T à $T_{\alpha\beta}$ est une isogénie de ce groupe sur $T'_{\alpha\beta}$; elle définit un isomorphisme $\varphi_{\alpha\beta}$ de $X^{\mathbf{Q}}(T'_{\alpha\beta})$ sur $X^{\mathbf{Q}}(T_{\alpha\beta})$ qui applique $X(T'_{\alpha\beta})$ sur un sous-groupe de $X(T_{\alpha\beta})$. Considérant $T_{\alpha\beta}$ et $T'_{\alpha\beta}$ comme des tores maximaux des groupes $Z_{\alpha\beta}$ et $Z'_{\alpha\beta}$, montrons que $\varphi_{\alpha\beta}$ *est spécial*. Les racines de $Z'_{\alpha\beta}$ sont les restrictions à $T'_{\alpha\beta}$ de celles des racines de G' qui sont combinaisons linéaires rationnelles de α' et β'. Si γ' est l'une de ces racines, on a $\varphi(\gamma') = q(\gamma)\gamma$, où γ est une racine de G qui est combinaison linéaire rationnelle de α et β, et on obtient de cette manière toutes les racines de G qui sont combinaisons linéaires rationnelles de α et β ; de plus, il est clair que $\varphi_{\alpha\beta}$ applique la restriction de γ' à $T'_{\alpha\beta}$ sur le produit par $q(\gamma)$ de la restriction de γ à $T_{\alpha\beta}$; ceci établit bien que $\varphi_{\alpha\beta}$ est spécial. Or $Z_{\alpha\beta}$ est de rang 1 ou 2 ; s'il est de rang 1, il est de type A_1 ; s'il est de rang 2, il est de l'un des types A_2, C_2, G_2 ou $A_1 + A_1$. Faisant usage des théorèmes 1 du n° 20.3, 2 du n° 22.4, 2 du n° 21.5 et 3 du n° 22.5, on obtient le résultat suivant :

Proposition 7. – *La restriction de f_T à $T_{\alpha\beta}$ peut se prolonger en une isogénie $f_{\alpha\beta}$ de $Z_{\alpha\beta}$ sur $Z'_{\alpha\beta}$.*

Démontrons maintenant la

Proposition 8. – *L'application f_T peut se prolonger en un épimorphisme de $N(T)$ sur $N(T')$ qui applique s_i sur s'_i $(1 \leq i \leq n)$.*

Désignons par W le groupe de Weyl de G et par w_i la réflexion par rapport à α_i. Introduisons un groupe libre W^* à n générateurs w_i^* $(1 \leq i \leq n)$; il existe un homomorphisme a^* de W^* dans le groupe des automorphismes de T qui associe à tout w_i^* l'automorphisme $t \to s_i\, t\, s_i^{-1}$ de T ; formons le produit semi-direct $N^*(T)$ de T et W^* relativement aux opérateurs $a^*(w^*)$; nous

considérerons T comme un sous-groupe invariant de ce groupe. Il est clair qu'il existe un homomorphisme u^* de $N^*(T)$ dans $N(T)$ qui coïncide avec l'identité sur T et qui applique w_i^* sur s_i $(1 \leq i \leq n)$.

Déterminons le noyau U^* de u^*. Si i et j sont des indices entre 1 et n, soit $m(i,j)$ l'ordre de l'élément $w_i\, w_j$ de W ; posons $(s_i\, s_j)^{m(i,j)} = t_{ij} \in T$. Il est clair que U^* contient le plus petit sous-groupe invariant U_0^* de $N^*(T)$ qui contienne les éléments

$$z_{ij}^* = t_{ij}^{-1}(w_i^*\, w_j^*)^{m(i,j)}\ .$$

Nous allons montrer que l'on a $U_0^* = U^*$. L'homomorphisme u^* définit par passage aux quotients un homomorphisme u_1^* de $N^*(T)/U_0^*$ dans $N(T)$ dont il suffira de montrer que c'est un monomorphisme. Il est clair que u_0^* induit un isomorphisme de TU_0^*/U_0^* sur T ; il suffira donc de montrer que l'homomorphisme u_1^* de $N^*(T)/TU_0^*$ dans $N(T)/T$ déduit de u_0^* par passage aux quotients est un monomorphisme. Or $N^*(T)/T$ est canoniquement isomorphe à W^* et le groupe qui correspond à TU_0^*/T dans cet isomorphisme est le plus petit sous-groupe invariant de W^* contenant les $(w_i^*\, w_j^*)^{m(i,j)}$. On sait que ce groupe n'est autre que le noyau de l'homomorphisme de W^* sur W qui applique w_i^* sur w_i $(1 \leq i \leq n)$ (n° 14.5, théorème 1). On en conclut que l'ordre de $N^*(T)/TU_0^*$ est égal à celui de W, donc à celui de $N(T)/T$. Par ailleurs, $u_1^*(N^*(T)/TU_0^*)$ contient les classes des s_i modulo T et est par suite $N(T)/T$ tout entier, ce qui montre bien que u_1^* est un monomorphisme, et même que u_0^* est un isomorphisme de $N^*(T)/U_0^*$ sur $N(T)$.

Ceci étant, montrons que f_T se prolonge en un homomorphisme f^* de $N^*(T)$ dans $N(T')$ qui applique w_i^* sur s_i' $(1 \leq i \leq n)$. Il suffit pour cela de montrer que l'on a $s_i'\, f_T(t)\, {s'}_i^{-1} = f_T(s_i\, t s_i^{-1})$ si $t \in T$. Or, désignons par χ' un caractère rationnel quelconque de T' et par w_i' la réflexion par rapport à α_i' ; on a

$$\chi'(s_i'\, f_T(t)\, {s'}_i^{-1}) = (w_i'(\chi'))(f_T(t)) = (\varphi(w_i'(\chi')))(t)\ \ ;$$

mais on sait que l'on a $\varphi \circ w_i' = w_i \circ \varphi$ (n° 18.3, proposition 5) ; la formule à démontrer résulte immédiatement de là.

Montrons maintenant que U^* est contenu dans le noyau de f^*. Il suffit de montrer que, si i et j sont des indices entre 1 et n, z_{ij}^* appartient au noyau de f^*. Or la restriction de f_T à T_{ij} peut se prolonger en une isogénie f_{ij} de Z_{ij} sur Z_{ij}' (proposition 7), et l'on peut même supposer en vertu de la proposition 6 que $f_{ij}(s_i) = s_i'$, $f_{ij}(s_j) = s_j'$. Il en résulte que l'on a

$$f_T(t_{ij}) = (s_i'\, s_j')^{m(i,j)}\ ,$$

d'où il résulte immédiatement que l'on a $f^*(z_{ij}^*) = 1$. Il résulte de là que f^* définit par passage aux quotients un homomorphisme $f_{N(T)}$ de $N(T)$ dans $N(T')$ qui prolonge f_T et applique s_i sur s_i' $(1 \leq i \leq n)$. Cet homomorphisme est un épimorphisme car $N(T')$ est engendré par T' et par les s_i'. Ceci démontre la proposition 8.

Nous désignerons dans ce qui suit par $f_{N(T)}$ l'homomorphisme (évidemment unique) de $N(T)$ sur $N(T')$ qui prolonge f_T et applique s_i sur s'_i ($1 \leq i \leq n$). Soient s un élément quelconque de $N(T)$ et w l'opération correspondante du groupe de Weyl de G ; posons $f_{N(T)}(s) = s'$ et soit w' l'opération du groupe de Weyl de G' définie par s' ; w et w' sont alors liées par la relation $\varphi \circ w' = w \circ \varphi$. Soit en effet χ' un caractère rationnel de T'. On a, pour $t \in T$, $\chi'(f_{N(T)}(s^{-1}\,ts)) = (\varphi(\chi'))(s^{-1}\,ts) = ((w \circ \varphi)(\chi'))(t)$; mais le premier membre est aussi égal à $\chi'(s'^{-1}\,f_T(t)s')$, donc à

$$(w'(\chi'))(f_T(t)) = ((\varphi \circ w')(\chi'))(t)\,,$$

ce qui démontre notre assertion.

Montrons que l'on a $f(s_\alpha) \in Z'_\alpha$ pour toute racine α de G par rapport à T. Il existe une racine fondamentale α_i et une opération w du groupe de Weyl W de G telles que $\alpha = w \cdot \alpha_i$ (n° 13.3, proposition 5) ; soit s un élément de $N(T)$ qui produise l'opération w. Il est clair que l'on a alors $sZ_i\,s^{-1} = Z_\alpha$, de sorte que l'on peut écrire $s_\alpha = s\,\overline{s}_i\,s^{-1}$, où $\overline{s}_i$ est un élément de Z_i qui ne diffère de s_i que par un élément de T_i. Il en résulte que l'on a $f_{N(T)}(s_\alpha) = s'\,f_{N(T)}(\overline{s}_i)\,s'^{-1}$, en posant $s' = f_{N(T)}(s)$. Si w' est l'opération du groupe de Weyl W' de G' qui correspond à s', il résulte de la relation $f_{N(T)}(\overline{s}_i) \in T'_i\,s'_i \subset Z'_i$ que $f_{N(T)}(s_\alpha)$ appartient au groupe $Z'_{\beta'}$ avec $\beta' = w'(\alpha'_i)$. Or on a

$$\varphi(\beta') = w(\varphi(\alpha'_i)) = q(\alpha_i)\,w(\alpha_i) = q(\alpha_i)\,\alpha\,,$$

ce qui montre bien que β' n'est autre que la racine α' de G' qui correspond à α, d'où finalement $f_{N(T)}(s_\alpha) \in Z'_\alpha$. *Nous pouvons donc supposer les s'_α choisis de telle manière que l'on ait*

$$f_{N(T)}(s_\alpha) = s'_\alpha$$

pour tout α ; c'est ce que nous ferons désormais.

