MÉMOIRES DE LA S. M. F.

JACQUES VELU

Courbes elliptiques munies d'un sous-groupe $\mathbb{Z}/n\mathbb{Z} \times \mu_n$

Mémoires de la S. M. F., tome 57 (1978)

<http://www.numdam.org/item?id=MSMF_1978__57__1_0>

© Mémoires de la S. M. F., 1978, tous droits réservés.

L'accès aux archives de la revue « Mémoires de la S. M. F. » (http://smf.emath.fr/Publications/Memoires/Presentation.html) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

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

BULLETIN

DE LA

SOCIÉTÉ MATHÉMATIQUE

DE FRANCE

PUBLIÉ

AVEC LE CONCOURS DU CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

SUPPLÉMENT au numéro de JUIN 1978

MÉMOIRE N° 57

Bull. Soc. math. France,
Mémoire 57, 1978, 152 p.

COURBES ELLIPTIQUES MUNIES D'UN SOUS-GROUPE $\mathbf{Z}/n\mathbf{Z} \times \mu_n$

(par Jacques VÉLU)

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

11, rue Pierre-et-Marie-Curie,
75231 PARIS CEDEX 05

Publication trimestrielle

SUPPLÉMENTS au Bulletin de la Société mathématique de France.

- Les *"Comptes rendus des séances"*, qui avaient paru annuellement de 1911 à 1938, ne sont plus disponibles séparément, mais sont tous incorporés, année par année, dans la réimpression du Bulletin de la Société mathématique de France, tomes 39 (1911) à 66 (1938), y compris, pour chacune des années 1911, 1921, 1922, 1923 et 1924 (séances du *"Cinquantenaire"* et séances ordinaires de 1924), les tables qui n'existaient pas à l'origine.

Les autres suppléments ci-après sont disponibles séparément :

- 1939. - Conférences de la Réunion internationale des mathématiciens [1937, Paris].

- *"Mémoires"* :

1. FORT (Jacques). - Contribution à l'étude des éléments tertiaires ... (Thèse).
2. GIRAUD (Jean). - Méthode de la descente.
3. GRILLET (P.-A.). - Homomorphismes principaux de tas et de groupoïdes (Thèse).
4. BERTRANDIAS (Françoise). - Ensembles remarquables d'adèles algébriques (Thèse).
5. BERTRANDIAS (Jean-Paul). - Espaces de fonctions bornées et continues ... (Thèse).
6. VO-KHAC Khoan. - Etude des fonctions quasi stationnaires ... (Thèse).
7. BERNAT (Pierre). - Sur le corps enveloppant d'une algèbre de Lie résoluble.
8. MALLIAVIN-BRAMERET (Marie-Paule). - Largeurs d'anneaux et de modules (Thèse).
9. RENAULT (Guy). - Etude des sous-modules compléments dans un module (Thèse).
10. ZINN-JUSTIN (Nicole). - Dérivations dans les corps et anneaux ... (Thèse).
11. BERTIN (Jean-Etienne). - Variété de Picard de type linéaire commutatif (Thèse).
12. AUBIN (Jean-Pierre). - Approximation des espaces de distributions ... (Thèse).
13. DEUTSCH (Nimet). - Interpolation dans les espaces vectoriels ... (Thèse).
14. ROBERT (Pierre). - Sur l'axiomatique des systèmes générateurs ... (Thèse).
15. FOUQUES (Alfred). - Systèmes de a-idéaux dans un demi-groupe ... (Thèse).
16. LEHMANN (Daniel). - Quelques propriétés des connexions induites ... (Thèse).
17. BRUTER (Claude P.). - Vue d'ensemble sur la théorie des matroïdes.
18. DIXMIER (Suzanne). - Sur les p-groupes ... (Thèse).
19. Contributions à la théorie des séries trigonométriques ...
20. KRÉE (Paul R.). - Distributions quasi homogènes et intégrales singulières.
21. de MATHAN (Bernard). - Approximations diophantiennes dans un corps local (Thèse).
22. CHADEYRAS (Marcel). - Essai d'une théorie nœthérienne homogène ... (Thèse).
23. KOSKAS (Maurice). - Structures algébriques multivoques. Applications (Thèse).
24. SPECTOR (René). - Sur la structure locale des groupes abéliens ... (Thèse).
25. Colloque de théorie des nombres [1969, Bordeaux].
26. MARTY (Robert). - Sous-groupes fonctoriels et relativisations (Thèse).
27. DHOMBRES (Jean G.). - Sur les opérateurs multiplicativement liés (Thèse).
28. GATESOUPE (Michel). - Sur les transformées de Fourier radiales (Thèse).
29. DELAROCHE (Claire). - Extensions des C^*-algèbres (Thèse).
30. RAÏS (Mustapha). - Distributions homogènes sur des espaces de matrices (Thèse).

31-32. Colloque d'analyse fonctionnelle [1971. Bordeaux].

33. Sur les groupes algébriques (ANANTHARAMAN et LUNA).

34. Contributions à l'analyse fonctionnelle (BONNARD, BOLLEY et CAMUS).

35. Contributions au calcul des probabilités (CONZE, REINHARD, BECKER, JACOD et DANG NGOC NGHIEM).

36. ROBERT (Gilles). - Unités elliptiques.

37. Journées arithmétiques [1973. Grenoble].

38. Journées de géométrie analytique [1972, Poitiers].

39-40. Table ronde d'analyse non archimédienne [1972, Paris].

41. RAYNAUD (Michèle). - Théorème de Lefschetz ... (Thèse).

42. FAKIR (Sabah). - Objets algébriquement clos ... (Thèse).

43. LIGOZAT (Gérard). - Courbes modulaires de genre 1 (Thèse).

44. ENOCK (Michel) et SCHWARTZ (Jean-Marie). - Une dualité dans les algèbres de von Neumann.

45. MOULIN (Hervé). - Prolongement des jeux à deux joueurs de somme nulle (Thèse).

46. Journées sur la géométrie de la dimension infinie ... [1975. Lyon].

47. PUIG (Luis). - Structure locale dans les groupes finis (Thèse).

48. Colloque sur les formes quadratiques [1975. Montpellier].

49-50. Utilisation des calculateurs en mathématiques pures [1975. Limoges].

51-52. Contributions à l'étude des opérateurs elliptiques et hypoelliptiques (B. HELFFER, G. MÉTIVIER).

53. KANTOR (Jean-Michel). - Formes ... ; HENDRIKS (Harris). - Obstruction ...

54. Fonctions harmoniques et théorèmes limites ... (A. RAUGI, J. ROSENBERG).

55-56. SOTO ANDRADE (Jorge). - Représentations de certains groupes symplectiques finis (Thèse).

57. VÉLU (Jacques). - Courbes elliptiques ... (Thèse).

© Tous droits réservés
Société mathématique de France.

Bull. Soc. math. France
Mémoire 57, 1978, p. 5-152.

COURBES ELLIPTIQUES

MUNIES D'UN SOUS-GROUPE $\mathbb{Z}/n\mathbb{Z} \times \mu_n$

par Jacques VÉLU (*)

TABLE DES MATIÈRES

Table des matières. 5

Introduction. 6

Première Partie.

Chapitre 1 : Le symbole de Weil. 10
Chapitre 2 : Les groupes $G(\delta)$ et les algèbres $L^*(\delta)$. 21
Chapitre 3 : Le plongement projectif d'une courbe elliptique associé à un sous-groupe cyclique. 34
Chapitre 4 : Les fonctions X_a et leurs relations. 43
Chapitre 5 : Etude du plongement de E dans $\mathbb{P}^{n-1}$ associé à une structure de niveau n. 56

Deuxième Partie.

Chapitre 6 : Le schéma $\mathcal{C}$. 73
Chapitre 7 : Le schéma $\mathcal{V}$. 91
Chapitre 8 : Les fibres singulières de $\mathcal{V}$. 101
Chapitre 9 : Quotient de $\mathcal{W}$ par μ_n. 111
Chapitre 10 : Conclusion. 137

Appendice : $H^2(\mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_r\mathbb{Z}, k^\times)$ avec action triviale. 146

Références. 152

(*) Thèse Sc. math. Univ. Paris-Sud, 1977.

INTRODUCTION

Le but de cette thèse est de construire pour tout nombre premier $n \geq 5$ un couple de schémas $(\mathcal{A}, \mathcal{V})$ au-dessus de $\mathbb{Z}[1/n]$ munis d'un morphisme $\mathcal{V} \xrightarrow{p} \mathcal{A}$ qui possède les propriétés suivantes.

i) $\mathcal{A}$ est une courbe projective lisse au-dessus de $\mathbb{Z}[1/n]$.

ii) $\mathcal{V}$ est une courbe elliptique généralisée au-dessus de $\mathcal{A}$ au sens de [De-Ra]. Plus précisément,

a) p est propre et plat, de présentation finie, de dimension relative 1,

b) les fibres géométriques sont soit des courbes propres lisses et connexes de genre 1, soit des polygones de Néron à n côtés (des n-gones). Nous notons $\tilde{\mathcal{V}}$ l'ouvert de lissité de p.

c) il existe un morphisme

$$+ : \tilde{\mathcal{V}} \underset{\mathcal{A}}{\times} \mathcal{V} \to \mathcal{V}$$

dont la restriction à $\tilde{\mathcal{V}}$ en fait un schéma en groupes commutatifs et qui définit une action du schéma en groupes $\tilde{\mathcal{V}}$ sur $\mathcal{V}$. De plus, les translations opèrent par rotation sur les composantes des fibres géométriques singulières de $\mathcal{V}$.

iii) Il existe un isomorphisme s entre le noyau $\mathcal{V}_n$ de la multiplication par n dans $\tilde{\mathcal{V}}$ et le $\mathbb{Z}[1/n]$-schéma $\mathcal{A} \times \mathbb{Z}/n\mathbb{Z} \times \mu_n$ et cet isomorphisme conserve la "forme de Weil".

iv) Si (S, E, λ) désigne une courbe elliptique généralisée au-dessus d'une base S sur $\mathbb{Z}[1/n]$ possédant les propriétés a) b) c) ci-dessus et si λ est un isomorphisme entre E_n et $S \times \mathbb{Z}/n\mathbb{Z} \times \mu_n$ conservant la "forme de Weil" il existe un unique couple de morphismes rendant cartésien le diagramme

$$\begin{array}{ccc} E & \longrightarrow & \mathcal{V} \\ \downarrow & & \downarrow \\ S & \longrightarrow & \mathcal{A} \end{array}$$

compatible avec les isomorphismes λ et s. En d'autres termes le triplet

$(\mathcal{A}, \mathcal{V}, s)$ est universel pour les propriétés énumérées plus haut.

Le schéma $\mathcal{A}$ est un sous-schéma fermé de $\mathbf{P}^{n-1}$ alors que le schéma $\mathcal{V}$ est un sous-schéma fermé de $\mathcal{A} \times \mathbf{P}^{n-1}$. Ils sont définis par des équations (quartiques pour $\mathcal{A}$, quadratiques pour $\mathcal{V}$). A titre d'exemple, les équations sont les suivantes quand n = 7. (Les points de $\mathcal{A}$ (resp. $\mathcal{V}$) ont des coordonnées projectives a(i) (resp. X(i)) indexées par $\mathbf{Z}/n\mathbf{Z}$).

Equations de $\mathcal{V}$

$-a(1)a(3)\,X(0)^2 + a(2)^2\,X(1)X(-1) - a(1)^2X(2)X(-2) = 0$

$a(2)a(1)X(0)^2 + a(3)^2\,X(2)X(-2) - a(2)^2X(3)X(-3) = 0$

$-a(3)a(2)X(0)^2 + a(1)^2\,X(3)X(-3) - a(3)^2X(1)X(-1) = 0$

$a(1)a(2)X(1)X(-1) - a(2)a(3)X(2)X(-2) - a(1)a(3)X(3)X(-3) = 0$

$-a(1)a(3)\,X(1)^2 + a(2)^2\,X(2)\,X(0) - a(1)^2\,X(3)\,X(-1) = 0$

$a(2)\,a(1)\,X(1)^2 + a(3)^2\,X(3)\,X(-1) - a(2)^2\,X(-3)X(-2) = 0$

$-a(3)a(2)X(1)^2 + a(1)^2X(-3)X(-2) - a(3)^2\,X(2)\,X(0) = 0$

$a(1)a(2)X(2)X(0) - a(2)a(3)\,X(3)X(-1) - a(1)a(3)X(-3)X(-2) = 0$

$-a(1)a(3)X(2)^2 + a(2)^2\,X(3)X(1) - a(1)^2X(-3)X(0) = 0$

$a(2)a(1)\,X(2)^2 + a(3)^2\,X(-3)X(0) - a(2)^2X(-2)X(-1) = 0$

$-a(3)a(2)\,X(2)^2 + a(1)^2\,X(-2)X(-1) - a(3)^2\,X(3)\,X(1) = 0$

$a(1)a(2)\,X(3)X(1) - a(2)a(3)\,X(-3)X(0) - a(1)a(3)X(-2)X(-1) = 0$

$-a(1)a(3)X(3)^2 + a(2)^2X(-3)X(2) - a(1)^2X(-2)X(1) = 0$

$a(2)a(1)X(3)^2 + a(3)^2X(-2)X(1) - a(2)^2\,X(-1)\,X(0) = 0$

$-a(3)a(2)\,X(3)^2 + a(1)^2\,X(-1)X(0) - a(3)^2\,X(-3)\,X(2) = 0$

$a(1)a(2)X(-3)X(2) - a(2)a(3)X(-2)X(1) - a(1)a(3)X(-1)X(0) = 0$

$$-a(1)a(3)X(-3)^2 + a(2)^2X(-2)X(3) - a(1)^2X(-1)X(2) = 0$$

$$a(2)a(1)\,X(-3)^2 + a(3)^2\,X(-1)X(2) - a(2)^2\,X(0)X(1) = 0$$

$$-a(3)a(2)\,X(-3)^2 + a(1)^2\,X(0)X(1) - a(3)^2\,X(-2)\,X(3) = 0$$

$$a(1)a(2)\,X(-2)X(3) - a(2)a(3)X(-1)X(2) - a(1)a(3)X(0)X(1) = 0$$

$$-a(1)a(3)X(-2)^2 + a(2)^2X(-1)X(-3) - a(1)^2X(0)\,X(3) = 0$$

$$a(2)\,a(1)\,X(-2)^2 + a(3)^2\,X(0)\,X(+3) - a(2)^2\,X(1)\,X(2) = 0$$

$$-a(3)a(2)X(-2)^2 + a(1)^2\,X(1)\,X(2) - a(3)^2\,X(-1)\,X(-3) = 0$$

$$a(1)a(2)X(-1)X(-3) - a(2)a(3)\,X(0)X(3) - a(1)a(3)X(1)X(2) = 0$$

$$-a(1)a(3)X(-1)^2 + a(2)^2\,X(0)X(-2) - a(1)^2\,X(1)X(-3) = 0$$

$$a(2)a(1)\,X(-1)^2 + a(3)^2\,X(1)\,X(-3) - a(2)^2\,X(2)X(3) = 0$$

$$-a(3)a(2)\,X(-1)^2 + a(1)^2\,X(2)X(3) - a(3)^2\,X(0)\,X(-2) = 0$$

$$a(1)a(2)\,X(0)\,X(-2) - a(2)a(3)\,X(1)\,X(-3) - a(1)a(3)\,X(2)X(3) = 0$$

Equations de $\mathcal{C}$

$$a(0) = 0$$
$$a(1) + a(-1) = 0$$
$$a(2) + a(-2) = 0$$
$$a(3) + a(-3) = 0$$

$$a(1)^3a(2) + a(2)^3a(-3) + a(-3)^3a(1) = 0\ .$$

On reconnaît dans cette dernière équation la célèbre "quartique de Klein" dont l'ensemble des points sur $\mathbb{C}$ n'est autre que $\overline{\mathcal{K}/\Gamma(7)}$, le complété du quotient du 1/2-plan de Poincaré $\mathcal{K}$ par le groupe

$$\Gamma(7) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) \;\middle|\; \begin{matrix} a \equiv d \equiv 1 \ (7) \\ b \equiv c \equiv 0 \ (7) \end{matrix} \right\}\ .$$

Dans ce travail le cas n = 3 a été exclu. Il est particulier et d'ailleurs bien connu. Il conduit aux mêmes résultats (construction des schémas $\mathcal{V}$ et $\mathcal{A}$ ayant les propriétés énoncées ci-dessus) mais $\mathcal{V}$ n'est plus intersection de quadriques, c'est la cubique d'équation

$$\lambda(X(0)^3 + X(1)^3 + X(2)^3 - 3X(0)X(1)X(2)) - \mu X(0)\,X(1)\,X(2) = 0$$

parfois appelée "cubique de Hesse", tandis que $\mathcal{A}$ est la droite projective $\mathbf{P}^1[1/3]$ paramétrée par λ et μ.