23.5 Présentation d'un groupe semi-simple

Proposition 9. – *Soient G^* un groupe abstrait et h un homomorphisme de G^* dans G ; supposons les conditions suivantes satisfaites :*

1) *G^* contient un sous-groupe $N^*(T)$ tel que h induise une bijection de ce groupe sur $N(T)$; si α est une racine de G, on désigne par s^*_α l'élément de $N^*(T)$ tel que $h(s^*_\alpha) = s_\alpha$; on désigne par T^*_α le sous-groupe de $N^*(T)$ tel que $h(T^*_\alpha) = T_\alpha$; si α, β sont des racines, on désigne par $T^*_{\alpha\beta}$ le sous-groupe de $N^*(T)$ tel que $h(T^*_{\alpha\beta}) = T_{\alpha\beta}$;*

2) *pour chaque racine α, G^* contient un sous-groupe Z^*_α tel que h induise une bijection de Z^*_α sur Z_α et que $T^*_\alpha \subset Z^*_\alpha$, $s^*_\alpha \in Z^*_\alpha$;*

3) *si α et β sont des racines de G, G^* contient un sous-groupe $Z^*_{\alpha\beta}$ tel que h induise une bijection de $Z^*_{\alpha\beta}$ sur $Z_{\alpha\beta}$ et que l'on ait $Z^*_\gamma \subset Z^*_{\alpha\beta}$ pour toute combinaison linéaire rationnelle γ de α et β qui est une racine ;*

4) *G^* est engendré par les Z^*_α pour toutes les racines α.*

L'homomorphisme h est alors un isomorphisme.

Nous choisirons un groupe de Borel B de G contenant T. Rappelons que, si $\Gamma(T)$ est le groupe des groupes à un paramètre de T, l'espace vectoriel $\Gamma^{\mathbf{Q}}(T) = \mathbf{Q} \otimes \Gamma(T)$ est en dualité avec $X^{\mathbf{Q}}(T) = \mathbf{Q} \otimes X(T)$. Nous choisirons un élément λ de la chambre de Weyl $\mathcal{C}$ qui correspond à B tel que les valeurs prises en λ par deux racines distinctes soient toujours distinctes. Nous désignerons par $\delta_1, \ldots, \delta_N$ les racines qui sont négatives sur $\mathcal{C}$ arrangées dans un ordre tel que l'on ait

$$\langle \lambda, \delta_1 \rangle < \langle \lambda, \delta_2 \rangle < \cdots < \langle \lambda, \delta_N \rangle ;$$

les $\langle \lambda, \delta_i \rangle$ étant < 0, on voit que, si δ_k est combinaison linéaire à coefficients entiers > 0 de δ_i et δ_j, on a $k < \min(i, j)$. Soit B^u le groupe des éléments unipotents de B ; si $1 \leq i \leq N$, $B^u \cap Z_{\delta_i}$ est un groupe P_i isomorphe à K ; nous désignerons par P^*_i le sous-groupe de $Z^*_{\delta_i}$ tel que $h(P^*_i) = P_i$. Si $1 \leq k \leq N$, nous désignerons par B^u_k l'ensemble $P_1 \ldots P_k$ (*i.e.* l'ensemble des $u_1 \ldots u_k$, $u_i \in P_i$) et par B^{*u}_k l'ensemble $P^*_1 \ldots P^*_k$. Il résulte du corollaire au lemme 1 du n° 17.2, que les B^u_k sont des sous-groupes de B. Montrons que ce sont des sous-groupes invariants de B. Comme chaque P_i est transformé en lui-même par les automorphismes intérieurs produits par les éléments de T, il suffira de montrer que, si $u \in P_i$, i étant un indice quelconque entre 1 et N, on a

$$u B^u_k \, u^{-1} = B^u_k \ ;$$

or il résulte encore du corollaire au lemme 1 du n° 17.2 que $B^u_k \, P_i$ est un sous-groupe de B^u, puis du lemme 1, b) du n° 13.1, que B^u_k est un sous-groupe invariant de $B^u_k \, P_i$. Montrons maintenant que B^{*u}_k est un sous-groupe invariant du groupe B^{*u} engendré par les P^*_i. Nous procédons par récurrence sur k ; désignant par B^{*u}_0 le groupe réduit à son élément neutre, supposons que l'on ait $k > 0$ et que notre assertion soit vraie pour $k - 1$. Il résulte immédiatement de l'hypothèse inductive que $B^{*u}_k = B^{*u}_{k-1} \, P^*_k$ est un groupe ; pour montrer qu'il est invariant, il suffira de montrer que, si $i > k$, $u^* \in P^*_i$, on a

$$u^* \, P^*_k \, u^{*-1} \subset B^{*u}_k \, .$$

Nous utiliserons pour cela le groupe $Z^*_{\delta_i \, \delta_k}$. Posons $u = h(u^*)$; soit v^* un élément de P^*_k et soit $v = h(v^*)$. L'élément uvu^{-1} de $Z_{\delta_i \delta_k}$ est dans le groupe engendré par les P_j pour les $j \leq k$ tels que δ_j soit combinaison linéaire à coefficients entiers ≥ 0 de δ_i et δ_k, le coefficient de δ_k étant $\neq 0$ (théorème 1

du n° 17.2). Les groupes P_j^* correspondants sont dans $Z^*_{\delta_i\,\delta_k}$; comme h induit un isomorphisme de $Z^*_{\delta_i\,\delta_k}$ sur $Z_{\delta_i\,\delta_k}$, $u^*\,v^*\,u^{*-1}$ est dans le groupe engendré par les P_j^* pour les j possédant les propriétés indiquées, donc est dans B_k^{*u}, ce qui montre que B_k^{*u} est distingué. On conclut de là que $B^{*u} = B_N^{*u}$. D'après le théorème 1, d) du n° 13.2, un élément de B^u ne se met que d'une seule manière sous la forme $u_1 \dots u_N$, avec $u_i \in P_i$ $(1 \leq i \leq N)$, on voit que h *induit un isomorphisme de* B^{*u} *sur* B^u.

Nous désignerons par T^* le sous-groupe de $N^*(T)$ tel que $h(T^*) = T$. Ce groupe est engendré par les T_α^* pour toutes les racines α de la forme δ_i. Si $\alpha = \delta_i$ et si β est une racine quelconque, l'existence de l'isomorphisme induit par h de $Z^*_{\alpha\beta}$ sur $Z_{\alpha\beta}$ montre que le normalisateur de P_i^* contient T_β^* ; ceci étant vrai pour toute racine β, on voit que le normalisateur de P_i^* contient T^*. Ceci étant vrai pour tout i, le normalisateur de B^{*u} contient T^*. On en conclut que $B^* = B^{*u}\,T^*$ est un sous-groupe de G^* ; comme B est produit semi-direct de B^u et T, h *induit un isomorphisme de* B^* *sur* B.

Pour chaque opération w du groupe de Weyl W de G, nous choisirons un élément $s(w)$ de $N(T)$ dont la classe modulo T soit w (en identifiant W à $N(T)/T$) ; nous désignerons par $s^*(w)$ l'élément de $N^*(T)$ tel que $h(s^*(w)) = s(w)$; on peut supposer que $s(w) = s_\alpha$, $s^*(w) = s_\alpha^*$ si w est la réflexion w_α par rapport à une racine α. Nous supposerons de plus que B est le groupe de Borel qui correspond au système fondamental $(\alpha_1, \dots, \alpha_n)$. Pour toute racine α, nous désignerons par P_α le sous-groupe unipotent de G associé à la racine α ; on a donc $P_\alpha = P_i$ si $\alpha = \delta_i$, $P_\alpha \subset Z_\alpha = Z_{-\alpha}$; nous désignerons par P_α^* le sous-groupe de Z_α^* tel que $h(P_\alpha^*) = P_\alpha$. Montrons que l'on a $s^*(w)\,P_\alpha^*\,(s^*(w))^{-1} = P^*_{w(\alpha)}$. Il suffit évidemment de le montrer quand w est la réflexion par rapport à une racine β (car, pour toute racine α, le normalisateur de P_α^* contient T^*). Or, dans ce cas, $s^*(w)$ et P_α^* sont dans $Z^*_{\alpha\beta}$ et l'assertion résulte de ce que h induit un isomorphisme de $Z^*_{\alpha\beta}$ sur $Z_{\alpha\beta}$.