A noter que les inverses des coefficients a(i) ($i \neq 0$) intervenant ci-dessus sont des formes modulaires de poids 1 pour le groupe $\Gamma(n)$. Nous nous réservons de revenir plus tard sur leurs propriétés et sur les relations qui les lient.

Nous comptons revenir aussi sur le lien découvert vers 1910 par Hurwitz entre les courbes modulaires X(n) et la "courbe de Fermat"

$$X^n + Y^n + Z^n = 0 ,$$

sujet que nous avons déjà esquissé dans [Vé].

Cette thèse a été tapée au Centre de Mathématiques de l'Ecole Polytechnique, Equipe de Recherche Associée au C.N.R.S. No 169.

PREMIERE PARTIE

Dans toute cette partie k désigne un corps, k_s une clôture séparable de k et $\Gamma = Gal(k_s/k)$. Nous considérons une courbe elliptique E définie sur k et si N est un entier inversible dans k nous notons

$$E_N = \{P \in E(k_s) \mid N.P = 0\}.$$

CHAPITRE 1

Le symbole de Weil

Le but de ce chapitre est d'introduire les notations, de rappeler la définition du symbole de Weil et de donner quelques formules utiles par la suite.

1.1 Sous-groupes finis de $E(k_s)$

Soit G un sous-groupe fini de $E(k_s)$. Dans tout ce qui suit nous notons N son cardinal que nous supposons inversible dans k. Nous avons $G \subset E_N$ et nous posons $G' = E_N/G$.

Proposition 1.1 : Il existe deux entiers $n \geq n' \geq 1$ uniquement déterminés avec $n' \mid n$ tels que G et G' soient isomorphes à $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n'\mathbb{Z})$.

Preuve : Soit $n = \prod_i p_i^{\alpha_i}$ l'annulateur de G. Alors, E_n est isomorphe à $\prod_i (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^2$ et il existe des entiers β_i avec $0 \leq \beta_i \leq \alpha_i$ tels que G soit isomorphe à $\prod_i (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}) \times (\mathbb{Z}/p_i^{\beta_i}\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n'\mathbb{Z})$ où $n' = \prod_i p_i^{\beta_i}$ $= N/n$. De même, G' est isomorphe à $(\mathbb{Z}/(N/n)\mathbb{Z}) \times (\mathbb{Z}/(N/n')\mathbb{Z}) =$ $(\mathbb{Z}/n'\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ et la proposition est démontrée.

Dans tout ce qui suit, les nombres n et n' attachés à un groupe G auront le sens qui leur est donné dans la proposition 1.1.

Remarques :

i) G cyclique équivaut à $n' = 1$.

ii) $G = E_n$ équivaut à $n' = n$.

1.2 G-modules

A la courbe elliptique E sont associés les groupes abéliens suivants :

- $K_k(E)^\times$, le groupe multiplicatif du corps des k-fonctions sur E ,
- $E(k)$, le groupe des k-points de E,
- $Div_k(E)$, le groupe des k-diviseurs de E, c'est le groupe des combinaisons $\mathbb{Z}$-linéaires formelles $\delta = \sum_{P \in E(k_s)} n_P\{P\}$ telles que les n_P soient nuls sauf un nombre fini d'entre eux et telles que $n_P = n_{\sigma P}$ pour tout $P \in E(k_s)$ et tout $\sigma \in \Gamma = Gal(k_s/k)$. En d'autres termes,

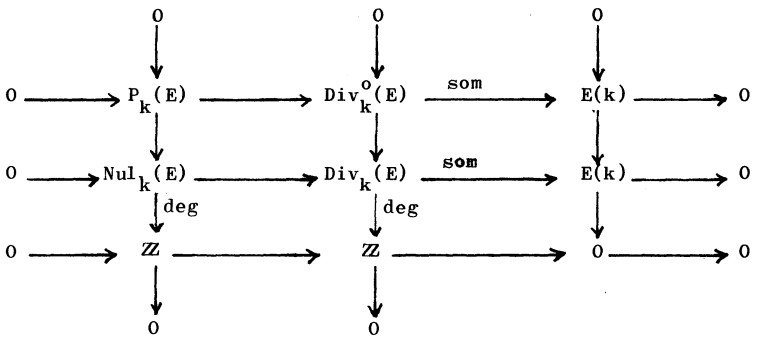
$$Div_k(E) = \mathbb{Z}\left[E(k_s)\right]^\Gamma.$$

- $Div_k^o(E)$, le noyau de l'homomorphisme surjectif deg : $Div_k(E) \to \mathbb{Z}$ défini par $deg(\sum_P n_P\{P\}) = \sum_P n_P$,

$Nul_k(E)$, le noyau de l'homomorphisme surjectif som : $Div_k(E) \to E(k)$ défini par $som(\sum_P n_P\{P\}) = \sum_P n_P.P$

- $P_k(E) = Div_k^o(E) \cap Nul_k(E)$.

Ces différents groupes sont liés par le diagramme commutatif exact



Il existe de plus un homomorphisme div : $K_k(E)^\times \xrightarrow{\text{div}} P_k(E)$, qui associe à toute fonction son diviseur .
Rappelons [ ] .

Théorème d'Abel : La suite

$$0 \longrightarrow k^\times \longrightarrow K_k(E)^\times \xrightarrow{\text{div}} P_k(E) \longrightarrow 0$$

est exacte.

Nous supposons jusqu'au paragraphe 1.4, $G \subset E(k)$. Nous faisons opérer G sur les groupes précédemment définis de la façon suivante :

- trivialement sur $k^\times$, $\mathbb{Z}$ et $E(k)$,
- par translation sur $K_k(E)$; plus précisément, si $f \in K_k(E)$ et si $g \in G$, on pose ${}^g f(x) = f(x-g)$ en notant x un point générique de E,
- par translation sur $\text{Div}_k(E)$; si $\delta = \sum_P n_P\{P\}$ et si $g \in G$, on pose ${}^g\delta = \sum_P n_P\{P+g\}$.

Comme $\deg({}^g\delta) = \deg(\delta)$ et $\text{som}({}^g\delta) = \text{som}(\delta) + (\deg\delta).g$, le groupe G opère aussi sur $\text{Div}_k^o(E)$ et $P_k(E)$ et il est clair que les suites

(1.1)

$$0 \longrightarrow \text{Div}_k^o(E) \longrightarrow \text{Div}_k(E) \xrightarrow{\deg} \mathbb{Z} \longrightarrow 0$$

$$0 \longrightarrow P_k(E) \longrightarrow \text{Div}_k^o(E) \xrightarrow{\text{som}} E(k) \longrightarrow 0$$

$$0 \longrightarrow k^\times \longrightarrow K_k(E)^\times \xrightarrow{\text{div}} P_k(E) \longrightarrow 0$$

sont des suites exactes de G-modules. Nous étudions au paragraphe 1.4 les suites de cohomologie qui s'en déduisent.

1.3 Isogénie de noyau G

Nous notons $E' = E/G$ la courbe isogène à E, λ l'isogénie $E \to E'$ et λ' l'isogénie duale $E' \to E$. Le noyau de λ' est $G' = E_N/G = \lambda(G)$. Nous faisons les identifications suivantes :

$K_k(E')$ avec $K_k(E)^G$, le sous-corps de $K_k(E)$ formé des fonctions invariantes par translation par les éléments de G. L'extension $K_k(E)$ de $K_k(E')$ est galoisienne et G est son groupe de Galois.

$\text{Div}_k(E')$ avec $\text{Div}_k(E)^G$, le sous-groupe de $\text{Div}_k(E)$ formé des diviseurs invariants par tanslation par les éléments de G ; si $\delta' \in \text{Div}_k(E)^G$, alors

$$\deg_E(\delta') = N\deg_{E'}(\delta')$$

$$som_E(\delta') = \lambda'(som_{E'}(\delta'))$$

$P_k(E')$ est un sous-groupe de $P_k(E)^G$, c'est l'image de $K_k(E)^{\times G}$ par l'homomorphisme div.

1.4 Suites de cohomologie

Dans ce paragraphe, nous étudions les suites de cohomologie qui se déduisent de (1.1)

Suite (A)

$$0 \longrightarrow Div_k^o(E)^G \longrightarrow Div_k(E)^G \xrightarrow{\deg} \mathbb{Z} \longrightarrow H^1(Div_k^o(E)) \longrightarrow H^1(Div_k(E))$$

Théorème 1.2 : Le groupe $H^1(Div_k(E))$ est nul.

Preuve : La structure de G-module de $Div_k(E)$ permet d'identifier $H^1(Div_k(E))$ avec $H^1(G, \mathbb{Z}[E(k_s)]^\Gamma)$, l'action de G sur $E(k_s)$ étant donnée par $P \xmapsto{g} P+g$. Cette action s'étend en une action de G sur l'ensemble quotient $A = E(k_s)/\Gamma$ puisque Γ opère trivialement sur G. Si H_r désigne le stabilisateur d'un point quelconque de l'orbite $r \in A/G$, nous avons $H^1(G,\mathbb{Z}[E(k_s)]^\Gamma) = \bigoplus_{r \in A/G} H^1(G,\mathbb{Z}[G/H_r])$; mais, $H^1(G,\mathbb{Z}[G/H_r]) = \mathrm{Hom}(H_r,\mathbb{Z})$ d'après le lemme de Shapiro et comme G est un groupe fini, nous avons toujours $\mathrm{Hom}(H_r,\mathbb{Z}) = 0$, ce qui prouve le théorème.

Corollaire 1.3 : 1) Si d est un 1-cocycle à valeurs dans $Div_k^o(E)$, il existe δ dans $Div_k(E)$ tel que $d_g = {}^g\delta - \delta$ pour tout g dans G ;

2) L'application $d \to \deg(\delta) \pmod N$ est un isomorphisme entre $H^1(Div_k^o(E))$ et $\mathbb{Z}/N\mathbb{Z}$.

Preuve : La première affirmation résulte du théorème 1.2. Pour la seconde, nous avons $\deg(Div_k(E)^G) = N\mathbb{Z}$ ce qui, dans la suite exacte A, donne un isomorphisme $0 \longrightarrow \mathbb{Z}/N\mathbb{Z} \longrightarrow H^1(Div_k^o(E)) \longrightarrow 0$ qu'il suffit d'expliciter pour obtenir l'affirmation 2.

Suite (B)

$$0 \longrightarrow P_k(E)^G \longrightarrow Div_k^o(E)^G \xrightarrow{som} E(k) \longrightarrow H^1(P_k(E)) \longrightarrow H^1(Div_k^o(E)) \xrightarrow{som} Hom(G,E(k))$$

Lemme 1.4 : Le groupe $som(H^1(Div_k^o(E)))$ est le sous-groupe de $Hom(G,E(k))$ formé des homothéties de G dans G. Il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Preuve : Comme G est isomorphe à $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}$, avec $n' \mid n$, le groupe des homothéthies de G dans G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Soit $d \in Z^1(Div_k^o(E))$. D'après le corollaire (1.3), il existe δ dans $Div_k(E)$ tel que $d_g = {}^g\delta - \delta$. Alors, $som(d_g) = (\deg \delta)g$ et $som(\delta)$ est l'homothétie de rapport $\deg \delta$. Réciproquement, prenons s dans $\mathbb{Z}$ et δ dans $Div_k(E)$ de degré s, $g \longrightarrow d_g = {}^g\delta - \delta$ est un 1-cocycle et $som(\delta)$ est l'homothétie de rapport s ce qui démontre le lemme.

Théorème 1.5 : Soit $d \in Z^1(P_k(E))$.