Si $w \in W$, nous désignerons par B_w^u (resp. B'^u_w) le groupe engendré par les P_i pour lesquels $w^{-1}(\delta_i)$ est la forme $-\delta_j$ (resp. δ_j) ; on sait que l'on a $B^u = B_w^u\,B'^u_w$ (n° 13.2, proposition 4). Nous désignerons par B_w^{*u} et B'^{*u}_w les sous-groupes de B^{*u} qui sont appliqués respectivement sur B_w^u et B'^u_w par h ; on a donc $B^{*u} = B_w^{*u}\,B'^{*u}_w$. Si $w^{-1}(\delta_i) = \delta_j$, on a $P_i^*\,s^*(w) = s^*(w)\,P_j^*$ d'après l'alinéa précédent ; il en résulte que l'on a

$$B^*\,s^*(w)\,B^* = B_w^{*u}\,s^*(w)\,B^*\,.$$

Si w est la réflexion $w(\alpha)$ associée à une racine fondamentale α, le groupe B'^{*u}_w est engendré par les P_i^* pour tous les i tels que $\delta_i \neq \alpha$ (n° 13.3, proposition 6) ; nous le désignerons par C_α^*. De plus, $w(\alpha)$ permute entre elles les racines δ_i qui sont $\neq \alpha$; il en résulte que s_α^* appartient au normalisateur de C_α^*. Soit $i(\alpha)$ l'indice tel que $\alpha = \delta_{i(\alpha)}$; le groupe $h(C_\alpha^*)$ est un sous-groupe distingué de B (*loc. cit.*), d'où il résulte que C_α^* est un sous-groupe distingué de B^*. Le normalisateur de C_α^* contient donc $P^*_{i(\alpha)}$ et T_α^* ; contenant aussi s_α^*, il

contient les groupes $P^*_{i(\alpha)}$, T^*_α et le transformé de $P^*_{i(\alpha)}$ par s^*_α, groupes qui engendrent le groupe Z^*_α (en vertu du fait que h induit un isomorphisme de Z^*_α sur Z_α). En conclusion, *le normalisateur de C^*_α contient Z^*_α.*

Désignons par G^*_0 la réunion des ensembles $B^*\, s^*(w)\, B^* = B^{*u}_w\, s^*(w)\, B^*$ pour tous les $w \in W$. Nous allons montrer que l'on a $Z^*_\alpha\, G^*_0 \subset G^*_0$ pour toute racine fondamentale α. Il suffit de montrer que l'on a $Z^*_\alpha\, B^*\, s^*(w)\, B^* \subset G^*_0$. Comme $B^* = C^*_\alpha\, P^*_{i(\alpha)}\, T^*$, et comme Z^*_α est contenu dans le normalisateur de C^*_α et contient $P^*_{i(\alpha)}$, il suffit de montrer que l'on a $Z^*_\alpha\, T^*\, s^*(w)\, B^* \subset G^*_0$, ou encore que $Z^*_\alpha\, s^*(w) \subset G^*_0$ puisque le normalisateur de Z^*_α contient T^*. On a $Z^*_\alpha = Z^*_\alpha\, s^*_\alpha$ et $s^*_\alpha\, s^*(w) = \theta^*\, s^*(w(\alpha)w)$, où θ^* est un élément de T^*_α ; on en conclut que l'on peut se ramener au cas où $w^{-1}(\alpha)$ est l'une des δ_i, c'est-à-dire où $P^*_{i(\alpha)}\, s^*(w) \subset s^*(w)\, B^*$; supposons donc qu'il en soit ainsi. Le groupe Z_α est la réunion des ensembles $P_{i(\alpha)}\, T_\alpha$ et $P_{i(\alpha)}\, s_\alpha\, T_\alpha\, P_{i(\alpha)}$ (corollaire 1 au théorème 3 du n° 13.4) ; Z^*_α est donc la réunion de $P^*_{i(\alpha)}\, T^*_\alpha$ et de $P^*_{i(\alpha)}\, s^*_\alpha\, T^*_\alpha\, P^*_{i(\alpha)}$. Comme $P^*_{i(\alpha)}\, s^*(w) \subset s^*(w)\, B^*$, $T^*\, s^*(w) = s^*(w)\, T^*$, il en résulte bien que $Z^*_\alpha\, s^*(w) \subset G^*_0$.

L'ensemble G^*_0 contient donc les Z^*_α pour toutes les racines fondamentales α ; de plus, si w est une opération quelconque du groupe de Weyl, on a

$$(s^*(w)\, Z^*_\alpha(s^*(w))^{-1})\, G^*_0 \subset G^*_0\,.$$

Mais on a

$$s^*(w)\, Z^*_\alpha(s^*(w))^{-1} = Z^*_{w(\alpha)}\,.$$

Comme toute racine peut être transformée en une racine fondamentale par une opération du groupe de Weyl, on voit que $Z^*_\alpha\, G^*_0 \subset G^*_0$ pour toute racine α. Comme G^* est engendré par les Z^*_α, on a $G^*_0 = G^*$.

Par ailleurs, on sait que les ensembles $h(B^{*u}_w\, s^*(w)\, B^*) = B^u_w\, s(w)\, B$ sont mutuellement disjoints et qu'un élément de $B^u_w\, s(w)\, B$ ne se met que d'une seule manière sous la forme $bs(w)b'$, avec $b \in B^u_w$, $b' \in B$ (n° 13.4, corollaire 1 au théorème 3). Il en résulte immédiatement que h est une bijection de $G^* = G^*_0$ sur G, ce qui démontre la proposition 9.

Corollaire. – *Soit f une application de G dans un groupe (abstrait) H. Supposons les conditions suivantes satisfaites : f induit un homomorphisme de $N(T)$ dans H ; pour tout couple (α, β) de racines de G, f induit un homomorphisme de $Z_{\alpha\beta}$ dans H. Alors f est un homomorphisme de G dans H.*

Pour tout $s \in G$, soit $f^*(s)$ l'élément $(s, f(s))$ de $G \times H$; soit G^* le sous-groupe de $G \times H$ engendré par les ensembles $f^*(Z_\alpha) = Z^*_\alpha$ pour toutes les racines α ; la projection de $G \times H$ sur G induit un homomorphisme h de G^* dans G. Pour montrer que f est un homomorphisme, il suffit évidemment de montrer que h est un isomorphisme de G^* sur G. Or cela résulte immédiatement de la proposition 9.

23.6 Fin de la démonstration du théorème 1

Nous allons d'abord montrer qu'il suffit de démontrer le théorème 1 *dans le cas où* G *et* G' *sont simplement connexes.* D'après la proposition 1, il existe en effet des groupes simplement connexes $\overline{G}$ et $\overline{G}'$ et des isogénies g de $\overline{G}$ sur G et g' de $\overline{G}'$ sur G' qui possèdent les propriétés suivantes : si $\overline{T}$, $\overline{T}'$ sont les tores maximaux de $\overline{G}$, $\overline{G}'$ tels que $g(\overline{T}) = T$, $g'(\overline{T}') = T'$, les exposants radiciels des isomorphismes spéciaux γ de $X^{\mathbf{Q}}(T)$ sur $X^{\mathbf{Q}}(\overline{T})$ et γ' de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(\overline{T}')$ attachés à g et g' sont tous égaux à 1. Il existe alors un isomorphisme $\overline{\varphi}$ de $X^{\mathbf{Q}}(\overline{T}')$ sur $X^{\mathbf{Q}}(\overline{T})$ tel que $\overline{\varphi} \circ \gamma' = \gamma \circ \varphi$. Montrons qu'il est spécial. Toute racine $\overline{\alpha}'$ de $\overline{G}'$ est l'image par γ' d'une racine α' de G' ; on a $\varphi(\alpha') = q\alpha$, où q est une puissance de l'exposant caractéristique de K et α une racine de G ; $\gamma(\alpha)$ est une racine de $\overline{G}$, et on a $\overline{\varphi}(\overline{\alpha}') = q\gamma(\alpha)$; réciproquement, on voit de la même manière que toute racine de $\overline{G}$ est le produit par une puissance de l'exposant caractéristique de K de l'image par $\overline{\varphi}$ d'une racine de $\overline{G}'$. Il reste à montrer que $\overline{\varphi}$ applique $X(\overline{T}')$ dans $X(\overline{T})$. Opérant comme ci-dessus pour les racines, on voit que, si on associe à toute opération $\overline{w}'$ du groupe de Weyl de $\overline{G}'$ l'automorphisme $\overline{w}$ de $X^{\mathbf{Q}}(\overline{T})$ défini par la condition $\overline{w} \circ \overline{\varphi} = \overline{\varphi} \circ \overline{w}'$, on obtient un isomorphisme du groupe de Weyl de $\overline{G}'$ sur celui de $\overline{G}$. Puisque $\overline{G}'$ est simplement connexe, $X(\overline{T}')$ est le groupe des poids. Si ϖ' est un poids de $\overline{G}'$, et $\overline{w}'$ une opération du groupe de Weyl, $\overline{w}'(\varpi') - \varpi'$ appartient au groupe $\overline{R}'$ des racines de $\overline{G}'$, dont l'image par $\overline{\varphi}$ est contenue dans le groupe $\overline{R}$ des racines de $\overline{G}$. Il s'ensuit que, pour toute opération $\overline{w}$ du groupe de Weyl de $\overline{G}$, $\overline{w}(\overline{\varphi}(\varpi')) - \overline{\varphi}(\varpi')$ appartient à $\overline{R}$; on en conclut que $\overline{\varphi}(\varpi')$ appartient au groupe des poids de $\overline{G}$, donc à $X(\overline{T})$ puisque $\overline{G}$ est simplement connexe. L'isomorphisme $\overline{\varphi}$ est donc bien spécial. Supposons que $\overline{\varphi}$ soit attaché à une isogénie $\overline{f}$ de $\overline{G}$ sur $\overline{G}'$. Alors $g' \circ \overline{f}$ est une isogénie de $\overline{G}$ sur G' à laquelle est attaché l'isomorphisme spécial $\overline{\varphi} \circ \gamma' = \gamma \circ \varphi$. Appliquant la proposition 6 du n° 18.4, on en conclut que φ est attaché à une isogénie de G sur G'.