1) Il existe $\delta \in Div_k(E)$ avec $\deg(\delta) \equiv 0 \pmod n$ tel que $d_g = {}^g\delta - \delta$,

2) Posons $\sigma(G) = \sum_{g \in G} g$. Alors les applications

$$d \longmapsto (som\,\delta + \frac{\deg \delta}{n}\,\sigma(G)) \in E(k)/\lambda'E'(k)$$

$$d \longmapsto (\frac{\deg \delta}{n}) \in \mathbb{Z}/n'\mathbb{Z}$$

définissent un isomorphisme entre $H^1(P_k(E))$ et $E(k)/\lambda'(E'(k)) \oplus \mathbb{Z}/n'\mathbb{Z}$

Preuve : L'assertion 1 résulte du théorème 1.2 et du fait que $som({}^g\delta - \delta) = (\deg \delta).g$. Avec les identifications du paragraphe 1.3, nous avons $Div_k^o(E)^G = Div_k^o(E')$ et $som(Div_k(E)^G) = \lambda'(E'(k))$. D'après le lemme 1.4 et le corollaire 1.3, l'image de $H^1(P_k(E))$ dans $H^1(Div_k(E))$ est un groupe cyclique d'ordre $N/n = n'$. Nous tirons donc de la suite (B) la suite exacte

$$0 \longrightarrow E(k)/\lambda'E'(k) \xrightarrow{u} H^1(P_k(E)) \xrightarrow{v} \mathbb{Z}/n'\mathbb{Z} \longrightarrow 0$$

où l'homomorphisme u associe au point P de E(k) la classe de cohomologie contenant le 1-cocycle $g \mapsto \{P+g\} - \{g\} - \{P\} + \{O\}$ et où l'homomorphisme v associe au 1-cocycle d la classe de $\frac{\deg(\delta)}{n}$ modulo n'. Pour montrer que cette suite exacte est scindée, il faut trouver un

relèvement de v, c'est-à-dire trouver un élément de $H^1(P_k(E))$ d'ordre n' dont l'image par v soit 1. Désignons par ε le 1-cocycle $g \longmapsto \varepsilon_g = n\{g\} - n\{0\}$ et par $\bar{\varepsilon}$ sa classe de cohomologie . Nous avons $v(\bar{\varepsilon}) = 1$, par conséquent $\bar{\varepsilon}$ engendre un groupe d'ordre divisible par n'. Calculons $n'\bar{\varepsilon}$. Nous avons

$$n'\varepsilon_g = {}^g\delta - \delta - \{\sigma(G) + g\} + \{\sigma(G)\} + \{g\} - \{0\}$$

avec

$$\delta = (N-1)\{0\} - \sum_{g \in G} \{g\} + \{\sigma(G)\}$$

dans $P_k(E)$, ce qui montre que

$$n'\bar{\varepsilon} = u(-\sigma(G)) . \tag{1.2}$$

Remarquons que $\sigma(G)$ est un élément de G annulé par 2 qui diffère de 0 et seulement si n et n' sont de parités différentes ce qui implique que n est pair et n' impair.
Si $\sigma(G) \in \lambda'E'(k)$, l'équation (1.2) prouve que $\bar{\varepsilon}$ est d'ordre n' et nous avons le relèvement cherché. Par contre, si $\sigma(G) \notin \lambda'E'(k)$, cette equation prouve que $\bar{\varepsilon}$ est d'ordre 2n'. Mais ceci ne peut se produire que si n' est impair. Alors, la classe de cohomologie $(n' + 1)\bar{\varepsilon}$ est d'ordre n' et son image par v est 1 ; c'est donc elle qui nous permet dans tous les cas de construire un relèvement de v.
Pour terminer la démonstration du théorème, il reste à expliciter la projection de $H^1(P_k(E))$ sur $E(k)/\lambda'E'(k)$ associée au relèvement de v. Soit d un 1-cocycle et d sa classe de cohomologie. Il existe δ dans $Div_k(E)$ tel que $d_g = {}^g\delta - \delta$ ce que nous récrivons

$$d_g = {}^g\delta' - \delta' + \{som(\delta) + g\} - \{g\} - \{som(\delta)\} + \{0\} + \frac{deg(\delta)}{n}\varepsilon_g$$

avec

$$\delta' = \delta - \{som(\delta)\} - (deg(\delta) - 1)\{0\} \text{ dans } P_k(E).$$

Ceci montre que $\bar{d} = u(som(\delta)) + \frac{deg(\delta)}{n}\bar{\varepsilon}$ et comme $\bar{\varepsilon} = (n' + 1)\bar{\varepsilon} + u(\sigma(G))$ d'après l'équation (1.2), nous obtenons

$$\bar{d} = u(som(\delta) + \frac{deg(\delta)}{n}\sigma(G)) + \frac{deg(\delta)}{n}(n'+1)\bar{\varepsilon}$$

ce qui donne les projections de $H^1(P_k(E))$ sur ses facteurs.
Il faut noter que parmi ces facteurs l'un varie avec k alors que le second est constant.

Remarques : i) Le facteur de $H^1(P_k(E))$ isomorphe à $E(k)/\lambda'E'(k)$ est représenté par les cocycles de la forme $g \mapsto {}^g\delta - \delta$ avec $\delta = \{P\} - \{0\}$ et $P \in E(k)$.

ii) Si n' est impair et si C est un sous-groupe cyclique d'ordre n de G, le cocycle $g \mapsto \sum_{r \in C} \{r+g\} - \{r\}$ engendre le facteur de $H^1(P_k(E))$ isomorphe à $Z/n'Z$.

Suite (C)

$$0 \to k^\times \to K_k(E)^{\times G} \xrightarrow{div} P_k(E)^G \longrightarrow Hom(G,k^\times) \to H^1(K_k(E)^\times) \to H^1(P_k(E)) \to H^2(k^\times)$$

Théorème 1.6 : Le groupe $H^1(K_k(E)^\times)$ est nul.

En effet, c'est le "théorème 90 de Hilbert" compte-tenu du fait que $G = Gal(K_k(E'))$. Nous en déduisons immédiatement

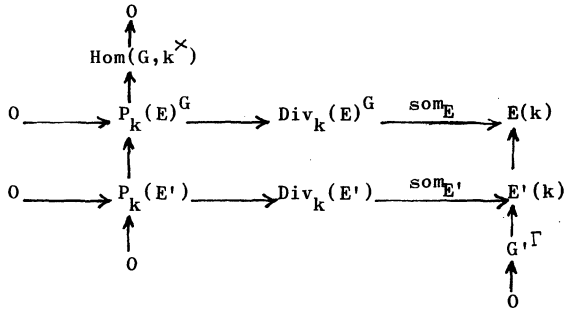
Corollaire 1.7 : La suite

$$0 \longrightarrow P_k(E') \longrightarrow P_k(E)^G \longrightarrow Hom(G,k^\times) \longrightarrow 0$$

est exacte et l'opérateur cobord $H^1(P_k(E)) \longrightarrow H^2(k^\times)$ est injectif.

Théorème 1.8 : Le groupe G'^Γ des points de G' contenus dans E'(k) et $Hom(G,k^\times)$ sont canoniquement isomorphes.

Preuve : Avec les identifications du paragraphe 1.3 et le résultat du corollaire 1.7, nous avons le diagramme commutatif exact suivant



et un tel diagramme définit de façon canonique un isomorphisme entre G'^{Γ} et $\mathrm{Hom}(G,k^{\times})$.

Corollaire 1.9 : La plus petite extension de k sur laquelle tous les points de G' sont rationnels est obtenue en adjoignant à k le groupe μ_n des racines n-èmes de 1.

Preuve : Nous avons $\mathrm{Hom}(G,k^{\times})$ isomorphe à G'^{Γ}, contenu dans G'. Si k contient μ_n, le groupe $\mathrm{Hom}(G,k^{\times})$ a le même cardinal que G et G' donc $G'^{\Gamma} = G'$. Réciproquement, si $G'^{\Gamma} = G'$ le groupe $\mathrm{Hom}(G,k^{\times})$ a N éléments et $k^{\times}$ contient μ_n.

1.5 La forme bilinéaire e_G et le symbole de Weil

Notons Ψ l'isomorphisme canonique entre G' et $\mathrm{Hom}(G,k_s^{\times}) = \mathrm{Hom}(G,\mu_n)$ donné par le théorème 1.8 et posons

$$e_G(g',g) = \Psi_{g'}(g)$$

pour tous $g' \in G'$ et $g \in G$. Alors e_G est une forme bilinéaire non dégénérée de $G' \times G$ dans μ_n .

Théorème 1.10 : Soit $\delta \in \mathrm{Div}^{o}_{k_s}(E)$ tel que $\lambda(\mathrm{som}(\delta)) = g'$ dans G', et soit f dans $K_{k_s}(E)^{\times}$ telle que

$$\mathrm{div}\ f = \sum_{r \in G} r_{\delta} .$$

Alors $f(x-g) = e_G(g',g)f(x)$ pour tout g dans G.

En effet, ce théorème ne fait qu'expliciter l'isomorphisme Ψ. Supposons la courbe E définie sur k et $G \not\subset E(k)$. Alors G, G' et e_G sont définis sur une extension algébrique de k et nous avons :

Théorème 1.11 : Soit $\sigma \in \Gamma$ alors $\sigma e_G(g',g) = e_{\sigma G}(\sigma g',\sigma g)$.

Preuve : Considérons une fonction f satisfaisant aux hypothèses du théorème 1.10. Alors, $\sigma e_G(g',g)\sigma f(x) = \sigma f(x-g) = (\sigma f)(x-\sigma g)$, et comme $\mathrm{div}\ \sigma f = {}^{\sigma g}(\sigma\delta)$ et $\sigma\lambda(\mathrm{som}(\sigma\delta)) = \sigma g'$, nous avons la relation cherchée

en appliquant le théorème 1.10 à la fonction σf.

Définition 1.12 : Si $G = E_n$, la suite exacte $0 \longrightarrow E_n \longrightarrow E_{n^2} \xrightarrow{n} E_n \longrightarrow 0$ définit un isomorphisme noté n^{-1} entre $G' = E_{n^2}/E_n$ et $G = E_n$. Le symbole de Weil est la forme bilinéaire non dégénérée $e_n : E_n \times E_n \longrightarrow \mu_n$ définie par

$$e_n(a,b) = e_{E_n}(n^{-1}a,b). \tag{1.3}$$

A l'aide de cette définition nous pouvons reformuler les théorèmes 1.10 et 1.11 dans le cas où $G = E_n$.

Théorème 1.13 : Soit a dans E_n.

1) Si δ dans $\mathrm{Div}^0_{k_s}(E)$ est tel que $n.\mathrm{som}(\delta) = a$, et si f dans $K_{k_s}(E)^\times$ est telle que $\mathrm{div}\, f = \sum_{g \in E_N} g\delta$, alors

$$f(x-b) = e_n(a,b)f(x)$$

pour tout b dans E_n.

2) Si $\sigma \in \Gamma$ nous avons

$$\sigma e_n(a,b) = e_n(\sigma a, \sigma b).$$

Théorème 1.14 : Pour tout g' dans E_N et pour tout g dans G nous avons

$$e_G(\lambda g', g) = e_N(g', g)$$

Preuve : Soit f dans $K_{k_s}(E)^\times$ telle que $\mathrm{div}\, f = \sum_{r \in G} (\{g' + r\} - \{r\})$. Soit g'' dans E_N tel que $Ng'' = g'$ et soit Ψ dans $K_{k_s}(E)^\times$ telle que $\mathrm{div}\, \Psi = \sum_{s \in E_N} (\{g'' + s\} - \{s\})$. D'après les théorèmes 1.10 et 1.13, nous avons $f(x-g) = e_G(\lambda g', g)f(x)$ et $\Psi(x-g) = e_N(g', g)\Psi(x)$. Mais, $\mathrm{div}(f/\Psi) = \sum_{r \in G} (\{g' + r\} - \{r\}) - \sum_{S \in E_N} (\{g'' + s\} - \{s\})$ et, si $a_1, \ldots, a_N$

désigne un système de représentants de G' dans E_N, nous pouvons écrire $\mathrm{div}(f/\Psi) = \sum_{r \in G} \left[\{g' + r\} - \{r\} - \sum_i \{g'' + a_i + r\} + \sum_i \{a_i + g\}\right]$ ce qui donne, en posant $\delta = \{g'\} - \{0\} - \sum_i \{g'' + a_i\} + \sum_i \{a_i\}$, la relation $\mathrm{div}(f/\Psi) = \sum_{r \in G} {}^r\delta$ qui montre, puisque $\delta \in P_{k_s}(E)$, que f/Ψ est dans $K_{k_s}(E)^{\times G}$ et que $e_N(g',g) = e_G(\lambda g', g)$.

Corollaire 1.15 : Soit $f \in K_{k_s}(E)^{\times}$ et soit $a \in E(k_s)$ tels que la fonction ${}^a f/f$ soit constante.
i) Si a est d'ordre infini, f est constante et ${}^a f/f = 1$.
ii) Si a est d'ordre fini, il est toujours possible de trouver un diviseur $\varepsilon \in \mathrm{Div}^o_{k_s}(E)$ et un groupe fini G d'ordre N tels que $\mathrm{div}\, f = \sum_{r \in G} {}^r\varepsilon$. De plus, pour une telle décomposition, $Na = N\mathrm{som}(\varepsilon) = 0$ et ${}^a f/f = e_N(\mathrm{som}(\varepsilon), a)$.

Preuve : L'affirmation i) résulte du fait que le support de div f est fini. Pour montrer ii), nous exhibons une décomposition de div f. En effet, si $\mathrm{div}\, f = \sum_{P \in E(k_s)} n_P\{P\}$, nous choisissons un point Q dans chaque orbite de $E(k_s)/C$ où C désigne le groupe cyclique engendré par a, et nous posons $\varepsilon = \sum_{Q \in E(k_s)/C} n_Q\{Q\}$. D'autre part, il est clair que pour une telle décomposition $\deg(\mathrm{div}\, f)) = N.\deg\varepsilon = 0$ et que $\mathrm{som}(\mathrm{div}\, f) = N.\mathrm{som}\,\varepsilon = 0$. Enfin, le théorème 1.10 montre que ${}^a f/f = e_G(\lambda(\mathrm{som}\,\varepsilon), a)$ où, comme toujours, λ désigne l'isogénie $E \to E/G$ et d'après le théorème 1.14 $e_G(\lambda(\mathrm{som}\,\varepsilon), a) = e_N(\mathrm{som}\,\varepsilon, a)$, ce qui prouve le corollaire.

Théorème 1.16 : La forme de Weil est alternée, de plus $e_G(g',g)e_{G'}(g,g') = 1$ pour tous g dans G et g' dans G', en identifiant G avec E'_N/G'.

Preuve : Soit a dans E_N. Il existe un groupe cyclique G d'ordre N contenant a et d'après le théorème 1.14, $e_N(a,a) = e_G(\lambda a, a) = e_G(0,a) = 1$; ce qui montre que la forme est alternée.
Soient g dans G, a dans $\frac{1}{N}$ G, g' dans G', b dans E_N, tels que $Na = g$ et $\lambda b = g'$. Considérons une fonction f ayant pour diviseur

$\sum_{r \in E_N} \{a+r\} - \{r\}$. Cette fonction est dans $K_{k_s}(E)^{\times G}$ car elle est égale au produit de toutes les translatées d'une même fonction par tous les éléments de G. C'est donc une fonction sur E' et son diviseur sur E' est de la forme $\sum_{r' \in G'} r'(\{\lambda a\} - \{\lambda 0\})$. Par conséquent nous avons $f(x-b) = e_{G'}(g,g')f(x)$. D'autre part nous avons aussi $f(x-b) = e_N(g,b)f(x)$ ce qui donne enfin $e_{G'}(g,g') = e_N(g,a) = e_N(a,g)^{-1} = e_G(g',g)^{-1}$ et la relation cherchée.

Théorème 1.17 : Si a et b sont dans E_{Nm} nous avons

$$e_{Nm}(a,b)^m = e_N(ma,mb).$$

Preuve : Soit δ dans $Div^o_{k_s}(E)$ avec $Nm.som(\delta) = a$. Si $div\, f = \sum_{r \in E_N} r\delta$, nous avons $f(x-b) = e_{Nm}(a,b)f(x)$ et $f(x-mb) = e_{Nm}(a,b)^m f(x)$. Désignons par (r_i) un système de représentants de E_{Nm}/E_N dans E_{Nm}. Nous pouvons écrire $div\, f = \sum_{s \in E_N} s\delta'$ avec $\delta' = \sum_i r_i(m\delta)$ ce qui donne $f(x-mb) = e_N(ma,mb)f(x)$ puisque δ' est dans $Div^o_{k_s}(E)$ et que $N.som(\delta') = ma$.

CHAPITRE 2

Les groupes G(δ) et les algèbres L*(δ).

Dans tout ce chapitre la lettre δ désigne un élément de $Div_k(E)$.

2.1 Extensions de groupes

Soit G un groupe, non nécessairement commutatif, dont la loi de composition est notée multiplicativement et soit

$$0 \longrightarrow A \longrightarrow B \xrightarrow{u} C \longrightarrow 0$$

une suite exacte de G-modules notés additivement.

A ces données sont associés une suite exacte de cohomologie et un opérateur cobord $\partial : H^1(C) \longrightarrow H^2(A)$. Plus précisément,

Lemme 2.1 : Soit $d \in Z^1(C)$. L'ensemble $F = \{(g,b) \in G \times B \mid u(b) = d(g)\}$ est un groupe pour la loi de composition

$$(g',b').(g,b) = (g'g, b' + {}^{g'}b).$$

De plus, F est une extension de A par G dont la classe dans $H^2(A)$ est le cobord de d.