Supposons donc G *et* G' *simplement connexes.* Pour toute racine α de G, la restriction de f_T à T_α se prolonge[4] en une isogénie f_α de Z_α sur Z'_α telle que $f_\alpha(s_\alpha) = s'_\alpha$. Soient maintenant α et β des racines de G ; soit A l'ensemble des racines qui sont combinaisons linéaires rationnelles de α et β ; supposons α et β linéairement indépendantes. Il existe deux racines γ, δ de A dont les restrictions à $T_{\alpha\beta}$ forment un système fondamental de racines de $Z_{\alpha\beta}$. La restriction de f_T à $T_{\alpha\beta}$ peut se prolonger en une isogénie $f_{\alpha\beta}$ de $Z_{\alpha\beta}$ sur $Z'_{\alpha\beta}$ qui applique s_γ sur s'_γ et s_δ sur s'_δ (proposition 8). On va montrer que $f_{\alpha\beta}$ prolonge f_α et f_β. Désignons par $N(T_{\alpha\beta})$ le normalisateur de $T_{\alpha\beta}$ dans $Z_{\alpha\beta}$; il est engendré par $T_{\alpha\beta}$ et par s_γ, s_δ. L'application $f_{\alpha\beta}$ coïncide avec $f_{N(T)}$ sur l'ensemble $T_{\alpha\beta} \cup \{s_\gamma, s_\delta\}$; elle coïncide donc avec $f_{N(T)}$ sur

[4] Cela résulte des constructions du n° 23.4 et en particulier des propositions 7 et 8 et de la dernière assertion du n° 23.4.

$N(T_{\alpha\beta})$, d'où il résulte qu'elle applique s_α sur s'_α et s_β sur s'_β. Elle induit donc une isogénie de Z_α sur Z'_α qui applique T_α sur T'_α et s_α sur s'_α. Or Z_α et Z'_α sont simplement connexes (proposition 2) ; il résulte alors de la proposition 4 que la restriction de $f_{\alpha\beta}$ à Z_α est identique à f_α ; on voit de même que sa restriction à Z_β est identique à f_β.

Nous allons maintenant définir une application f de G dans G'. Nous utiliserons les notations de la démonstration de la proposition 9 ; pour tout $w \in W$, nous désignerons par $B(w)$ l'ensemble des i $(1 \leq i \leq N)$ tels que $P_i \subset B^u_w$. Soit s un élément de G. Il existe un élément $w \in W$, des éléments $u_i \in P_i$ $(i \in B(w))$, un élément $t \in T$ et des éléments $u'_j \in P_j$ $(1 \leq j \leq N)$ tels que l'on ait

$$s = \prod_{i \in B(w)} u_i \cdot s(w) t \prod_{j=1}^{N} u'_j \ ;$$

de plus, ces éléments sont tous uniquement déterminés par la donnée de s. Pour tout i, nous désignerons par f_i la restriction de f_{δ_i} à P_i ; nous poserons

$$f(s) = \prod_{i \in B(w)} f_i(u_i) \cdot f_{N(T)}\left(s(w)t\right) \prod_{j=1}^{N} f_j(u'_j)\,.$$

L'application f ainsi définie prolonge manifestement f_T. Si α est l'une des racines δ_i, Z_α est engendré par P_i et par $s(w(\delta_i))$, où $w(\delta_i)$ est la réflexion par rapport à δ_i. Il en résulte immédiatement que f prolonge f_α ; comme toute racine est ou bien de la forme δ_i ou bien de la forme $-\delta_i$, on voit que la restriction de f à Z_α est un homomorphisme de ce groupe. On voit de même que, si α et β sont des racines quelconques, la restriction de f à $Z_{\alpha\beta}$ est un homomorphisme de ce groupe dans G'. Enfin, comme f prolonge $f_{N(T)}$, sa restriction à $N(T)$ est un homomorphisme. Il résulte alors du corollaire à la proposition 9 que f est un homomorphisme de G dans G'.

Montrons maintenant que f est un morphisme de la variété G dans la variété G'. L'application $(t, u_1, \ldots, u_N) \to t u_1 \ldots u_N$ est un isomorphisme de la variété $T \times P_1 \times \ldots \times P_N$ sur la variété B ; il en résulte immédiatement que f induit un morphisme de la variété B dans G'. Soit w_0 l'élément du groupe de Weyl qui transforme l'ensemble des δ_i en l'ensemble des $-\delta_i$; alors $(b^u, b') \to b^u\, s(w_0) b'$ est un isomorphisme de la variété $B^u \times B$ sur une sous-variété ouverte U de G ; il en résulte que la restriction de f à U est un morphisme de cette variété dans G'. Comme f est un homomorphisme de groupes et induit un morphisme d'une sous-variété ouverte de G dans G', f est un morphisme de la variété G dans G'.

La composante neutre dans le noyau de f admet un tore maximal contenu dans T et est semi-simple ; comme f induit une isogénie de T sur T', il en résulte que le noyau de f est fini. Comme $f(G)$ contient tous les groupes Z'_α, on a $f(G) = G'$. L'application f est donc une isogénie. Comme elle prolonge

f_T, l'isomorphisme spécial de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(T)$ attaché à f n'est autre que φ. Le théorème 1 est donc établi.

23.7 Conséquences et applications

Enonçons d'abord les corollaires au théorème 1.

Corollaire 1. – *Soient G et G' des groupes algébriques semi-simples ; soient T et T' des tores maximaux de G et G'. Pour que G et G' soient isomorphes, if faut et il suffit qu'il existe un isomorphisme φ de $X(T')$ sur $X(T)$ qui induise une bijection de l'ensemble des racines de G' sur celui des racines de G ; l'isomorphisme de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(T)$ qui prolonge φ est alors attaché à un isomorphisme de G sur G'.*

La condition est évidemment nécessaire, car, s'il existe un isomorphisme de G sur G', il en existe aussi un[5] qui applique T sur T'. Le caractère suffisant de la condition et la dernière assertion se déduisent du théorème 1 et de la proposition 6 du n° 18.4.

Corollaire 2. – *Soient G un groupe algébrique semi-simple, T un tore maximal de G et $(\alpha_1, \ldots, \alpha_n)$ un système fondamental de racines de G par rapport à T. Soit π une permutation de l'ensemble $\{\alpha_1, \ldots, \alpha_n\}$ qui définisse un automorphisme du diagramme de Dynkin. Soit φ l'automorphisme de $X^{\mathbf{Q}}(T)$ qui transforme α_i en $\pi(\alpha_i)$. Si φ transforme $X(T)$ en lui-même, il est attaché à un automorphisme de G.*

Cela résulte du corollaire 1.

Corollaire 3. – *Les notations étant celles du corollaire 2, le quotient du groupe des automorphismes de G par le groupe des automorphismes intérieurs est isomorphe au groupe des permutations de l'ensemble $\{\alpha_1, \ldots, \alpha_n\}$ qui définissent un automorphisme du diagramme de Dynkin et se prolongent en un automorphisme de $X(T)$.*

Cela résulte du corollaire 2 et la proposition 1 du n° 17.3.

Corollaire 4. – *Utilisons les notations du corollaire 2 ; supposons de plus que G soit simplement connexe ou adjoint*[6]*. Le quotient du groupe des automorphismes de G par le groupe des automorphismes intérieurs est alors isomorphe au groupe des automorphismes d'un diagramme de Dynkin de G.*

En effet, toute permutation de $\{\alpha_1, \ldots, \alpha_n\}$ qui définit un automorphisme du diagramme de Dynkin se prolonge en un automorphisme du groupe des racines, qui se prolonge lui-même en un automorphisme du groupe des poids.

[5] Ceci résulte du théorème de conjugaison des tores maximaux (n° 6.5, théorème 5).

[6] Voir la définition 1 du n° 21.1.

On notera que tous les groupes de l'un des types G_2, F_4 ou E_8 sont isomorphes entre eux ; en effet, dans le cas de ces groupes, le groupe des racines est identique au groupe des poids.

Pour terminer, donnons la construction des deux isogénies "exceptionnelles" en caractéristique 2. On rappelle aussi l'existence de l'isogénie exceptionnelle du groupe G_2 avec lui-même en caractéristique 3 (n° 21.4, proposition 1). Supposons que le corps K soit de caractéristique 2. Soit G un groupe algébrique semi-simple de type F_4 ; soit T un tore maximal de G. Utilisons les notations de l'exposé 19. Les formules

$$\varphi(\omega_1) = \omega_4 - \omega_1 \qquad \varphi(\omega_2) = \omega_2 + \omega_3$$

$$\varphi(\omega_3) = \omega_2 - \omega_3 \qquad \varphi(\omega_4) = \omega_1 + \omega_4$$

définissent un automorphisme φ de $X^{\mathbf{Q}}(T)$ qui applique $X(T)$ dans lui-même ; on a

$$\varphi(\alpha_1) = 2\alpha_4\,,\ \varphi(\alpha_2) = 2\alpha_3\,,\ \varphi(\alpha_3) = \alpha_2\,,\ \varphi(\alpha_4) = \alpha_1\,.$$

Soit Q une forme quadratique définie positive que $X^{\mathbf{Q}}(T)$ invariante par le groupe de Weyl ; notons $(\lambda \mid \mu)$ le produit scalaire de deux éléments λ et μ relativement à Q. On a $(\omega_i \mid \omega_j) = 0$ si $i \neq j$, et les $(\omega_i \mid \omega_i)$ sont tous égaux entre eux. Il en résulte aussitôt que l'on a $Q(\varphi(\lambda)) = 2Q(\lambda)$. Si donc w est une opération du groupe de Weyl, $\varphi \circ w \circ \varphi^{-1}$ laisse encore Q invariante. Si w est la réflexion par rapport à l'une des racines fondamentales, $\varphi \circ w \circ \varphi^{-1}$ est la réflexion par rapport à un hyperplan de $X^{\mathbf{Q}}(T)$, et transforme l'une au moins des racines fondamentales en son opposée. Il en résulte aussitôt que $w \to \varphi \circ w \circ \varphi^{-1}$ est un automorphisme du groupe de Weyl, donc que, pour toute racine α, $\varphi(\alpha)$ est de la forme $q\alpha'$, où q est un nombre égal à 1 ou 2. L'automorphisme φ est donc spécial ; il définit une isogénie du groupe G sur lui-même, qui n'a pas d'analogue en caractéristique 0.

Supposons toujours que K soit de caractéristique 2. Soient G un groupe de type B_n et G' un groupe de type C_n ; soient T et T' des tores maximaux de G et G', $(\alpha_1, \ldots, \alpha_n)$ et $(\alpha'_1, \ldots, \alpha'_n)$ des systèmes fondamentaux de racines de G et G' par rapport à T et T' respectivement donnant lieu aux diagrammes de Dynkin indiqués à l'exposé 19. Nous poserons

$$\alpha_i = \omega_i - \omega_{i+1} \qquad (1 \leq i \leq n-1)\,, \qquad \alpha_n = \omega_n$$

$$\alpha'_i = \omega'_i - \omega'_{i+1} \qquad (1 \leq i \leq n-1)\,, \qquad \alpha'_n = 2\omega'_n\,.$$

Les formules $\varphi(\omega'_i) = \omega_i$ $(1 \leq i \leq n)$ définissent un isomorphisme φ de $X^{\mathbf{Q}}(T')$ sur $X^{\mathbf{Q}}(T)$. Il est clair que, si α' est une racine quelconque de G', $\varphi(\alpha')$ est de la forme $q\alpha$, où α est une racine de G et q un entier égal à 1 ou 2. Le groupe $X(T')$ est contenu dans le groupe engendré par les ω'_i ; son image par φ est donc contenue dans $X(T)$. L'isomorphisme φ est donc spécial et est

attaché à une isogénie[7] de G sur G'. Considérons maintenant l'isomorphisme $2\,\varphi^{-1}$ de $X^{\mathbf{Q}}(T)$ sur $X^{\mathbf{Q}}(T')$; il applique toute racine de G soit sur une racine de G' soit sur le double d'une racine de G'. Si G n'est pas simplement connexe, *i.e.* s'il est isomorphe à $\mathrm{SO}(2n+1)$, $X(T)$ est engendré par les racines et $2\,\varphi^{-1}$ est spécial ; il définit donc une isogénie de G' sur $\mathrm{SO}(2n+1)$. Si G est simplement connexe, $X(T)$ est engendré par les racines et par l'élément $\frac{1}{2}\sum_{i=1}^{n}\omega_i$, dont l'image par $2\,\varphi^{-1}$ est $\sum_{i=1}^{n}\omega'_i$. Si G' est simplement connexe $\sum_{i=1}^{n}\omega'_i$ appartient toujours à $X(T')$, et $2\,\varphi^{-1}$ définit une isogénie de G' sur G ; il en est encore ainsi si G' n'est pas simplement connexe dans le cas où n est pair.

[7] On peut l'expliciter ainsi. Il existe une isogénie $f : G \to \mathrm{SO}(2n+1)$ car G est de type B_n et que $\mathrm{SO}(2n+1)$ est adjoint de type B_n ; il existe aussi une isogénie $f' : \mathrm{Sp}\,n \to G'$ d'après le théorème 1 du n° 22.3. Enfin, comme K est de caractéristique 2, on a construit au n° 22.2 une isogénie $\omega : \mathrm{SO}(2n+1) \to \mathrm{Sp}\,n$. L'isogénie cherchée est $f' \circ \omega \circ f$.

24. Conclusion

Il resterait à compléter les résultats précédents en montrant qu'il existe des groupes semi-simples de tous les types possibles. Dans le mémoire "Sur certains groupes simples" (Tôhoku Math. Journ., 1954), C. Chevalley a montré que, pour tout type simple $\mathfrak{T}$, il existe un groupe algébrique semi-simple de type $\mathfrak{T}$; on montre facilement que ces groupes sont "adjoints" au sens de la définition 1 du n° 21.1. Il en résulte que, pour tout type de diagramme de Dynkin, simple ou non, il existe un groupe G_0 du type en question tel que, T_0 désignant un tore maximal de G_0, $X(T_0)$ soit engendré par les racines. Si M est un sous-groupe du groupe des poids contenant le groupe des racines, M est engendré par des poids dominants ; le raisonnement de la démonstration de la proposition 1 du n° 23.1 permet alors d'établir qu'il existe un groupe semi-simple G et une isogénie f de G sur G_0 qui possède les propriétés suivantes : si T est le tore maximal de G tel que $f(T) = T_0$ et φ l'isomorphisme de $X^{\mathbf{Q}}(T_0)$ sur $X^{\mathbf{Q}}(T)$ attaché à f, les exposants radiciels de φ sont égaux à 1, et φ applique $X(T)$ sur le groupe donné M.

25. Postface[1]
Sur les problèmes de classification des groupes

25.1 De Galois à Lie et Cartan

Dans ses travaux sur la théorie des équations algébriques, Galois introduit la notion de groupe, puis celle de sous-groupe invariant et enfin celle de groupe simple ; d'une manière qui sera précisée par Jordan et Hölder, il montre que tout groupe fini est "composé" de groupes simples, et qu'en principe il suffit de savoir résoudre les équations à groupe de Galois simple. Les groupes cycliques d'ordre premier étaient déjà apparus (implicitement) dans les travaux de Lagrange et Gauss, et Galois introduit les premiers groupes simples non commutatifs, à savoir $\mathrm{PSL}_2(\mathbb{F}_p)$ (pour p premier). Il reviendra ensuite à Jordan d'introduire les groupes linéaires classiques sur un corps premier $\mathbb{F}_p$: linéaire, orthogonal, symplectique (appelé "abélien", ou "hyperabélien" jusque vers 1935).

On en est là vers 1870 quand Sophus Lie commence à développer la théorie des groupes "finis et continus". Son ambition est de créer une théorie de Galois des équations différentielles – mais de ce point de vue, c'est un essai avorté – ce qui l'amène naturellement à l'idée de groupe de Lie simple. Les groupes linéaires "classiques" sont assez rapidement reconnus, et leur simplicité prouvée. Y en a-t-il d'autres ? La réponse est donnée par Killing [14] en 1888, puis confirmée dans la thèse d'Elie Cartan [4] en 1894. Pour prouver cela, il faut introduire de nouvelles méthodes : au lieu de considérer les groupes de Lie, on considère les algèbres de Lie correspondantes – appelées à l'époque "groupes infinitésimaux". On peut alors utiliser des méthodes d'algèbre linéaire, en liaison avec la forme quadratique, dite de Killing, dont la non-dégénérescence caractérise, selon un critère d'E. Cartan, les algèbres de Lie semi-simples (c'est-à-dire, les produits d'algèbres simples). La nomenclature A_n, B_n, C_n, D_n pour les groupes classiques s'impose après E. Cartan, et la nouveauté réside dans les cinq groupes "exceptionnels" désignés par

$$E_6\,,\ E_7\,,\ E_8\,,\ F_4\,,\ G_2\,.$$

Les méthodes d'Elie Cartan sont compliquées et peu transparentes. Entre 1930 et 1940, de nouvelles méthodes géométriques sont développées par

[1] Postface de Pierre Cartier, ajoutée en septembre 2004.

E. Witt, H.M.S. Coxeter, B.L. van der Waerden – sous l'influence d'Hermann Weyl. Ce dernier associe à chaque groupe de Lie compact G un groupe fini W, le *groupe de Weyl*, qui admet une représentation linéaire fidèle dans un espace vectoriel de dimension égale au rang ℓ de G. Ce groupe est engendré par des réflexions orthogonales et laisse un réseau invariant. La classification de ces groupes de réflexions est entreprise par Coxeter, et se trouve coïncider avec celle des groupes de Lie simples. Il faudra attendre Chevalley [6] en 1948, puis Harish-Chandra [13], pour avoir une explication *a priori* de cette coïncidence.

25.2 Retour aux groupes finis

L'analogie entre les groupes de Lie classiques et les groupes finis obtenus comme groupes classiques sur un corps fini était patente. Il restait à obtenir les analogues finis des groupes de Lie exceptionnels. Dickson, au début du 20^{e} siècle, ne se contenta pas de définir les groupes classiques sur un corps quelconque (et en particulier sur un corps fini) ; il construisit, par des méthodes algébriques, les analogues finis de G_2 et E_6. En 1953, Chevalley construisit les analogues des groupes exceptionnels F_4, E_6 et E_7 sur un corps quelconque. Il m'a souvent expliqué que c'est à la suite d'échecs répétés dans la construction de E_8 – la complexité des calculs rebutant même un calculateur aussi entraîné que lui – qu'il se résolut à chercher une méthode générale qui permettrait d'associer directement un groupe à toute algèbre de Lie simple $\mathfrak{g}$ (sur le corps des nombres complexes) et à tout corps commutatif K. C'est l'objet d'un de ses articles les plus fameux [8]. Il y introduisit un grand nombre d'outils nouveaux, mais *les groupes algébriques n'y apparaissaient pas explicitement.* Cet article ouvrit la voie à toute une série de travaux (Tits, Steinberg, Ono, ...) qui permirent la construction de nouveaux groupes finis simples – les groupes de Chevalley et leurs variantes "tordues" [5].