Preuve : L'ensemble F n'est pas vide puisque l'application u est surjective. La loi de composition est interne car $u(b' + {}^{g'}b) = u(b') + {}^{g'}u(b) = d(g') + {}^{g'}d(g) = d(g'g)$ puisque d est un cocycle. Un calcul facile montre que F est un groupe pour cette loi. L'homomorphisme de F dans G défini par $(g,b) \mapsto g$ est surjectif car l'application u est surjective, et son noyau qui est formé des éléments (1,a) avec a dans A est isomorphe à A, donc F est une extension de A par G. Si s est un relèvement de G dans F, le 2-cocycle α associé à s est défini par

$s(g').s(g) = \alpha(g',g).s(g'g)$. Soit b_g tel que $s(g) = (g,b_g)$. Alors, $\alpha(g',g) = b_{g'} + {}^{g'}b_g - b_{g'g} = \partial\, d(g',g)$ ce qui termine la démonstration du lemme.

2.2 L'extension $G(\delta)$

Nous reprenons les notations du chapitre 1 pour appliquer le lemme 2.1 à un sous-groupe fini G de E(k) et à la suite exacte de G-modules

$$0 \longrightarrow k^{\times} \longrightarrow K_k(E)^{\times} \xrightarrow{\text{div}} P_k(E) \longrightarrow 0$$

Ici, la loi de G est notée additivement et celle de $B = K_k(E)^{\times}$ est notée multiplicativement ! Jusqu'à la fin de ce chapitre nous supposerons $\mu_n \subset k^{\times}$.

Définition 2.2 : Soit $\delta \in \text{Div}_k(E)$ tel que n divise $\deg \delta$. Le lemme 2.1 associe au cocycle $g \mapsto {}^g\delta - \delta$ une extenion de $k^{\times}$ par G que nous noterons $G(\delta)$.

En d'autres termes,

$$G(\delta) = \{(g,\varphi) \in G \times K_k(E)^{\times} \mid \text{div}\, \varphi = {}^g\delta - \delta\}$$

muni de la loi

$$(g,\varphi)(g',\varphi') = (g+g', \varphi.{}^g\varphi')$$

$G(\delta)$ est une extension centrale de $k^{\times}$ par G puisque G opère trivialement sur $k^{\times}$. Au chapitre 3 nous nous interesserons au cas où $\delta = \sum_{r \in C} \{r\}$ avec C un groupe cyclique d'ordre n impair et $G = E_n$. Auparavant, nous allons démontrer quelques propriétés des extensions $G(\delta)$ dans le cas général.

D'après le théorème A.4 de l'appendice, et comme nous avons supposé μ_n contenu dans $k^{\times}$, l'extension $G(\delta)$ est déterminée à isomorphisme près par la forme bilinéaire alternée $< , > : G \times G \to \mu_n$ et par l'application $v : G \to k^{\times}/k^{\times n}$ définis de la façon suivante. Si (g,φ) et

(g',φ') sont dans $G(\delta)$,

$$<g',g> = (g',\varphi').(g,\varphi).(g',\varphi')^{-1}.(g,\varphi)^{-1} = \frac{\varphi'.g'\varphi}{g_{\varphi'}.\varphi}$$

et $v(g)$ est l'image dans $k^\times/k^{\times n}$ de $s \in k^\times$ défini par $(g,\varphi)^n = (0,s)$. En fait, la connaissance de l'application v équivaut à celle de l'application $u : G \to k^{\times 1/n}/k^\times$ défini par

$$u(g)^n = v(g) \tag{2.1}$$

et ce sont les applications $<\ ,\ >$ et u que nous allons étudier maintenant.

Proposition 2.3 : Soient g et g' dans G, alors

$$<g,g'> = e_n(g',g)^{\frac{\deg\delta}{n}} \tag{2.2}$$

Preuve : Soit $\delta_o \in \mathrm{Div}^o_k(E)$ tel que $\delta = \delta_o + \{\mathrm{som}\,\delta\} - \{0\} + \deg\delta\,\{0\}$. Fixons $Q \in E(k_s)$ tel que $NQ = \mathrm{som}\,\delta$. Les diviseurs du membre de droite des équations (2.3) ci-dessous étant principaux, il existe des fonctions α, Ψ, w, w' dans $K_{k_s}(E)^\times$ telles que

$$\begin{aligned} \mathrm{div}\,\alpha &= \delta_o \\ \mathrm{div}\,\Psi &= \{\mathrm{som}\,\delta\} - \{0\} + \sum_{r\in G}(\{r\} - \{r+Q\}) \\ \mathrm{div}\,w &= n\{g\} - n\{0\} \\ \mathrm{div}\,w' &= n\{g'\} - n\{0\} \end{aligned} \tag{2.3}$$

Il existe alors deux constantes u et u' dans $k_s^\times$ telles que

$$\varphi = u\,\frac{g_\alpha}{\alpha}.\frac{g_\Psi}{\Psi}.w^{\frac{\deg\delta}{n}}$$

$$\varphi = u'\frac{g'\alpha}{\alpha}.\frac{g'\Psi}{\Psi}.w'^{\frac{\deg\delta}{n}}$$

ce qui donne $\frac{\varphi}{g\varphi}.\frac{g_{\varphi'}}{\varphi'} = \left(\frac{w}{g'w}.\frac{g_{w'}}{w'}\right)^{\frac{\deg\delta}{n}}$, et nous ramène à démontrer la proposition 2.3 dans le cas où $\delta = n\{0\}$. Soit C un sous-groupe de E_n, cyclique d'ordre n, contenant g et soit λ l'isogénie $E \to E/C$. D'après le théorème 1.13 nous avons $e_n(g',g) = e_C(\lambda g', g)$. Fixons $R \in E(k_s)$ tel que

$nR = \sigma(C)$ et fixons $f \in K_{k_s}(E)^\times$ telle que

$$\operatorname{div} f = \sum_{r \in C} (\{g'+R+r\}-\{R+r\}).$$

D'après le théorème 1.10, nous avons ${}^{g}f/f = e_C(\lambda g', g)$. Comme le diviseur $\sum_{r \in C}(\{0\} - \{R + r\})$ est principal, c'est le diviseur d'une fonction μ et la relation $\operatorname{div} f = \operatorname{div} w' + \sum_{r \in C}(\{0\} - \{R + r\}) - \sum_{r \in C}(\{g'\} - \{R + r + g'\})$ montre qu'il existe une constante $v \in k_s^\times$ telle que $f = v\, w' \frac{\mu}{{}^{g}\mu}$ d'où

$$e_n(g', g) = e_C(\lambda g', g) = \frac{g_{w'}}{w'} \frac{g_\mu\, g'_\mu}{\mu^{g+g'}\mu}. \tag{2.4}$$

Or $\operatorname{div} {}^{g}\mu/\mu = \operatorname{div} w$. Par conséquent il existe une constante v' telle que ${}^{g}\mu/\mu = v'w$ et en reportant dans (2.4) nous obtenons le résultat cherché.

Lemme 2.4 : Soit (g,φ) dans $G(\delta)$.

i) Il existe $\varepsilon \in \operatorname{Div}_{k_s}(E)$ et $u_\varepsilon \in k_s^\times$ tels que

a) $\delta - \varepsilon \in P_{k_s}(E)$

b) ${}^{g}\varepsilon = \varepsilon$

c) $\varphi = u_\varepsilon . {}^{g}R/R$ pour toute fonction R satisfaisant la condition $\operatorname{div} R = \delta - \varepsilon$.

ii) Si d désigne l'ordre de g, la constante u_ε est dans $k^{\times 1/d} \subset k^{\times 1/n}$

Si ε' est un autre diviseur satisfaisant les conditions a) et b), le rapport $u_{\varepsilon'}/u_\varepsilon$, est dans μ_d.

iii) L'application $g \mapsto u_\varepsilon \in k^{\times 1/n}/k^\times$ est l'application u définie par (2.1).

Preuve : i) Si $\deg \delta \neq 0$, nous désignons par C un groupe cyclique d'ordre n contenant g et par Q un point de $E(k_s)$ tel que

$$(\deg \delta).Q = \operatorname{som} \delta - \frac{(\deg \delta).\sigma(C)}{n}.$$

Alors, $\varepsilon = \frac{\deg \delta}{n} \sum_{r \in C} {}^{r}\{Q\}$ satisfait à a) et b). Si $\deg \delta = 0$, et si Q

est un point de $E(k_s)$ tel que $N.Q = \text{som}\ \delta$ le diviseur $\varepsilon = \sum_{r \in G} \{Q + r\} - \{r\}$ satisfait à a) et b). Pour toute fonction R telle que $\text{div}\ R = \delta - \varepsilon$, nous avons $\text{div}\ \varphi = \text{div}\ {}^{g}R/R$, par conséquent la constante u_ε existe et ne dépend évidemment pas de la normalisation de R.

ii) Comme $(g,\varphi)^d = u_\varepsilon^d.({}^{g}R/R).({}^{2g}R/{}^{g}R)\ldots({}^{R}/{}^{(d-1)g}R) = u_\varepsilon^d$,

nous avons $u_\varepsilon^d \in k^\times$ qui ne dépend pas du choix de ε.

iii) L'égalité $u_\varepsilon^n = (g,\varphi)^n$ montre que l'image de u_ε dans $k^{\times 1/n}/k^\times$ n'est autre que u(g).

La proposition 2 et le lemme 2 nous permettent de décrire l'extension $G(\delta)$. Nous allons le faire un peu plus explicitement et réinterpréter les constantes u_ε définies dans le lemme 2.4. D'après le théorème 1.5 le groupe $H^1(P_k(E))$ est somme directe de deux groupes, l'un isomorphe à $E(k)/\lambda'E'(k)$, l'autre à $\mathbb{Z}/n'\mathbb{Z}$. L'image du premier groupe correspond aux extensions $G(\delta)$ avec δ de la forme $\{P\} - \{O\}$ où $P \in E(k)$, l'image du second aux extensions $G(\ell\{O\})$ avec $\ell \equiv 0 \pmod n$. Nous allons traiter ces deux cas séparément.

2. Image de $E(k)/\lambda'E'(k)$ dans $H^2(k^\times)$.

Soit P dans E(k) et considérons $G(\{P\} - \{O\})$. D'après la proposition 2.3 c'est un groupe commutatif et sa structure en tant qu'extension de $k^\times$ par G est complètement déterminée par l'homomorphisme $u : G \to k^{\times 1/n}/k^\times$. Nous noterons u^P cet homomorphisme pour marquer sa dépendance de P.

Soient Ψ_1 l'isomorphisme $\text{Hom}(\Gamma,G') \to \text{Hom}(\Gamma,\text{Hom}(G,\mu_n))$ déduit de l'isomorphisme $G' \to \text{Hom}(G,\mu_n)$ donné par le théorème 1.8.

Ψ_2 l'isomorphisme canonique

$\text{Hom}(\Gamma,\text{Hom}(G,\mu_n)) \to \text{Hom}(G,\text{Hom}(\Gamma,\mu_n))$,

Ψ_3 l'isomorphisme $\text{Hom}(G,\text{Hom}(\Gamma,\mu_n)) \to \text{Hom}(G,k^{\times 1/n}/k^\times)$ déduit de l'isomorphisme $\text{Hom}(\Gamma,\mu_n) \to k^{\times 1/n}/k^\times$,

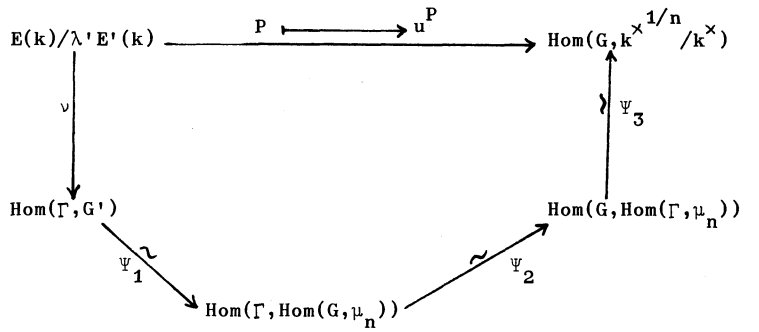
ν : $E(k)/\lambda'E'(k) \to \text{Hom}(\Gamma,G')$ l'injection déduite de l'opérateur cobord associé à la suite exacte de Γ-modules

$$0 \longrightarrow G' \longrightarrow E'(k_s) \xrightarrow{\lambda'} E(k_s) \longrightarrow 0 \quad ;$$

alors

Proposition 2.5 : L'application $P \mapsto u^P$ est un homomorphisme et c'est le composé $\Psi_3 \Psi_2 \Psi_1 \nu$.

En d'autres termes le diagramme suivant est commutatif.



Preuve : Nous reprenons la démonstration du lemme 2.4. Soient $Q \in E(k_s)$ et $R \in K_{k_s}(E)^\times$ tels que $N.Q = P$ et $\operatorname{div} R = \{P\} - \{0\} - \sum_{r \in G} \{Q+r\} - \{r\}$.

Si $(g,\varphi) \in G_P$, il existe une constante $u \in k_s^\times$ telle que $\varphi = u.{}^g R/R$. Cette constante dépend de g,φ et Q mais son image dans $k^{\times 1/n}/k^\times$ ne dépend pas de φ. Pour cette raison, nous la noterons $u(g,Q)$. Si Q' est un autre point tel que $N.Q' = P$, nous avons $u(g,Q)/u(g,Q') = e_N(Q-Q',g)$.
En effet, $\varphi = u(g,Q').{}^g R'/R' = u(g,Q).{}^g R/R$ et $u(g,Q')/u(g,Q) = {}^g(R/R')/(R'/R)$
Comme $\operatorname{div} R/R' = \sum_{r \in G} \{Q'+r\} - \{Q+r\}$, il suffit d'appliquer le corollaire 1.15 pour obtenir le résultat. Nous sommes maintenant en mesure de démontrer la proposition 2.5 .

a) A la suite exacte de Γ-modules $0 \to G' \to E'(k_s) \xrightarrow{\lambda'} E(k_s) \to 0$ est associée l'injection : $E(k)/\lambda'E'(k) \to \operatorname{Hom}(\Gamma,G')$. Si $\sigma \in \Gamma$, l'homomorphisme $\nu P \in \operatorname{Hom}(\Gamma,G')$ est donné par $\sigma \to {}^\sigma(\lambda Q) - (\lambda Q) = \lambda({}^\sigma Q - Q)$.

b) L'homomorphisme $\Psi_1 \nu P \in \operatorname{Hom}(\Gamma,\operatorname{Hom}(G,\mu_n))$ est donné par

$$\sigma \longmapsto (g \mapsto e_N({}^\sigma Q - Q, g)).$$

c) L'homomorphisme $\Psi_2 \Psi_1 \nu P \in \operatorname{Hom}(G,\operatorname{Hom}(\Gamma,\mu_n))$ est donné par

$$g \longmapsto (\sigma \mapsto c_N({}^\sigma Q - Q, g))$$

d) Les groupes $\operatorname{Hom}(\Gamma,\mu_n)$ et $k^{\times 1/n}/k^\times$ sont isomorphes. Comme

$c_N({}^\sigma Q - Q, g) = u(g, {}^\sigma Q)/u(g,Q) = {}^\sigma u(g,Q)/u(g,Q)$, l'image de l'homomorphisme $\sigma \to e_N({}^\sigma Q - Q, g)$ appartenant à $\mathrm{Hom}(\Gamma, \mu_n)$ dans $k^{\times 1/n}/k^\times$ est l'image de $u(g,Q)$ dans $k^{\times 1/n}/k^\times$.

e) Il en résulte que l'homomorphisme $\Psi_3\Psi_2\Psi_1 \nu P$ dans $\mathrm{Hom}(G, k^\times/k^\times)$ est donnée par $g \to u(g,Q)$ qui n'est autre que u_P

Remarque : L'accouplement $E(k)/\lambda'E'(k) \times G \longrightarrow k^{\times 1/n}/k^\times$ défini par $(P,g) \to u(g,Q)$ a été etudié par plusieurs auteurs [Ba], [Ro].