On pouvait dès lors songer à reprendre la classification de tous les groupes finis simples. Une fois compris comment un groupe algébrique simple sur un corps de caractéristique $p \neq 0$ permet d'engendrer des groupes finis simples (en prenant les points sur un corps fini $\mathbb{F}_q$), il était urgent d'explorer la classification des groupes algébriques simples en caractéristique p. La situation était peu encourageante : au niveau des algèbres de Lie, Witt avait introduit de nouvelles algèbres de Lie simples ; au niveau des groupes, la classification des groupes formels commutatifs en caractéristique p, obtenue par J. Dieudonné, nous découvrait un monde nouveau, qui n'est pas encore complètement exploré. Ce fut donc un coup de tonnerre lorsque Chevalley *annonça qu'il avait prouvé que la classification des groupes algébriques simples était indépendante de la caractéristique, $p \neq 0$ ou $p = 0$.*

La classification des groupes finis simples se poursuivit par la construction des 26 groupes "sporadiques" qui ne semblent avoir aucun lien avec les groupes algébriques, et l'annonce que ceux-ci fermaient la classification [12].

25.3 L'histoire du séminaire

La première annonce de Chevalley eut lieu pendant le Congrès Bourbaki de juin 1956, à Die, où il donna en présence de Borel, Godement, Serre, Bruhat et moi-même, parmi d'autres participants, un long exposé décrivant ses méthodes. Il s'appuyait de manière essentielle sur les résultats de Borel [1] obtenus un an plus tôt, concernant en particulier les sous-groupes résolubles connexes maximaux (appelés depuis "sous-groupes de Borel"). Je laisse à Borel [2] le soin d'expliquer la gestation de ses résultats, qui sont d'ailleurs l'objet des chapitres 4 à 7 du présent ouvrage, écrits par A. Grothendieck.

Je voudrais décrire rapidement l'atmosphère mathématique du temps à Paris. Entre 1947 et 1960, l'activité de recherche en mathématiques "pures" était centrée sur le Séminaire Cartan, qui se tenait traditionnellement le lundi à l'Ecole Normale Supérieure, de 14 à 16 heures[2]. Cartan s'intéressait à de multiples aspects de la topologie, des fonctions de variables complexes, des fonctions automorphes ... Borel et Grothendieck y avaient participé au début, mais Serre était le principal acteur – hormis Cartan bien sûr. Lorsque Chevalley s'installa à Paris, à l'automne 1955, le Séminaire Cartan devint (pour une année) le "Séminaire Cartan-Chevalley" et se consacra aux fondements de la géométrie algébrique (voir la section suivante). Parmi les conférenciers, outre Chevalley, on trouve en particulier Godement et moi-même. Dans la mouvance du Séminaire Cartan, j'avais en 1954-55, et en collaboration avec Michel Lazard, dirigé un Séminaire consacré à l'étude de la structure et de la classification des algèbres de Lie complexes. Nous utilisâmes largement des documents internes de Bourbaki. En fait, toutes ces manifestations participaient de l'élan donné par Bourbaki et qui allait se concrétiser par la publication des volumes de Bourbaki sur les groupes de Lie (entre 1965 et 1975).

Le terrain était donc favorable, et Chevalley s'assura de la collaboration de Grothendieck, Lazard et moi-même pour un Séminaire qui débuta à l'automne 1956 et dura jusqu'en février 1958. Le Séminaire de Chevalley continua encore deux années, sur d'autres thèmes plus liés à la géométrie algébrique, et non plus centrés sur un objectif unique.

25.4 Fondements de la géométrie algébrique

Les années 1950 furent une époque de changements très rapides dans ce sujet. A partir de 1935, s'appuyant sur les acquis de l'"algèbre moderne" (titre de son ouvrage fameux), B.L. van der Waerden entreprit de donner des fondements algébriques rigoureux à la théorie des variétés algébriques de dimension

[2] A partir de 1955, L. Schwartz développa un autre pôle, plus tourné vers l'Analyse, et qui devait donner naissance au courant des mathématiques "appliquées" autour de J.-L. Lions.

supérieure (au moins égale à 2) ; le cas des courbes était déjà bien compris, grâce aux efforts de Dedekind, Weber, Deuring, Hasse, qui développèrent l'analogie entre les nombres algébriques et les fonctions algébriques d'une variable. En particulier, Chow et van der Waerden développèrent une théorie des multiplicités d'intersection.

Lorsqu'André Weil entreprit de rédiger sur une base solide sa démonstration de l'hypothèse de Riemann-Artin pour les courbes algébriques sur un corps fini, les théories existantes avaient deux lacunes :

– une théorie des intersections en caractéristique $p \neq 0$, qui tienne compte des phénomènes d'extensions algébriques purement inséparables ;

– une construction de la jacobienne d'une courbe.

La théorie des intersections est locale ; Zariski et Samuel l'avaient formulée en termes d'anneaux locaux, et la formule des "Tor" de Serre en est le couronnement naturel. La construction de la jacobienne est un phénomène global, qui força Weil à introduire des variétés "abstraites" par recollement – en imitant une procédure familière en géométrie différentielle.

L'exposé de Weil n'était guère intrinsèque, et la notion de corps de définition d'une variété n'était guère maniable. Ceci fut corrigé de manière à peu près simultanée par Serre [15] et Chevalley [9]. Serre utilisa les méthodes déjà éprouvées en théorie des fonctions de plusieurs variables complexes : il basait tout sur la *topologie de Zariski*, et les faisceaux correspondants. Sa méthode fonctionnait bien si le corps de base K est algébriquement clos, car on peut alors identifier une variété algébrique X sur K à l'ensemble $X(K)$ de ses points rationnels. Chevalley se restreignait aux variétés irréductibles, mais ne supposait pas le corps de base K algébriquement clos. Pour lui, une variété X sur K était décrite par le *schéma*[3] correspondant :

– le corps F des fonctions rationnelles sur X, une extension de type fini de K ;

– une collection d'anneaux locaux $\mathcal{O}_x$, de corps des fractions F, et contenant K.

Chevalley accordait un rôle mineur à la topologie de Zariski, contrairement à Serre.

Pour les besoins de ma thèse, j'essayai de faire une synthèse des deux points de vue, en n'obligeant pas le corps de base à être algébriquement clos comme Serre, et les variétés à être irréductibles comme Chevalley. Les deux premiers chapitres de cet ouvrage donnent un exposé un peu maladroit de ma synthèse. En fait, *tout le reste de l'ouvrage ne s'intéresse qu'aux corps de base algébriquement clos*, et l'on aurait pu se contenter de la présentation de Serre.

[3] Attention : le schéma d'une variété n'est pas constitué par l'ensemble de ses points, mais par l'ensemble ordonné des sous-variétés irréductibles.

Grothendieck balayera toutes ces difficultés en introduisant les schémas généraux[4] – il semblait à cette époque qu'on dût réapprendre les bases de la géométrie algébrique tous les cinq ans !

25.5 Groupes algébriques

Il n'est pas dans mon intention de réécrire ici l'histoire des groupes algébriques, d'autant plus que Borel l'a fait de main de maître dans [2], chapitres V et VI. Pour nous, le point de départ est constitué par le livre de Chevalley sur les groupes algébriques linéaires [7]. Il y définit la notion de groupe algébrique de matrices sur un corps K, et, par analogie avec la théorie des groupes de Lie, introduit l'algèbre de Lie associée à un groupe algébrique. Un résultat important est la *décomposition de Jordan additive*

$$X = X_s + X_n$$

d'une matrice X en somme d'une partie semi-simple X_s et d'une partie nilpotente X_n avec $X_s X_n = X_n X_s$. Si $\mathfrak{g} \subset \mathfrak{gl}_n(K)$ est l'algèbre de Lie d'un groupe algébrique, elle est stable par décomposition de Jordan :

$$\textit{pour tout } X \in \mathfrak{g}\textit{, on a } X_s \in \mathfrak{g} \textit{ et } X_n \in \mathfrak{g}.$$

La réciproque est fausse, et Chevalley développe à cette occasion la notion de réplique, qui permet de construire la plus petite algèbre de Lie "algébrique"[5] contenant une matrice X donnée.

La théorie de Lie ne fonctionne correctement que si le corps K est de caractéristique 0. La théorie différentielle en caractéristique $p \neq 0$ fut un sujet important de recherches vers 1950 (Jacobson, Dieudonné, Barsotti, Tate, moi-même ...), avec des applications à la théorie des courbes et des variétés abéliennes[6] ; curieusement, elle n'intervient essentiellement pas dans l'étude des groupes algébriques simples.

Il fallait inventer des méthodes plus globales, ce qui fut fait par Kolchin et Borel. Ces auteurs découvrirent l'importance de la *décomposition de Jordan multiplicative*

$$g = g_s \cdot g_u = g_u \cdot g_s$$

avec g_s semi-simple et g_u unipotent (c'est-à-dire $1 - g_u$ nilpotent). Un groupe algébrique G est stable par cette décomposition :

$$\textit{pour tout } g \in G\textit{, on a } g_s \in G \textit{ et } g_u \in G.$$

[4] En particulier, la notion de produit fibré $X \underset{S}{\times} Y$ de deux schémas au-dessus de la même base S résout une fois pour toutes les problèmes liés à l'extension des scalaires.

[5] C'est-à-dire, correspondant à un sous-groupe algébrique de $\mathrm{GL}_n(K)$.

[6] Cette direction se poursuit encore aujourd'hui : "cohomologie cristalline".