2.4 L'extension $E_n(n\{0\})$

Nous noterons dans ce paragraphe, pour simplifier, $E_n^\times = E_n(n\{0\})$, et nous allons étudier les applications $<\ ,\ >$ et u attachées à cette extension de $k^\times$ par E_n.

Proposition 2.6 :

i) Soient g et g' dans E_n. Alors $<g,g'> = e_n(g',g)$

ii) Soient g dans E_n, φ une fonction telle que $\mathrm{div}(\varphi) = n\{g\} - n\{0\}$, et a dans E_{2n} tel que $2a = g$. Alors u(g) est l'image dans $k^{\times 1/n}/k^\times$ de $\varphi(a)$.

iii) L'homomorphisme u^2 est trivial et quand n est impair il en est de même de l'homomorphisme u.

Preuve : L'affirmation i) résulte immédiatement de la proposition 2.3. Avant de démontrer ii), remarquons qu'étant donnés (g,φ) dans E_n et a dans E_{2n} tels que $2a = g$, le point a n'est pas dans le support de $\mathrm{div}(\varphi)$ et que $\varphi(a)$ est toujours dans $k^\times$. Introduisons quelques notations. La lettre X désigne une fonction sur E n'ayant pour pôles qu'un pôle double au point 0. A cette fonction est associée une section (ensembliste) de $E^*_{2n} \to E_{2n}$ qui fait correspondre à tout $a \in E_{2n}$ la fonction Ψ_a sujette aux conditions

$$\mathrm{div}\,\Psi_a = 2n\{a\} - 2n\{0\}$$

$$\Psi_0 = 1$$

$$\Psi_a/X^n(0) = 1 \quad \text{pour} \quad a \neq 0.$$

On remarque immédiatement que

$$\Psi_{-a}(x) = \Psi_a(-x) \tag{2.5}$$

$$\Psi_a(x)\Psi_a(-x) = \left[X(x) - X(a)\right]^{2n} \text{ pour } a \neq 0 \tag{2.6}$$

$$\Psi_D(x) = \Psi_D(-x) = \left[X(x) - X(D)\right]^n \text{ pour } D \in E_2 - \{0\} \tag{2.7}$$

Lemme 2.7 :

i) Soient (g,φ) dans E_n^* et dans E_{2n} tels que $2a = g$. Si $a \neq 0$,

$$\frac{\varphi(a+x)}{\varphi(a)} = \frac{\varphi(a)}{\varphi(a-x)} = \frac{\Psi_a(x)}{\left[X(x) - X(a)\right]^n} \tag{2.8}$$

ii) Soient (g,φ) et (g',φ') dans E_n et soient a et a' dans E_{2n} tels que $2a = g$ et $2a' = g'$. Si $a \neq 0$, $a' \neq 0$, $a \neq \pm a'$,

$$\frac{\varphi(a+a')}{\varphi(a)} \cdot \frac{\varphi'(a')}{\varphi'(a'+a)} = (-1)^n e_{2n}(a',a) \tag{2.9}$$

iii) Soient (g,φ) dans E_n^* et a dans E_{2n} tels que $2a = g$. Si $a \neq 0$ et si $D \in E_2 - \{0\}$ est tel que $D \neq a$,

$$\varphi(a+D) = (-1)^n e_2(D,na)\varphi(a) \tag{2.10}$$

Preuve : L'affirmation i) s'obtient en comparant les diviseurs et les valeurs en 0 des membres de (2.8).

ii) Avec (2.8) le membre de gauche de (2.9) est égal à $(-1)^n \frac{\Psi_a(a')}{\Psi_{a'}(a)}$ qui, est aussi $(-1)^n \frac{\Psi_{-a}(-a')}{\Psi_{a'}(a)}$ par (2.6). Mais la proposition 2.3 montre que $\frac{\Psi_{-a}(-a')}{\Psi_{a'}(a)} = \frac{\Psi_{a'}(x)}{\Psi_{a'}(x+a)} \cdot \frac{\Psi_{-a}(x-a')}{\Psi_{-a}(x)} = e_{2n}(-a,a') = e_{2n}(a',a)$, ce qui donne (2.9).

iii) Si on écrit (2.9) avec $a' = D$ on obtient (2.10) après avoir remarqué que $e_{2n}(D,a) = e_2(D,na)$.

Lemme 2.8 : Soient (g,φ) dans E_n^* et a dans E_{2n} tels que $2a = g$. Si g est d'ordre $d > 1$,

$$u^d = (g,\varphi)^d = \begin{cases} (-1)^n \varphi(a)^d & \text{si } d.a = 0 \\ \varphi(a)^d & \text{si } d.a \neq 0 \end{cases} \tag{2.11}$$

Preuve : Nous avons $u^d = (g,\varphi)^d = \varphi.{}^{g}\varphi\ldots{}^{(d-1)g}\varphi$. Introduisons des fonctions $\varphi_o,\varphi_1,\ldots,\varphi_{d-1}$ sujettes aux conditions

$$\operatorname{div}\varphi_t = n\{tg\} - n\{0\}$$
$$\varphi_0 = 1$$
$$\varphi_1 = \varphi$$

Alors,

$$u^d = \frac{\varphi_1.{}^{g}\varphi_1}{\varphi_2}\ \frac{\varphi_2.{}^{2g}\varphi_1}{\varphi_3}\ \ldots\ldots\ \frac{\varphi_{d-1}.{}^{(d-1)g}\varphi_1}{\varphi_o} = \prod_{t=1}^{d-1} s_t$$

avec

$$s_t = \frac{\varphi_t.{}^{tg}\varphi_1}{\varphi_{t+1}}$$

que nous allons calculer.

Lemme 2.9

$$(2.12)\qquad s_t = \begin{cases} (-1)^n \dfrac{\varphi_1(a)\varphi_t(ka)}{\varphi_{t+1}((t+1)a)} & \text{si } t \not\equiv d-1 \pmod d \\ \dfrac{\varphi_1(a)\varphi_t(ta)}{\varphi_{t+1}((t+1)a)} & \text{si } t \equiv d-1 \pmod d \end{cases}$$

Preuve : Puisque $\varphi_o = 1$, nous avons $s_{d-1} = \dfrac{\varphi_{-1}(x)\varphi_1(x+g)}{\varphi_o(x)} = \varphi_{-1}(-a)\varphi_1(a)$.

Supposons donc $t \not\equiv d-1$. Deux cas sont à considérer.

1) $t = 1$.

Si $3a \neq 0$ nous avons $s_1 = \dfrac{\varphi_1(x)\varphi_1(x-g)}{\varphi_2(x)} = \dfrac{\varphi_1(a)\varphi_1(-a)}{\varphi_2(a)}$.

Or la relation (2.9) montre en prenant $a' = -g$ que

$$(-1)^n = \frac{\varphi_1(-a)\varphi_{-2}(-g)}{\varphi_1(a)\varphi_{-2}(-a)} = \frac{\varphi_1(-a).\varphi_2(g)}{\varphi_1(a)\ \varphi_2(a)} \text{ donc que } \frac{\varphi_1(a).\varphi_1(-a)}{\varphi_2(a)} = (-1)^n \frac{\varphi_1(a)^2}{\varphi_2(2a)} .$$

Si $3a = 3g = 0$ nous procédons directement en choisissant, ce qui est toujours possible, deux fonctions X et Y sur la courbe E n'ayant pour

pôles respectivement qu'un pôle double, triple, en 0, liées par une relation de la forme $Y^2 + a_1XY + a_3Y = X^3$ avec $a_1 \in k$, $a_3 \in k^\times$, $g = (0,0)$ et $\varphi = Y^{n/3}$. Alors, $\varphi_2 = \alpha(Y + a_1X + a_3)^{n/3}$ avec $\alpha \in k^\times$ et $2g = (0,-a_3)$. Comme $\varphi_1(-g) = (-a_3)^{n/3}$ nous avons $\dfrac{\varphi_1(x)\varphi_1(x-g)}{\varphi_2(x)} = \dfrac{(-a_3)^{n/3}}{\alpha} = (-1)^n \dfrac{\varphi_1(2g)^2}{\varphi_2(g)}$

Mais on peut vérifier en utilisant (2.10) que le nombre de droite de (2.11) ne dépend ni du choix de a, ni du choix de t dans sa classe de congruence modulo d. Par conséquent, en prenant a = 2g nous obtenons bien $s_1 = (-1)^n \dfrac{\varphi_1(a)}{\varphi_2(2a)}$.

2) $1 < t < d-1$

Alors $s_t = \dfrac{\varphi_t(x)\varphi_1(x-tg)}{\varphi_{t+1}(x)} = \dfrac{\varphi_t(ta+a)\varphi_1(a-ta)}{\varphi_{t+1}((t+1)a)}$ et les relations (2.8) et (2.9) montrent que

$$s_t = \frac{\varphi_t(ta+a)\varphi_1(a)\,\varphi_1(a)\,\varphi_t(ta)}{\varphi_t(ta)\varphi_1(a+ta)\,\varphi_{t+1}((t+1)a)} = (-1)^n \frac{\varphi_1(a)\varphi_t(a)}{\varphi_{t+1}((t+1)a)}$$

ce qui achève la démonstration du lemme 2.9. Démontrons maintenant le lemme 2.8.

a) Si $d = 2$, d'après (2.12) $u^2 = s_1 = \varphi_{-1}(-a)\varphi_1(a)$. Mais $\varphi_{-1} = \varphi_1$ et c'est une fonction paire, donc $u^2 = \varphi_1(a)^2$.

b) Si $d > 2$, d'après (2.12) $u^d = (-1)^{n(d-2)}\varphi_1(a)^d \dfrac{\varphi_{-1}(-a)}{\varphi_{-1}(-a+da)}$.

Comme d divise n nous avons $(-1)^{n(d-2)} = (-1)^n$. Quand $d.a = 0$ nous trouvons $u^d = (-1)^n\varphi(a)^d$. Quand $d.a \neq 0$ nous sommes dans les conditions de validité de (2.10) puisque $d.a \in E_2 - \{0\}$ et $d.a \neq a$ donc $\dfrac{\varphi_{-1}(-a)}{\varphi_{-1}(-a+da)} = (-1)^n$ et $u^d = \varphi(a)^d$ ce qui termine la démonstration du lemme 2.8 et de la proposition 2.6, l'affirmation iii) résultant immédiatement du lemme 2.7, iii) qui montre que $\varphi(a)^2 \in k^\times$.

Il résulte de la proposition 2.6 que l'extension E_n^* a une structure particulièrement simple quand n est impair, c'est le groupe de Heisenberg attaché à E_n. Nous pouvons même, dans ce cas, donner un résultat encore plus précis.

Définition 2.10 : Nous notons $g \overset{W}{\mapsto} (g, W_g)$ la section ensembliste de de $E_n^* \longrightarrow E_n$ définie par les conditions

$$W_o = 1 , \qquad W_g(\tfrac{n+1}{2} g) = -1 \tag{2.13}$$

Proposition 2.11 : Le 2-cocycle associé à la section W est égal à $e_n^{\frac{n+1}{2}}$, en d'autres termes,

$$(g+g', W_{g+g'}) = e_n(g,g')^{\frac{n+1}{2}} . (g, W_g).(g', W_{g'}) . \tag{2.14}$$

Preuve : Posons $a = \frac{n+1}{2} g$ et $a' = \frac{n+1}{2} g'$. Si $\alpha = \frac{W_{g+g'}(x)}{W_g(x) W_{g'}(x-g)}$ nous avons $(g+g', W_{g+g'}) = \alpha(g, W_g)(g', W_{g'})$ et quatre cas sont à considérer.

a) $g = 0$ ou $g' = 0$ alors $\alpha = 1$

b) $g = g' \neq 0$ alors $\alpha = \dfrac{W_{2g}(x)}{W_g(x) W_g(x-g)} = - \dfrac{W_{2g}(2a)}{W_g(a)^2} = 1$ d'après le lemme 2.7 et la normalisation de W_g.

c) $g = -g' \neq 0$ alors $\alpha = \dfrac{1}{W_{-g}(x) W_g(x+g)} = \dfrac{1}{W_{-g}(-a) W_g(a)} = 1.$

d) $g = 0$, $g' = 0$, $g = g'$ alors $\alpha = \dfrac{W_{g+g'}(a+a')}{W_g(a+a') W_{g'}(a'-a)} = - \dfrac{W_g(a)\ W_{g'}(a')}{W_g(a+a')\, W_g(a'-a)}$

et $\alpha = e_{2n}(a,a') = e_n(a,2a') = e_n(g,g')^{(n+1)/2}$ d'après (2.7) et (2.9).

2.5 L'algèbre graduée $L^*(\delta)$

Définition 2.12 : Soit d un entier > 0. Nous notons

$$L(d.\delta) = \{ f \in K_k(E) \mid \mathrm{div}(f) + d.\delta \geq 0 \}$$

et

$$L^*(\delta) = \bigoplus_d L(d.\delta).$$

Les k-espaces vectoriels $L(d.\delta)$ sont de dimension finie et l'espace $L^*(\delta)$ est muni naturellement par la multiplication des fonctions d'une structure d'algèbre graduée par $\mathbf{N}$. De plus, $L(0.\delta) = k$.

Proposition 2.13 : i) Soient f dans $L(d.\delta)$ et (g,φ) dans $G(\delta)$. La fonction ${}^{g}f.\varphi^{d}$ est dans $L(d.\delta)$.

ii) Si $\tau_d(g,\varphi)$ désigne l'automorphisme $f \to {}^{g}f.\varphi^{d}$ de $L(d.\delta)$, l'application $\tau_d : (g,\varphi) \to \tau_d(g,\varphi)$ est une représentation de $G(\delta)$ dans $L(d.\delta)$. De plus, les représentations τ_d s'étendent en une représentation τ de $G(\delta)$ dans le groupe des automorphismes de l'algèbre graduée $L^*(\delta)$. Nous appellerons τ la représentation canonique de $G(\delta)$.

iii) Si δ est un diviseur positif de degré supérieur ou égal à 2 et si $d \geq 1$, la représentation τ_d a pour noyau le sous-groupe de $G(\delta)$ formé des éléments $(0,\varphi)$ où φ est une constante telle que $\varphi^d = 1$. En particulier, τ_1 est fidèle.