De plus, pour tout homomorphisme de groupes algébriques $f : G \to G'$, l'image d'un élément semi-simple (resp. unipotent) de G est semi-simple (resp. unipotent) dans G'. Ceci montre que la décomposition de Jordan multiplicative, définie par référence à un plongement $G \subset \mathrm{GL}_n(K)$, est en fait intrinsèque.

Kolchin s'efforce de développer une théorie de Galois des équations différentielles ; sur le modèle de Galois, les groupes résolubles (et nilpotents) y jouent un rôle fondamental. Kolchin, suivi en cela par Borel, étudie la structure des groupes résolubles et reconnaît l'importance des groupes unipotents (où tout élément est unipotent). En particulier, pour un groupe commutatif, on a une décomposition de Jordan globale en produit direct de deux sous-groupes

$$G = G_s \cdot G_u \,,$$

où G_s (resp. G_u) se compose des éléments semi-simples (resp. unipotents) de G. Les groupes semi-simples (resp. réductifs) sont caractérisés par le fait de ne posséder aucun sous-groupe algébrique connexe invariant commutatif (resp. et unipotent) non réduit à l'unité.

Revenons aux fondements de la géométrie algébrique. Kolchin se construit, sur le modèle de Weil, un système fort compliqué, et Borel, dans son grand article, hésite entre plusieurs présentations concurrentes. Si l'on veut définir un groupe algébrique G, sans référence à une représentation linéaire fidèle particulière $G \subset \mathrm{GL}_n(K)$, on peut considérer la catégorie de toutes les représentations linéaires de G : c'est le *point de vue tannakien*. On introduit ensuite *l'anneau représentatif* $\mathcal{O}$ formé des coefficients des représentations. La multiplication dans $\mathcal{O}$ reflète le produit tensoriel des représentations, les éléments du groupe G correspondent aux homomorphismes de K-algèbres de $\mathcal{O}$ dans K, et la multiplication dans G correspond à un coproduit

$$\Delta : \mathcal{O} \to \mathcal{O} \otimes_K \mathcal{O} \,,$$

un homomorphisme d'algèbres. Autrement dit, $\mathcal{O}$ est une *algèbre de Hopf*. L'algèbre $\mathcal{O}$ est soumise aux restrictions suivantes :

(a) elle est commutative ;

(b) elle est engendrée sur K par un nombre fini d'éléments ;

(c) elle ne contient pas d'élément nilpotent non nul.

L'hypothèse (a) est essentielle, l'hypothèse (b) est commode, et j'ai prouvé que l'hypothèse (c) résulte de (a) si le corps K est de caractéristique 0.

On peut fort bien développer sur cette base la théorie des groupes algébriques linéaires, mais l'obstacle provient des espaces homogènes. Par exemple, la droite projective $\mathbb{P}^1(K)$ est l'espace homogène G/B, où $G = \mathrm{GL}_2(K)$ et B se compose des matrices triangulaires $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ avec $ad \neq 0$. Or, Borel démontre les résultats fondamentaux suivants :

(1) Si un groupe algébrique résoluble connexe agit sur une variété projective, il possède un point fixe.

(2) Si B est un sous-groupe de Borel de G (résoluble connexe maximal), l'espace homogène G/B est une variété projective.

Il faut donc sortir du cadre des variétés affines. Il faut aussi construire les espaces homogènes G/H et en particulier les groupes quotients. La première démonstration d'existence à la fois transparente et convaincante est due à Chevalley ; elle constitue le chapitre 8 de cet ouvrage.

25.6 Systèmes de racines

La classification d'E. Cartan repose sur la considération des systèmes de racines. Soit $\mathfrak{g}$ une algèbre de Lie semi-simple complexe ; une sous-algèbre de Cartan $\mathfrak{h}$ de $\mathfrak{g}$ est une sous-algèbre commutative de $\mathfrak{g}$, dont tous les éléments agissent de manière semi-simple dans $\mathfrak{g}$ par la représentation adjointe, et maximale pour ces propriétés. Ayant fixé $\mathfrak{g}$ et $\mathfrak{h}$, il existe un ensemble R de formes linéaires sur $\mathfrak{h}$, les racines, et une décomposition en somme directe

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in R} \mathfrak{g}_\alpha \,,$$

où $\mathfrak{g}_\alpha$, de dimension 1, se compose des $X \in \mathfrak{g}$ tels que $[H, X] = \alpha(H) \cdot X$ pour tout H dans $\mathfrak{h}$. Si α est une racine, il en est de même de $-\alpha$. On choisit pour toute racine α un élément X_α non nul de $\mathfrak{g}_\alpha$ et l'on pose $H_\alpha = [X_\alpha, X_{-\alpha}]$; c'est un élément de $\mathfrak{h}$ et l'on peut normaliser les choses de sorte que $\alpha(H_\alpha) = 2$. L'élément H_α, appelé la coracine associée à α, est défini sans ambiguïté dans $\mathfrak{h}$. L'ensemble $R \subset \mathfrak{h}^*$ et l'application $\alpha \mapsto H_\alpha$ de R dans $\mathfrak{h}$ constituent le *système de racines* associé à $\mathfrak{g}$ et $\mathfrak{h}$. Parmi les propriétés de ce système, notons les suivantes :

(A) *Pour α, β dans R, le nombre $\beta(H_\alpha)$ est entier.*

(B) *Pour α dans R, définissons la réflexion S_α par*

$$S_\alpha(H) = H - \alpha(H) \cdot H_\alpha$$

pour H dans $\mathfrak{h}$, et de manière duale dans $\mathfrak{h}^*$

$$S_\alpha(\lambda) = \lambda - \lambda(H_\alpha) \cdot \alpha \,.$$

Alors R est stable par S_α pour tout α dans R.

Ces propriétés constituent les axiomes d'un système de racines.

A ma connaissance, c'est au chapitre 14 du présent ouvrage qu'on trouve la première présentation autonome des systèmes de racines. Ce chapitre est une commande qui m'avait été faite par Chevalley. Dans la situation ci-dessus,

les réflexions S_α engendrent un groupe fini W, le *groupe de Weyl*. On montre facilement qu'il existe une base $\{\alpha_1, \ldots, \alpha_\ell\}$ de $\mathfrak{h}^*$ formée de racines, et telle que toute racine soit de la forme $\pm(m_1\,\alpha_1 + \cdots + m_\ell\,\alpha_\ell)$ où $m_1, \ldots, m_\ell$ sont des entiers positifs (base des racines). Le groupe W est alors engendré par les réflexions $S_i = S_{\alpha_i}$ pour $1 \leq i \leq \ell$. La question de Chevalley était : les relations du type $(S_i\,S_j)^{m_{ij}} = 1$ suffisent-elles à donner une présentation du groupe W ? En fait, ni Chevalley, ni moi-même, ne savions que ceci avait été prouvé vers 1935 par Coxeter (ce que Borel nous apprit quelque temps plus tard).

La stratégie de Chevalley est d'associer à un groupe algébrique semi-simple un système de racines, d'appliquer le théorème de classification des systèmes de racines (Witt, van der Waerden, ... vers 1935), puis de montrer qu'un groupe algébrique semi-simple est caractérisé, à isogénie près, par son système de racines.

On avait là un deuxième exemple d'une situation conduisant à un système de racines. Borel, Chevalley et moi-même n'eurent guère de mal à convaincre Bourbaki de développer les systèmes de racines *per se*, et c'est là l'origine du manuel bien connu de Bourbaki sur le sujet [3].

25.7 La méthode de Chevalley

Nous décrivons maintenant rapidement le contenu de cet ouvrage. Les chapitres 1 à 8 ne sont que des préliminaires, contenant en particulier les résultats de Kolchin et Borel. Au chapitre 9, on prouve que si G est un groupe algébrique connexe, tout sous-groupe de Borel B de G est égal à son normalisateur dans G. Chevalley a toujours dit qu'ensuite il n'y avait plus qu'à suivre la pente !

Il faut ensuite construire le système de racines. Soient donc G un groupe algébrique semi-simple (connexe) et T un tore maximal. On prouve que T est la composante neutre de son normalisateur $\mathcal{N}(T)$, et l'on introduit le groupe fini $\mathcal{N}(T)/T = W$, selon une méthode globale utilisée par H. Weyl, Samelson et Borel pour les groupes de Lie compacts. On introduit ensuite le groupe $X(T)$ des homomorphismes de groupes algébriques de T dans le groupe multiplicatif $\mathbb{G}_m = \mathrm{GL}_1(K)$. C'est un groupe commutatif libre de rang ℓ égal à la dimension de T. Ce qui va jouer le rôle du dual $\mathfrak{h}^*$ d'une algèbre de Cartan est l'espace vectoriel $X^{\mathbb{R}}(T) = \mathbb{R} \otimes_{\mathbb{Z}} X(T)$ sur le corps $\mathbb{R}$ des nombres réels. Le groupe W agit sur $X^{\mathbb{R}}(T)$, mais il faut définir les racines (sans utiliser l'algèbre de Lie !). Pour cela, on montre qu'il existe des sous-tores S de T de dimension $\ell - 1$, dont le centralisateur $\mathcal{Z}(S)$ est de dimension $\ell + 2$. Le groupe $\mathcal{Z}(S)/S$ est isomorphe à $\mathrm{SL}_2(K)$ ou à $\mathrm{PGL}_2(K)$. L'étude de ce dernier groupe permet d'introduire deux éléments opposés $\pm\alpha$ de $X(T) \subset X^{\mathbb{R}}(T)$ tels que S soit la composante neutre du noyau de α. En faisant varier S, on obtient toutes les racines.