Preuve : Les affirmations i) et ii) sont immédiates, montrons iii). Soit (g,φ) dans le noyau de τ_d. Alors , ${}^{g}f.\varphi^{d} = f$ pour toute fonction f dans $L(d.\delta)$. En prenant pour f la fonction constante égale à 1, nous obtenons $\varphi^d = 1$. Donc φ est constante, ${}^{g}\delta = \delta$ et ${}^{g}f = f$ pour toute fonction f dans $L(d.\delta)$. En particulier $({}^{g}r)^d = {}^{g}(r^d) = r^d$ pour toute fonction r dans $L(\delta)$ et il existe une constante ε_r telle que ${}^{g}r = \varepsilon_r.r$. Supposons que g diffère de 0. Le point A étant dans le support de δ, il en est de même du point A + g et, d'après le théorème de Riemann-Roch, il existe une fonction s dans $L(\delta)$ n'ayant pour pôles qu'un pôle simple en A et en A + g. Si g n'est pas d'ordre 2, le diviseur $A+\{A+g\}$ n'est pas invariant par translation par g et on ne peut pas avoir de relation ${}^{g}s = \varepsilon_s.s$. Par conséquent, $2g = 0$ et $\varepsilon_r^2 = 1$ pour toute fonction r dans $L(\delta)$. Mais dans ce cas $2|n$ ce qui n'est possible avec nos hypothèses que si la caractéristique de k n'est pas 2. Si $\varepsilon_s = -1$, la fonction $r = s+1$, qui est dans $L(\delta)$, ne peut pas vérifier une équation du type ${}^{g}r = \varepsilon_r.r$ avec $\varepsilon_r^2 = 1$. Par conséquent, $\varepsilon_s = 1$. Ceci implique que la fonction s vue comme fonction sur la courbe quotient de E par le groupe d'ordre 2 engendré par g n'a qu'un pôle simple, ce qui est impossible en vertu du théorème de Riemann-Roch. La fonction s n'existe pas, $g = 0$, et la proposition 2.13 est démontrée.

Lemme 2.14 : Soient δ et δ' deux diviseurs positifs linéairement équivalents. Les extensions $G(\delta)$ et $G(\delta')$ sont isomorphes ainsi que leurs représentations canoniques. Plus précisément, si R est une fonction telle que $\operatorname{div} R = \delta' - \delta$ les applications

$\nu : G(\delta) \longrightarrow G(\delta')$

$\mu : L^*(\delta) \longrightarrow L^*(\delta')$, définies par

$\nu(g,\varphi) = (g, \varphi . \frac{g_R}{R})$

$\mu(f) = f/R^d$ pour toute $f \in L(d.\delta)$

sont des isomorphismes et

$$\nu(g,\varphi)\mu(f) = \mu((g,\varphi)f).$$

Enfin, si $\sigma : G \longrightarrow G(\delta)$ est une section ensembliste de $G(\delta) \longrightarrow G$, l'application $\mu\sigma$ en est une de $G(\delta') \longrightarrow G$ et les 2-cocyles associés sont égaux.

Preuve : Il est clair que div $\mu(f) + \delta' \geq 0$ et div $\varphi . \frac{g_R}{R} = {}^{g}\delta' - \delta'$. De plus $\nu(g,\varphi)\mu(f) = (g, \varphi . \frac{g_R}{R})\, f/R = \frac{g_f}{g_R} . \varphi . \frac{g_R}{R} = ({}^{g}f.\varphi)/R = \mu({}^{g}f.\varphi) = \mu((g,\varphi)f)$. Enfin, notons $\sigma(g) = (g, \varphi_g)$. Le cocycle associé à σ est donné par la relation

$$\varphi_g . {}^{g}\varphi_{g'} = \alpha(g,g')\varphi_{g+g'}$$

L'application $\mu\sigma$ est une section de $G(\delta') \to G$ car div $\varphi_g . \frac{g_R}{R} = {}^{g}\delta' - \delta'$. Notons α' le cocyle associé, alors $\alpha = \alpha'$ car

$$\varphi_g . \frac{g_R}{R} . {}^{g}\varphi_{g'} \frac{{}^{g+g'}R}{g_R} = \alpha'(g,g')\varphi_{g+g'} . \frac{{}^{g+g'}R}{R}$$

Remarque : L'application ν du lemme précédent ne dépend pas de la normalisation de R alors que μ en dépend.

CHAPITRE 3

Le plongement projectif d'une courbe elliptique associé à un sous-groupe cyclique.

Dans tout ce chapitre nous supposons $E_n \subset E(k)$ et la lettre C désigne un sous-groupe cyclique d'ordre n de E_n. Enfin, nous notons $\underline{C}$ le diviseur

$$\underline{C} = \sum_{g \in C} \{g\} \tag{3.1}$$

et à tout $a \in E_n$ nous associons le caractère $\chi_a \in \mathrm{Hom}(C, \mu_n)$ défini par

$$\chi_a(g) = e_n(a,g) \quad \text{pour tout } g \text{ dans } C. \tag{3.2}$$

En particulier, le caractère χ_o est l'élément neutre de $\mathrm{Hom}(C, \mu_n)$.

3.1 L'extension $E_n(\underline{C})$ et l'algèbre $L^*(\underline{C})$.

L'extension $E_n(\underline{C})$ de $k^\times$ par E_n, définie au paragraphe 2.2 est l'ensemble des couples (a,φ) avec a dans E_n et φ dans $K_k(E)^\times$ tels que

$$\mathrm{div}(\varphi) = {}^a\underline{C} - \underline{C}.$$

On vérifie immédiatement que $E_n(\underline{C})$ contient les sous-groupes suivants :

- $\{(0,t) \mid t \in k^\times\}$ que nous identifions à $k^\times$,
- $\{(g,1) \mid g \in C\}$ que nous identifions à C,
- $\{(g,t) \mid g \in C,\ t \in k^\times\}$ que nous identifions à $C \times k^\times$ et qui est d'indice n dans $E_n(\underline{C})$.

L'algèbre graduée $L^*(\underline{C})$ définie au paragraphe 2.5 porte une structure supplémentaire. En effet, associons à tout caractère $\chi \in \mathrm{Hom}(C, \mu_n)$ et à tout entier $d \geq 0$ l'espace vectoriel

$$L(dC,\chi) = \{f \in L(d\underline{C}) \mid g_f = \chi(g).f \quad \text{pour tout } g \text{ dans } C\} . \tag{3.3}$$

Alors $$L(d\underline{C}) = \bigoplus_{\chi} L(dC,\chi) \quad \text{et}$$

$$L^{*}(\underline{C}) = \bigoplus_{d,\chi} L(dC,\chi).$$

Si les fonctions f et f' appartiennent respectivement à $L(dC,\chi)$ et $L(d'C,\chi')$, la fonction f.f' appartient à $L((d+d')C,\chi\chi')$. Par conséquent, $L^{*}(\underline{C})$ est munie naturellement d'une structure d'algèbre graduée par $\mathbb{N} \times \mathrm{Hom}(C,\mu_n)$. Dans ce qui suit, lorsque nous parlerons de la graduation de $L^{*}(\underline{C})$ c'est de cette graduation dont il s'agira.

Remarque : Soit E' la courbe elliptique quotient de E par l'isogénie de noyau C et soit O' l'élément neutre de E'. Alors, l'espace $L(dC,\chi_o)$ s'identifie à $\{f' \in K_k(E')^{\times} \mid \mathrm{div}_{E'}(f') + d.\{O'\} \geq O\}$.

Proposition 3.1 :
i) Les espaces $L(C,\chi)$ sont de dimension 1.
ii) Si (a,φ) est dans $E_n(\underline{C})$, la fonction φ est une base de $L(C,\chi_a)$.
iii) Pour tout $d \geq 0$, l'application $\tau_d(a,\varphi)$ est un isomorphisme de $L(dC,\chi)$ sur $L(dC,\chi\chi_a^d)$.

Preuve : Soient g dans C et (a,φ) dans $E_n(\underline{C})$. D'après la proposition 2.3 nous avons $\langle a,g\rangle = \varphi/{}^{g}\varphi = e_n(a,g)$. Donc ${}^{g}\varphi = \chi_a(g).\varphi$ et comme φ est dans $L(\underline{C})$, nous voyons que φ est dans $L(C,\chi_a)$. Soit f dans $L(dC,\chi)$. Alors ${}^{g}({}^{a}f.\varphi^{d}) = {}^{a+g}f.({}^{g}\varphi)^{d} = \chi(g).{}^{a}f.({}^{g}\varphi)^{d}$ et, d'après ce qui précède, ${}^{g}({}^{a}f.\varphi^{d}) = \chi(g).\chi_a(g)^{d}.({}^{a}f.\varphi^{d})$. Ceci montre que $\tau_d(a,\varphi)$ envoie $L(dC,\chi)$ dans $L(dC,\chi.\chi_a^{d})$ et on en déduit immédiatement que $\tau_d(a,\varphi)$ est un isomorphisme de $L(dC,\chi)$ sur $L(dC,\chi.\chi_a^{d})$. Il en résulte que la représentation τ_d permute entre eux les espaces $L(dC,\chi)$, transitivement quand d est premier à n et que dans ce cas, ils ont même dimension, indépendamment de χ. En particulier, comme l'espace $L(C,\chi_o)$ ne contient que les constantes, nous avons $1 = \dim L(C,\chi_o) = \dim L(C,\chi)$ pour tout χ. Enfin, la fonction φ qui une fonction non nulle de $L(C,\chi_a)$ est une base de cet espace.

Proposition 3.2 :
La représentation τ_1 est irréductible. Plus précisément, si ρ désigne la représentation irréductible de degré 1 de $C \times k^{\times}$ dans k obtenue en faisant opérer C trivialement et $k^{\times}$ par multiplication sur k, la représentation τ_1 est isomorphe à $\mathrm{Ind}_{C\times k^{\times}}^{E_n(\underline{C})}(\rho)$.

Preuve : Soit $f \in L(\underline{C})$. Pour tout $\chi \in \mathrm{Hom}(C,\mu_n)$, la fonction $\sum_{g\in C} \chi(g)^{-1}.{}^g f$ est dans $L(C,\chi)$. Par conséquent, grâce à la proposition 3.2 iii) on voit que la représentation τ_1 n'a pas de sous-espace irréductible non trivial. Le groupe C opère trivialement sur l'espace $L(C,\chi_o)$ qui est isomorphe à k et le groupe $k^\times$ y opère par multiplication. De plus, le stabilisateur de $L(C,\chi_o)$ est $C \times k^\times$ et les espace $L(C,\chi)$ sont permutés transitivement par par $C \times k^\times$. Ceci suffit pour affirmer que la représentation τ_1 est induite par ρ.[Se]

3.2 L'homomorphisme θ.

Soit $S^*(\underline{C})$ l'algèbre symétrique de l'espace vectoriel $L(\underline{C})$. Puisque $L(\underline{C}) = \oplus_\chi L(\underline{C},\chi)$, cette algèbre porte une structure naturelle d'algèbre graduée par le monoide $\mathbb{N} \times \mathrm{Hom}(C,\mu_n)$. De plus, l'homomorphisme canonique $\theta : S^*(\underline{C}) \longrightarrow L^*(\underline{C})$ respecte les structures d'algèbres graduées par $\mathbb{N}\times \mathrm{Hom}(C,\mu_n)$ de $S^*(\underline{C})$ et $L^*(\underline{C})$. Nous notons $K^*(\underline{C})$ le noyau de θ. C'est un idéal gradué de $S^*(\underline{C})$.

Dans ce paragraphe nous allons étudier θ et $K^*(\underline{C})$. Pour simplifier les notations, et puisque le groupe C est fixé, nous posons :

$L = L^*(\underline{C})$, $S = S^*(\underline{C})$, $K = K^*(\underline{C})$, $L_{d,\chi} = L(d.\underline{C},\chi)$, et nous notons $S_{d,\chi}$(resp.$K_{d,\chi}$) la partie homogène de degré (d,χ) de S(resp.K) , $\theta_{d,\chi}$ la restriction à $S_{d,\chi}$ de θ , $L_d = L(d.\underline{C})$, $S_d = \oplus_\chi S_{d,\chi}$, $K_d = \oplus_\chi K_{d,\chi}$.

Théorème 3.3 : Si $n \geq 3$, l'homomorphisme θ est surjectif. De plus,

$$\dim L_{d,\chi} = d, \qquad \text{pour tout } \chi \in \mathrm{Hom}(C,\mu_n) \tag{3.4}$$

Preuve : Pour démontrer le théorème, il suffit de voir

Lemme 3.4 : Pour tout (d,χ) avec $d \geq 1$, il existe d^2 fonctions $\varphi_{i,j}^{(d)}$ avec $1\leq i\leq d$ et $1\leq j\leq d$, dans L_1, telles que les d fonctions

$$f_i^{(d)} = \varphi_{i,1}^{(d)}\cdot\varphi_{i,2}^{(d)}\cdots\varphi_{i,d}^{(d)}$$

soient linéairement indépendantes et soient dans $L_{d,\chi}$.

En effet, il résulte de ce lemme que $\dim L_{d,\chi} \geq \dim \operatorname{Im} \theta_{d,\chi}$ pour tout (d,χ) avec $d \geq 1$ et comme $\dim L_d = \sum_{\chi} \dim L_{d,\chi} = nd$ d'après le théorème de Riemann-Roch, nous trouvons $\dim L_{d,\chi} = d$ et $L_{d,\chi} = \operatorname{Im} \theta_{d,\chi}$.

Preuve du lemme 3.4 : Fixons χ et raisonnons par récurrence sur d. Si $d = 1$, l'espace $L_{1,\chi}$ est de dimension 1 d'après la proposition 3.1, et il suffit de prendre pour $\varphi^{(1)}_{1,1}$ n'importe quelle fonction non nulle de L_1.

Maintenant, supposons construites les $(d-1)^2$ fonctions $\varphi^{(d-1)}_{i,j}$. Posons alors $\varphi^{(d)}_{i,j} = \varphi^{(d-1)}_{i,j}$ pour $1 \leq i \leq d-1$ et $1 \leq j \leq d-1$ puis, prenons pour $\varphi^{(d)}_{i,d}$ la fonction constante égale à 1.

Lemme 3.5 : Supposons $n>2$. Pour tout (d,χ) avec $d \geq 2$, il existe $\chi_1, \chi_2, \ldots \chi_d$ dans $\operatorname{Hom}(C, \mu_n)$, non triviaux, tels que $\chi = \chi_1 \chi_2 \ldots \chi_d$.

Preuve : Supposons écrits tous les caractères sous la forme $\chi = \chi_1 \chi_2 \ldots \chi_d$. En multipliant chacune de ces n équations par un caractère non trivial nous obtenons une décomposition de tous les caractères en produits de $d+1$ caractères non triviaux. Il suffit donc d'examiner le cas $d = 2$.

Si χ est trivial, nous prenons n'importe quel caractère non trivial χ' et nous écrivons $\chi = \chi' . \chi'^{-1}$. Si χ n'est pas trivial, puisque $n>2$, il existe un caractère non trivial χ' différent de χ et nous écrivons $\chi = (\chi\chi'^{-1})\chi'$.

A l'aide du lemme précédent nous écrivons χ sous la forme $\chi = \chi_1 \ldots \chi_d$ avec des caractères χ_i non triviaux et nous prenons pour $\varphi^{(d)}_{d,j}$ n'importe quelle fonction non nulle de L_{1,χ_j}. Nous avons maintenant construit d^2 fonctions dans L_1 telles que les d fonctions $f^{(d)}_i$ soient dans $L_{d,\chi}$. De plus, ces fonctions sont linéairement indépendantes car les $f^{(d)}_i$ pour $1 \leq i \leq d-1$ sont dans $L_{d-1,\chi}$ et sont indépendantes tandis que $f^{(d)}_d$ est dans $L_{d,\chi} - L_{d-1,\chi}$. Ceci achève la démonstration du lemme 3.4 et par conséquent celle du théorème 3.3. On en déduit immédiatement

Corollaire 3.6 : La suite $0 \to K_{d,\chi} \longrightarrow S_{d,\chi} \xrightarrow{\theta_{d,\chi}} L_{d,\chi} \longrightarrow 0$ est exacte.

Si $n=3$, on a

$$\begin{cases} \dim K_{d,\chi} = 0 & \text{si } d \leq 2 , \\ \dim K_{3,\chi} = 0 & \text{si } \chi \neq \chi_o , \\ \dim K_{3,\chi_o} = 1 . \end{cases}$$

Si $n>3$, on a $\begin{cases} \dim K_{d,\chi} = 0 \text{ si } d\leq 1 , \\ \dim K_{2,\chi} = \dfrac{n-4+r_\chi}{2} , \text{ où } r_\chi \text{ désigne le} \end{cases}$

nombre de $\chi' \in \mathrm{Hom}(C,\mu_n)$ tels que $\chi'^2 = \chi$.

3.3 L'idéal $K^*(C)$ avec $n>3$.

Choisissons un générateur φ_χ de $L_{1,\chi}$ pour tout $\chi \in \mathrm{Hom}(C,\mu_n)$.

Théorème 3.7 : Soient $\chi_1,\chi_1',\chi_2,\chi_2',\chi_3,\chi_3'$ dans $\mathrm{Hom}(C,\mu_n)$ tels que

$$\chi_1\chi_1' = \chi_2\chi_2' = \chi_3\chi_3' .$$

Alors il existe trois constantes $\alpha_1,\alpha_2,\alpha_3$ non toutes nulles telles que

$$\alpha_1\varphi_{\chi_1}\varphi_{\chi_1'} + \alpha_2\varphi_{\chi_2}\varphi_{\chi_2'} + \alpha_3\varphi_{\chi_3}\varphi_{\chi_3'} = 0.$$

De plus, si les six caractères sont distincts, aucune des constantes α_i n'est nulle.

Preuve : Soient a et a' dans E_n tels que $\chi_1 = \chi_a$ et $\chi_1' = \chi_{a'}$. Alors les trois fonctions 1, $\dfrac{\varphi_{\chi_2}\varphi_{\chi_2'}}{\varphi_{\chi_1}\varphi_{\chi_1'}}$, $\dfrac{\varphi_{\chi_3}\varphi_{\chi_3'}}{\varphi_{\chi_1}\varphi_{\chi_1'}}$ sont invariantes par translation par les éléments de C et sont dans l'espace vectoriel $L({}^a\underline{C}+{}^{a'}\underline{C})$. Si λ désigne l'isogénie $E \longrightarrow E/C = E'$, ces fonctions considérées comme fonctions sur E' sont dans l'espace vectoriel $L(\{\lambda a\}+\{\lambda a'\})$ qui est de dimension 2, d'où leur dépendance linéaire et l'existence des constantes α_i. Supposons maintenant que les six caractères sont différents et que $a_2 = 0$. Il suffit alors de prendre la valeur en a de $\alpha_1\varphi_{\chi_1}\varphi_{\chi_1'} + \alpha_3\varphi_{\chi_3}\varphi_{\chi_3'}$ pour voir que cette fonction ne peut être nulle que si $\alpha_1 = \alpha_3 = 0$. Par raison de symétrie on voit donc qu'aucune des constantes α_i ne peut être nulle.

Nous déduisons immédiatement du théorème 3.7 .

Corollaire 3.8 : Soit $\chi \in \mathrm{Hom}(C,\mu_n)$. L'espace vectoriel $K_{2,\chi}$ est engendré par les polynômes de la forme

$$\alpha_1\varphi_{\chi_1}\varphi_{\chi_1'} + \alpha_2\varphi_{\chi_2}\varphi_{\chi_2'} + \alpha_3\varphi_{\chi_3}\varphi_{\chi_3'}$$

avec $\chi_1\chi_1' = \chi_2\chi_2' = \chi_3\chi_3' = \chi$.

Théorème 3.9 : Si n>3, l'idéal K est engendré par ses éléments de degré 2; autrement dit $K = K_2.S$,

Preuve : Nous désignons par $\chi_0, \chi_1, \ldots, \chi_{k-1}$ les éléments de $\mathrm{Hom}(C, \mu_n)$. Comme $n \geq 4$, il est toujours possible de trouver χ_r et χ_s tels que

$$(3.5) \qquad \chi_r \neq \chi_0 , \qquad \chi_s^2 \neq \chi_0 , \chi_r \text{ et } \chi_r^2 .$$

En effet, il suffit de prendre par exemple pour χ_r un générateur de $\mathrm{Hom}(C, \mu_n)$ et de poser $\chi_s = \chi_r^{-1}$ quand n>4 (resp. $\chi_s = \chi_r^2$ quand n = 4). Nous fixons deux caractères χ_r et χ_s possédant les propriétés (3.5) Nous désignons par $(K_2.S)_{d,\chi}$ les éléments de $S_{d,\chi}$ qui sont dans l'idéal $K_2.S$ de S et nous dirons que deux éléments de S sont équivalents si leur différence est dans l'idéal de S engendré par K_2 et φ_{χ_0} .

Lemme 3.10 : Tout élément de $S_{d,\chi}$ est équivalent à un multiple du polynôme $P_{d,\chi}$ défini par

$$P_{d,\chi} = \begin{cases} \varphi_{\chi_r}^{d-2} \varphi_{\chi_s} \varphi_{\chi_r \chi_s^{-1}} & \text{si } \chi \chi_r^{1-d} = \chi_0 \\ \varphi_{\chi_r}^{d} & \text{si } \chi \chi_r^{1-d} = \chi_r \\ \varphi_{\chi_r}^{d-1} \varphi_{\chi_s} & \text{si } \chi \chi_r^{1-d} = \chi_s \\ \varphi_{\chi_r}^{d-1} \varphi_{\chi_i} & \text{si } \chi_i = \chi \chi_r^{1-d} \neq \chi_0, \chi_r, \chi_s \end{cases}$$

Preuve : Soit $m = \varphi_{\chi_0}^{\alpha_0} \varphi_{\chi_1}^{\alpha_1} \ldots \varphi_{\chi_{n-1}}^{\alpha_{n-1}} \in S_{d,\chi}$. Nous posons $d_s(m) = \alpha_s$ et $d'(m) = d - \alpha_0 - \alpha_r - \alpha_s$. Le théorème 3.7 montre que si χ_i et χ_j sont différents de χ_0 , χ_r et χ_s on peut écrire dans S le produit $\varphi_{\chi_i} . \varphi_{\chi_j}$ comme combinaison linéaire d'un élément de $K_{2,\chi_i\chi_j}$, de $\varphi_{\chi_0} \varphi_{\chi_i\chi_j}$ et de $\varphi_{\chi_r} \varphi_{\chi_i\chi_j\chi_r^{-1}}$ si $\chi_i\chi_j \neq \chi_r$ (resp. de $\varphi_{\chi_s} \varphi_{\chi_i\chi_j\chi_s^{-1}}$ si $\chi_s \neq \chi_i\chi_j$). Par conséquent, tout monôme m de $S_{d,\chi}$ tel que $d'(m) \geq 2$ est équivalent à un monôme m' tel que $d'(m') = d'(m) - 1$ et par récurrence nous en déduisons que tout monôme m de $S_{d,\chi}$ est équivalent à un monôme m' tel que $d'(m') \leq 1$. Nous rangeons les monômes qui ont cette propriété et qui ne sont pas équivalents à 0 en deux ensembles

$$U = \{\varphi_{\chi_r}^{u}\varphi_{\chi_s}^{v} \mid u,v\geq 0 \quad u+v>0\}$$

$$V = \{\varphi_{\chi_r}^{u}\varphi_{\chi_s}^{v}\varphi_{\chi_i} \mid u,v\geq 0 \ , \ \chi_i \neq \chi_o,\chi_r,\chi_s\}.$$

a) Comme nous avons supposé $\chi_s^2 \neq \chi_r$, le théorème 3.7 nous permet d'écrire dans S le produit $\varphi_{\chi_s}^2$ comme combinaison linéaire d'un élément de K_{2,χ_s^2} de $\varphi_o\varphi_{\chi_s^2}$ et de $\varphi_{\chi_r}\varphi_{\chi_s^2}\chi_r^{-1}$. Par conséquent, si $m \in U$ et si $d_s(m)\geq 2$, il existe m' dans V équivalent à m, tel que $d_s(m') = d_s(m)-2$.

b) De même, si $\chi_i \neq \chi_r\chi_s^{-1}$, d'après le théorème 3.7 nous pouvons écrire dans S le produit $\varphi_{\chi_s}\varphi_{\chi_i}$ comme combinaison linéaire d'un élément de $K_{2,\chi_s\chi_i}$ de $\varphi_{\chi_o}\varphi_{\chi_s\chi_i}$ et de $\varphi_{\chi_r}\varphi_{\chi_s\chi_r^{-1}\chi_i}$. Par conséquent, si $m = \varphi_{\chi_r}^{u}\varphi_{\chi_s}^{v}\varphi_{\chi_i} \in V$ est tel que $d_s(m)\geq 1$ et $\chi_i \neq \chi_r\chi_s^{-1}$ il existe $m' \in V$ équivalent à m tel que $d_s(m') = d_s(m) - 1$.

c) Si $m = \varphi_{\chi_r}^{u}\varphi_{\chi_s}^{v}\varphi_{\chi_r\chi_s^{-1}}$ est tel que $d_s(m) = v \geq 2$, nous pouvons utiliser le raisonnement fait en a) pour montrer que m est équivalent à un multiple de $\varphi_{\chi_r}^{u+1}\varphi_{\chi_s}^{v-2}\varphi_{\chi_r\chi_s^{-1}}\varphi_{\chi_s^2\chi_r^{-1}}$. Or nous avons supposé $\chi_s^2 \neq \chi_r^2$. Par conséquent, d'après le théorème 3.7, il est possible d'écrire dans S le produit $\varphi_{\chi_r\chi_s^{-1}}\varphi_{\chi_s^2\chi_r^{-1}}$ comme combinaison linéaire d'un élément de K_{2,χ_s}, de $\varphi_{\chi_o}\varphi_{\chi_s}$ et de $\varphi_{\chi_r}\varphi_{\chi_s\chi_r^{-1}}$ et m est équivalent à un multiple m' de $\varphi_{\chi_r}^{u+2}\varphi_{\chi_s}^{v-2}\varphi_{\chi_s\chi_r^{-1}}$ qui est tel que $d_s(m') = d_s(m) - 2$.

Nous déduisons de a),b),c) que tout monôme m de $S_{d,\chi}$ est équivalent soit à un monôme m' de U tel que $d_s(m') \leq 1$, soit à un monôme de V tel que $d_s(m') = 0$, soit à un multiple de $\varphi_{\chi_r}^{d-2}\varphi_{\chi_s}\varphi_{\chi_r\chi_s^{-1}}$. Il suffit maintenant d'écrire quels sont les monômes m' de $S_{d,\chi}$ satisfaisant ces conditions pour voir que m' est nécessairement un multiple de $P_{d,\chi}$.

Nous sommes en mesure de terminer la démonstration du théorème 3.9. Soient $d\geq 2$ et $P \in K_{2,\chi}$. D'après le lemme 3.10, il existe P'' dans l'idéal engendré par K_2,P' dans $S_{d-1,\chi}$ et une constante α tels que

$$P = P'' + \varphi_{\chi_o} P' + \alpha P_{d,\chi} \ .$$

Mais, $\theta(P) = \theta(P'') + \theta(P') + \alpha\,\theta(P_{d,\chi}) = 0$. La constante α est nécessairement nulle sinon la fonction $\theta(P)$ aurait un pôle en 0, donc $\theta(P') = 0$ et $P' \in K_{d-1,\chi}$. Par récurrence on en déduit que $P \in K_2.S$ puisque $K_{1,\chi} = \{0\}$.

3.4 L'idéal $K^*(C)$ avec n = 3.

Choisissons un générateur φ_χ de $L_{1,\chi}$ pour tout $\chi \in \mathrm{Hom}(C,\mu_n)$.

Théorème 3.11 : L'espace vectoriel K_{3,χ_o} est engendré par un élément

$$R = a_o\varphi^3_{\chi_o} + \alpha_1\varphi^3_{\chi_1} + \alpha_2\varphi^3_{\chi_2} + \beta\varphi_{\chi_o}\varphi_{\chi_1}\varphi_{\chi_2}$$

tel que les α_i ne soient pas nuls.

Preuve : Soit R un générateur de K_{3,χ_o}. Comme tout élément de $S_{3,\chi}$ est combinaison linéaire de $\varphi^3_{\chi_o}, \chi^3_{\chi_1}, \varphi^3_{\chi_2}$ et de $\varphi_{\chi_o}\varphi_{\chi_1}\varphi_{\chi_2}$, il existe pour R une décomposition de la forme annoncée. Il suffit alors de regarder l'ordre du pôle de $\theta(R)$ en 0 pour voir que si $\alpha_1 = 0$ on a aussitôt $\alpha_2 = 0, \beta = 0$. $\alpha_o = 0$ et $R = 0$. De même si $\alpha_2 = 0$. Enfin, si a désigne un zéro de φ_{χ_1}, le calcul de la valeur en a de $\theta(R)$ montre que si $\alpha_o = 0$ on a aussi $\alpha_2 = 0$ donc $R = 0$.

Théorème 3.12 : Si n = 3 l'idéal K de S est engendré par ses éléments de degré 3.

Preuve : Nous notons χ_o, χ_1, χ_2 les éléments de Hom (C,μ_3) et nous dirons que deux éléments de S sont équivalents si leur différence est dans l'idéal engendré par K_3 et φ_{χ_o}.

Lemme 3.13 : Soit (d,χ) avec $d>2$. Tout élément de $S_{d,\chi}$ est équivalent à un multiple du polynôme $p_{d,\chi}$ défini par

$$P_{d,\chi} = \begin{cases} \varphi_{\chi_1}\varphi_{\chi_2}^{d-1} & \text{si } \chi = \chi_2^{d-2} \\ \varphi_{\chi_1}^2\varphi_{\chi_2}^{d-2} & \text{si } \chi = \chi_2^{d-1} \\ \varphi_{\chi_2}^d & \text{si } \chi = \chi_2^d \end{cases}$$

Preuve : Soit $m = \varphi_{\chi_o}^{\alpha_o}\varphi_{\chi_1}^{\alpha_1}\varphi_{\chi_2}^{\alpha_2} \in S_{d,\chi}$. Nous posons $d_1(m) = \alpha_1$. Le théorème 3.11 montre que $\varphi_{\chi_1}^3$ s'écrit dans S comme combinaison linéaire d'un élément de K_{3,χ_o} de $\varphi_{\chi_o}^3$, de $\varphi_{\chi_2}^3$ et de $\varphi_{\chi_o}\varphi_{\chi_1}\varphi_{\chi_2}$. Par conséquent, si $m \in S_{d,\chi}$ est tel que $d_1(m) \geq 3$, il existe m' dans $S_{d,\chi}$ équivalent à m tel que $d_1(m') = d_1(m) - 3$. Nous en déduisons par récurrence que tout monôme est équivalent à un monôme de $S_{d,\chi}$ tel que $d_1(m') \leq 2$, et comme les seuls monômes de $S_{d,\chi}$ satisfaisant cette condition sont les multiples de $P_{d,\chi}$ le lemme est démontré.