L'étape suivante (chapitre 15) est une extension de la méthode de Borel-Weil pour construire les représentations projectives irréductibles. On se donne un tore maximal T de G, puis un sous-groupe de Borel B de G contenant T, correspondant au choix d'une base du système de racines. Si λ est un caractère de T, "dominant" par rapport à B, on l'étend en un caractère de B, trivial sur le radical unipotent U de B. Au caractère λ, on associe un fibré en droites L_λ de base G/B ; la représentation cherchée de G agit sur l'espace projectif associé à l'espace vectoriel des sections de L_λ. Elle n'est pas toujours irréductible si le corps K est de caractéristique $p \neq 0$, mais elle contient une unique sous-représentation irréductible.

La fin du séminaire (qui correspond aux exposés de l'automne 1957) est consacrée au *théorème d'unicité*. Soient G et G' deux groupes algébriques semi-simples connexes, T un tore maximal de G, et T' un tore maximal de G'. Un isomorphisme u de $X(T)$ sur $X(T')$ correspond à un isomorphisme v de T sur T'. Pour que v s'étende en un isomorphisme de G sur G', il faut (bien sûr !) et il suffit que u transforme l'ensemble $\Phi \subset X(T)$ des racines de G en l'ensemble $\Phi' \subset X(T')$ des racines de G'.

La démonstration est très longue, et suppose une analyse détaillée des groupes de rang 2 et des groupes de type A_n. Le théorème du chapitre 14 sur l'engendrement du groupe de Weyl sert à montrer comment reconstruire un groupe algébrique semi-simple connexe à partir de ses sous-groupes de rang 2. En fait, la démonstration de Chevalley couvre le cas des isogénies, c'est-à-dire le cas des homomorphismes surjectifs à noyau fini. C'est là que les phénomènes de caractéristique $p \neq 0$ se manifestent, en particulier par l'existence du morphisme de Frobenius qui transforme une matrice $g = (g_{ij})$ en la matrice (g_{ij}^p). Il faut admirer l'art avec lequel Chevalley esquive les difficultés de cette situation, et aussi la découverte d'isogénies exceptionnelles (en particulier G_2 en caractéristique 3 et F_4 en caractéristique 2). Elles joueront un rôle dans la construction de nouveaux groupes finis simples.

Le Séminaire Chevalley ne donne pas la construction d'un groupe correspondant à un système de racines donné. Chevalley renvoie pour cela à son article du Tohoku Math. J. [8]. Il reviendra sur ce sujet dans un exposé Bourbaki [10]. Il a donc démontré l'unicité, mais non l'existence dans sa classification. Celle-ci est plus précise, même dans le cas des groupes de Lie compacts, que ce qui était connu, car elle permet de distinguer des groupes isogènes, un résultat "global" que ne peut donner la classification des algèbres de Lie semi-simples.

L'étape suivante sera le Séminaire SGA3 de Demazure et Grothendieck consacré aux schémas en groupes [11].

Bibliographie

1. A. Borel, *Groupes linéaires algébriques*, Ann. of Math. (2) **64** (1956), pp. 20-82 = *Œuvres* I, pp. 490-552.
2. A. Borel, Essays in the history of Lie groups and algebraic groups, Amer. Math. Soc., Hist. of Math., vol 21, 2001.
3. N. Bourbaki, Groupes et algèbres de Lie, Chap. 4, 5, 6, Masson, Paris, 1981.
4. E. Cartan, Sur la structure des groupes de transformations finis et continus, Thèse, Nony, Paris, 1894 = *Œuvres Complètes* I_1, pp. 137-287.
5. R. Carter, Finite groups of Lie type, Conjugacy classes and complex characters, Wiley, 1985.
6. C. Chevalley, *Sur la classification des algèbres de Lie simples et de leurs représentations*, C.R. Acad. Sci. Paris **227** (1948), pp. 1136-8.
7. C. Chevalley, Théorie des groupes de Lie II. Groupes algébriques, Hermann, Paris, 1951.
8. C. Chevalley, *Sur certains groupes simples*, Tôhoku Math. J. (2) **7** (1955), pp. 14-66.
9. C. Chevalley, *Sur la théorie des variétés algébriques*, Nagoya Math. J. **8** (1955), pp. 1-43.
10. C. Chevalley, *Certains schémas de groupes semi-simples*, Sém. Bourbaki, vol. 6, 1960/61, Exp. **219**, Soc. Math. France, 1995.
11. M. Demazure et A. Grothendieck (édit.), Schémas en groupes I, II, III (SGA3), Lecture Notes in Math. vol. 151-153, Springer, 1970.
12. D. Gorenstein, Finite simple groups, an introduction to their classification, Plenum Press, 1982.
13. Harish-Chandra, *On some applications of the universal algebra of a semi-simple Lie algebra*, Trans. Amer. Math. Soc. **70** (1951), pp. 28-96 = *Coll. Papers* I, pp. 292-360.
14. W. Killing, *Die Zusammensetzung der stetigen endlichen Transformationsgruppen*, I, II, III, IV, Math. Annalen **31** (1886), pp. 252-290 ; **33** (1888), pp. 1-48 ; **34** (1889), pp. 57-122 ; **36** (1890), pp. 161-189.
15. J.-P. Serre, *Faisceaux algébriques cohérents*, Ann. of Maths. (2) **61** (1955), pp. 197-278 = *Œuvres* I, pp. 310-391.

Index

(k, K)-ensemble algébrique, 10
k-topologie, 11
k'-topologie, 20

absolument irréductible, 20
adjoint (groupe), 226
algèbre affine, 25
apparentées (localités), 25
application régulière, 10
application rationnelle, 21
arête, 122
associé à une racine α (isomorphisme), 193

carte, 11
chambre, 122, 159
chambre de Weyl, 118, 124
coefficient (d'une représentation), 41
cohomomorphisme, 91
complète (variété), 62
composable, 91
composante neutre, 34
composantes irréductibles, 3
composantes presque simples, 190
conditions (C), 140

diagonal, 45
diagonalisable, 45
diagramme admissible, 202
diagramme de Dynkin, 201
dimension de groupe, 205
diviseur, 163
diviseur positif, 164
diviseur principal, 164
dual, 46

elément régulier, 84
elément semi-simple, 50
ensemble algébrique, 10
ensemble fermé de racines, 179
entiers de Cartan, 178, 201
epais, 34

espace de transformation algébrique, 69
espace des coefficients, 41
exposant caractéristique, 41
exposants radiciels, 194

fonction composée, 91
fonction régulière, 16
fonction rationnelle, 21

grassmannienne, 64
groupe à un paramètre, 108
groupe algébrique, 33
groupe algébrique affine, 43
groupe algébrique de matrices, 33, 41
groupe algébrique diagonalisable, 45
groupe algébrique linéaire, 41
groupe de Weyl, 107
groupe de Weyl d'un diagramme, 204
groupe des caractères rationnels, 46
groupe des poids, 176
groupe des racines, 176
groupe linéaire associé à une représentation projective, 171
groupe symplectique projectif, 238

homomorphisme de systèmes locaux, 3
hyperplans limitrophes, 122

irréductible (espace), 2
isogénie, 191
isogénie des puissances q-ièmes, 192
isomorphisme attaché à une isogénie, 193
isomorphisme spécial, 194

linéairement équivalents (diviseurs), 164
localement fermé, 13
localité, 25

Main theorem de Zariski, 61
morphisme d'ensembles algébriques, 10

mur, 122

nœthérien (espace), 1
nilpotent (groupe), 35
non ramifié, 59
non ramifiée (localité), 65

orbite, 69
ouvert affine, 11

partie nilpotente, 48
partie semi-simple, 51
partie tubulaire, 95
partie unipotente, 51
poids, 171, 175
poids dominant, 172
poids dominant minimal, 215
poids dominants fondamentaux, 176
poids fondamentaux, 204
presque simple, 190
primitif (sous-groupe), 123
produit d'ensembles algébriques, 17
produit d'une famille de sous-groupes, 139
puissance extérieure (d'une représentation), 221

racine, 132, 152, 204
racine infinitésimale, 231
racines fondamentales, 145, 154
radical d'un groupe algébrique, 107
radicielle (isogénie), 191
reflexion, 151
régulier (élément), 84
régulier (sous-espace), 124
régulier (tore), 113
représentation contragrédiente, 41, 168, 221
représentation infinitésimale, 232
représentation projective, 167
représentations projectives fondamentales, 176
resoluble, 35
restriction d'un système local, 4

séparable (algèbre), 56
schéma, 26
schéma affine, 26
semi-invariant, 43
semi-régulier (sous-espace), 124
semi-régulier (tore), 113
semi-simple (endomorphisme), 47
semi-simple (groupe algébrique), 107
simple (représentation projective), 167
simple (système de racines), 189
simplement connexe (groupe), 226
singulier (sous-espace), 124
singulier (tore), 113
sous-ensemble algébrique, 15
sous-groupe de Borel, 75
sous-groupe de Cartan, 83
sous-groupe radiciel, 184
sous-groupe unipotent (associé à une racine), 193
spectre (d'une algèbre), 8
support d'un diviseur, 164
système de racines, 152
système de racines simples, 154
système linéaire de diviseurs, 164
système local de fonctions, 3

topologie de Zariski, 8, 11
tore algébrique, 45

unipotent (élément), 50
unipotent (endomorphisme), 48
unipotent (groupe algébrique), 51

variété algébrique, 24
variété des drapeaux de V, 65
variété des drapeaux de type $(d_1, \ldots, d_k)$, 65
variété normalisée, 60
variété projective, 62
variété quotient, 92