Soit maintenant $P \in K_{d,\chi}$ avec $d \geq 3$. D'après le lemme 3.14 il existe $P'' \in (K_3.S)_{d,\chi}$, $P' \in S_{d-1,\chi}$ et une constante α tels que

$$P = P'' + \varphi_{\chi_o} P' + \alpha P_{d,\chi}$$

Or $\theta(P) = \theta(P') + \alpha\,\theta(P_{d,\chi}) = 0$ et la constante α est nécessairement nulle sinon la fonction $\theta(P)$ aurait un pôle en 0. Donc $\theta(P') = 0$ et $P' \in K_{d-1,\chi}$. Par récurrence on en déduit que P est dans $K_3.S$ puisque $K_{d,\chi}$ est nul pour $d \leq 2$, ce qui démontre le théorème 3.12

Soit δ un diviseur positif sur une courbe elliptique. Si deg $\delta \geq 3$, ce diviseur est très ample et il lui est associé un plongement projectif π de E dans $\mathbb{P}L(\delta)$ l'espace projectif associé à $L(\delta)[Mu]$. Supposons $\delta = \underline{C}$. Quand $n = 3$ le théorème 3.12 montre que $\pi(E)$ est une cubique de $\mathbb{P}^2$. Quand $n \geq 4$, le théorème 3.9 montre que $\pi(E)$ est une intersection de quadriques dans $\mathbb{P}^{n-1}$.

Au chapitre 5 nous étudierons plus en détail ce plongement.

CHAPITRE 4

Les fonctions X_a et leurs relations.

Dans tout ce chapitre nous supposerons l'entier n.impair et $E_n \subset E(k)$. La lettre C désigne un sous-groupe cyclique d'ordre n de E_n et le symbole $\underline{C}$ a le même sens qu'en (3.1).

4.1 Les fonctions X_a

D'après le théorème d'Abel et comme nous avons supposé le nombre n impair, les diviseurs $\underline{C}$ et $n\{0\}$ sont linéairement équivalents. D'après le lemme 2.14 les extensions $E_n(C)$ et $E_n(n\{0\})$ ainsi que leurs représentations canoniques sont isomorphes. Au paragraphe 2.4 nous avons défini une section ensembliste W de $E_n(n\{0\}) \to E_n$, et grâce au lemme 2.14 nous pouvons construire une section de $E_n(\underline{C}) \to E_n$ qui définit le même 2-cocycle que W.

Définition 4.1 : Soit $R \in K_k(E)^\times$ telle que $\mathrm{div}(R) = \underline{C} - n\{0\}$.
A tout élément $a \in E_n$ nous associons la fonction définie par

$$X_a = W_a \cdot \frac{{}^aR}{R} \tag{4.1}$$

où W_a est la fonction définie par (2.10).

Nous noterons $X_a = X_{a,C}$ lorsque nous aurons besoin de marquer la dépendance de C.

Proposition 4.2 : La fonction X_a est la seule à vérifier les deux conditions

$$\mathrm{div}(X_a) = {}^a\underline{C} - \underline{C} = \sum_{g \in C} \{g+a\} - \{g\} \tag{4.2}$$

$$\begin{cases} X_a = 1 & \text{si } a \in C \\ X_a\left(\frac{n+1}{2}\, a\right) = 1 & \text{si } a \notin C \end{cases} \tag{4.3}$$

Preuve : Il suffit donc de vérifier (4.3) car il est clair que X_a satisfait (4.2). La fonction R est paire. En effet, div(R(x)) = div(R(-x)) donc R(x) = εR(-x) avec $\varepsilon^2 = +1$. Or, $0 \notin \mathrm{Supp}(\mathrm{div}(R))$ d'où, R(0) = εR(0) et ε = 1. De plus, si a ∈ C les points $\frac{n+1}{2}$ a et $-\frac{n+1}{2}$ a ne sont pas supp(div(R)) donc $\frac{{}^aR}{R}(\frac{n+1}{2}\ a) = \frac{R(-\frac{n+1}{2}\ a)}{R(\frac{n+1}{2}\ a)} = 1$ et comme $W_a(\frac{n+1}{2}\ a) = -1$ par définition nous obtenons $X_a(\frac{n+1}{2}\ a) = -1$ quand a ∉ C. Par contre, si a ∈ C, les points $\frac{n+1}{2}$ a et $-\frac{n+1}{2}$ a sont dans supp(div(R)) avec la multiplicité 1 et $\frac{{}^aR}{R}(\frac{n+1}{2}\ a) = -1$ compte-tenu de la parité de R. Ceci montre que $X_a(\frac{n+1}{2}\ a) = 1$ si a ∈ C.

Proposition 4.3 : Le groupe C étant fixé, les diverses fonctions X_a vérifient

(4.4) $\quad X_{a+a'} = e_n(a,a')^{\frac{n+1}{2}}\ X_a . {}^aX_{a'}$

(4.5) $\quad X_{a'} = e_n(a,a')^{\frac{n+1}{2}}\ X_a \qquad$ si a'-a ∈ C.

(4.6) $\quad X_{a+a'} = X_a . {}^aX_{a'} \qquad$ si a et a' sont dans un même sous-groupe cyclique de E_n.

(4.7) $\quad X_a(x) = X_{-a}(-x)$.

Preuve : L'identité (4.4) résulte immédiatement du lemme 2.14 et de la relation (2.14). Les identités (4.5) et (4.6) sont des cas particuliers de (4.4). Enfin, (4.7) s'obtient en comparant les diviseurs de chaque membre et leur valeur en $\frac{n+1}{2}$ a.

Proposition 4.4

i) La fonction X_a est une base de $L(C,\chi_a)$. Autrement dit,

$$ {}^gX_A = e_n(a,g)X_a \quad \text{pour tout } g \in C$$

ii) Soit φ ∈ L(C). S'il existe a ∈ E_n tel que ${}^g\varphi = \chi_a(g)\varphi$ pour tout g ∈ C alors il existe une constante α telle que φ = αX_a.

iii) Soient $a_1,\ldots,a_s$ et a dans E_n. Ou bien X_a n'appartient pas à l'espace vectoriel engendré par les fonctions X_{a_i} ou bien il existe un indice i et une constante α tels que $X_a = \alpha X_{a_i}$ et dans ce cas $a-a_i \in C$ et $\alpha = e_n(a,a_i)^{\frac{n+1}{2}}$.

Preuve : Les affirmations i) et ii) résultent immédiatement de la proposition 3.1. L'affirmation iii) résulte de ce que $L(\underline{C}) = \bigoplus_{\chi} L(\underline{C},\chi)$ et de (4.5).

4.2 Comparaison de $E_n(\underline{C})$ et $E_n(\underline{C}')$ et de leurs représentations canoniques.

Dans ce paragraphe, C et C' désignent deux sous-groupes cycliques d'ordre n de E_n. Nous posons

$$d(C,C') = \#(C \cap C'). \tag{4.8}$$

Nous avons donc $n = d(C,C) = d(C',C')$.

Comme les diviseurs $\underline{C}$ et $\underline{C}'$ sont linéairement équivalents, les extensions $E_n(\underline{C})$ et $E_n(C')$ sont isomorphes ainsi que leurs représentations canoniques et le lemme 2.14 dont nous reprenons les notations associe à toute fonction R telle que

$$\mathrm{div}(R) = \underline{C}' - \underline{C} \tag{4.9}$$

un isomorphisme $\mu : L^*(\underline{C}) \to L^*(\underline{C}')$. La fonction R n'est définie qu'à un multiple près par (4.9); nous allons voir qu'il est possible de la normaliser de façon canonique.

Définition 4.5 : Nous posons :

$$R_C^{C'} = \sum_{g' \in C'} X_{g',C} \tag{4.10}$$

Proposition 4.6 : La fonction $R_C^{C'}$ n'est pas nulle et satisfait à

$$\mathrm{div}(R_C^{C'}) = \underline{C}' - \underline{C}, \tag{4.11}$$

$$R_C^{C'} \cdot R_{C'}^{C} = n.d(C',C). \tag{4.12}$$

Preuve : Soit R une fonction non nulle satisfaisant à(4.9). On obtient immédiatement

$$X_{a,C'} = X_{a,C} \cdot \frac{a_R}{R} \quad \text{pour tout } a \in E_n \,, \tag{4.13}$$

et comme $X_{g,C} = X_{g',C'} = 1$ pour $g \in C$ et $g' \in C'$, nous avons

$$\begin{cases} X_{g',C} = \dfrac{R}{g'_R} & \text{pour tout } g' \in C' \\ X_{g,C'} = \dfrac{g_R}{R} & \text{pour tout } g \in C \,. \end{cases} \tag{4.14}$$

Soit $\varphi = \dfrac{R_C^{C'}}{R} = \sum_{g'} \dfrac{1}{g'_R}$ et soit r' un élément quelconque de C'. Alors,

$r'\varphi = (\sum_{g'} r' X_{g',C} \frac{R}{r'_R}) = (\sum_{g'} r' X_{g',C} X_{r',C}) / R = \varphi$, ce qui prouve que φ est constante.

Calculons $R_C^{C'} R_{C'}^{C} = \sum_{g,g'} X_{g',C} X_{g',C} = \sum_{g,g'} {}^{g}R/g'_R = \sum_{g} {}^{g}R \sum_{g'} \dfrac{1}{g'_R} = (\sum_{g} {}^{g}R)\varphi$.

Or nous venons de voir que φ est constante donc $\varphi = {}^{g}\varphi = \sum_{g'} \dfrac{1}{g+g'_R}$ pour tout $g \in C$ et $R_C^{C'} R_{C'}^{C} = \sum_{g} {}^{g}R \sum_{g'} \dfrac{1}{g+g'_R} = \sum_{g,g'} \dfrac{g_R}{g+g'_R} = \sum_{g'} {}^{g}X_{g',C}$.

Comme ${}^{g}X_{g',C} = e_n(g',g) X_{g',C}$ d'après la proposition 4.4 nous obtenons

$$R_C^{C'} R_{C'}^{C} = \sum_{g'} X_{g',C} \left[\sum_{g} e_n(g',g) \right]$$

Le terme figurant entre crochets est nul si $g' \notin C$ et est égal à n si $g' \in C$, cas où $X_{g',C} = 1$ ce qui donne enfin $R_C^{C'} R_{C'}^{C} = n \sum_{g' \in C \cap C'} 1 = n.d(C',C)$.

Il en résulte que $R_C^{C'}$ n'est pas nulle et (4.11) est prouvé puisque $\varphi = \dfrac{R_C^{C'}}{R}$ est constante.

Corollaire 4.7 : Nous avons :

$$X_{a,C'} = X_{a,C} \frac{{}^{a}R_C^{C'}}{R_C^{C'}} \quad \text{pour tout } a \in E_n \,. \tag{4.15}$$

$$X_{g',C} = \frac{R_C^{C'}}{g' R_C^{C'}} = \frac{{}^{g'}R_{C'}^{C}}{R_{C'}^{C}} \quad \text{pour tout } g' \in C'. \tag{4.16}$$

$$\sum_{g' \in C'} \frac{1}{g' R_C^{C'}} = 1 \,. \tag{4.17}$$

Preuve : Les formules (4.15) et (4.16) ne sont autres que (4.13) et (4.14) écrites avec $R_C^{C'}$ à la place de R. La formule (4.17) s'obtient en divisant les deux membres de (4.10) par $R_C^{C'}$.

Corollaire 4.8 : Soit X une fonction sur E n'ayant pour pôles qu'un pôle double en 0. Soient g un générateur de C et g' un générateur de C' Alors

$$(4.19) \qquad X_{g',C} = \prod_{r=1}^{\frac{n-1}{2}} \frac{[X(x-g') - X(rg)]\,[X(x) - X(rg')]}{[X(x-g') - X(rg')]\,[X(x) - X(rg)]}$$

Preuve : Les fonctions $R_C^{C'}$ et $\prod_{r=1}^{\frac{n-1}{2}} \frac{X(x) - X(rg')}{X(x) - X(rg)}$ qui ont même diviseur sont multiples l'une de l'autre et il suffit d'utiliser (4.14).

Définition 4.9 : Notons $L(\underline{C},\underline{C}')$ le sous-espace de $L(\underline{C})$ engendré par les fonctions $X_{g',C}$ avec $g' \in C'$.

Théorème 4.10 :

$$(4.20) \qquad \dim L(\underline{C},\underline{C}') = n/d(C,C')$$

Preuve : La proposition 4.4 montre que la dimension de L(C,C') est égale à l'indice de $C \cap C'$ dans C, ce qui prouve (4.20).

Théorème 4.11 : L'application μ associée à $R_C^{C'}$ par lemme 2.14 est un isomorphisme entre $L(\underline{C},\underline{C}')$ et $L(\underline{C}',\underline{C})$. Plus précisément, soit $a \in E_n$, A toute fonction $\varphi \in L(\underline{C})$ est associée une constante $\lambda_a(\varphi)$ telle que

$$(4.21) \qquad \lambda_a(\varphi).X_{a,C'} = \mu\Big(\sum_{g' \in C'} e_n(-a,g')X_{g',C}.^{g'}\varphi\Big) = \sum_{g' \in C'}\left[e_n(-a,g')X_{g',C}.\frac{^{g'}\varphi}{R_C^{C'}}\right]$$

ou encore

$$(4.22) \qquad \lambda_a(\varphi).^a R_C^{C'}.X_{a,C} = \sum_{g' \in C'} e_n(-a,g')X_{g',C}.^{g'}\varphi \ .$$

De plus, la forme linéaire $\varphi \mapsto \lambda_a(\varphi)$ est définie par

$$(4.23) \qquad \lambda_a(X_{b,C}) = e_n(a,b)^{\frac{n+1}{2}}.\varepsilon(a-b)$$

où $\varepsilon : E_n \longrightarrow \mu_n \cup \{0\}$ est donnée par

$$(4.24)\quad \varepsilon(r) = \begin{cases} 0 & \text{si } r \notin C'+C \\ e_n(\bar{r}',\bar{r})^{\frac{n+1}{2}} & \text{si } r = \bar{r}'+\bar{r} \text{ avec } \bar{r}' \in C' \text{ et } \bar{r} \in C. \end{cases}$$

Preuve : Les égalités (4.21) et (4.22) sont équivalentes d'après (4.15). La fonction $\sum_{g' \in C'} e_n(-a,g')X_{g',C} \cdot {}^{g'}\varphi$ est dans $L(\underline{C})$. Soit $r' \in C'$. Nous avons

$$r'\mu\Big(\sum_{g'} e_n(-a,g')X_{g',C} \cdot {}^{g'}\varphi\Big) = \Big(\sum_{g'} e_n(-a,g')^{r'}X_{g',C} \cdot {}^{r'+g'}\varphi\Big)/{}^{r'}R_C^{C'} =$$

$$= \mu\Big(\sum_{g'} e_n(-a,g')^{r'}X_{g',C} \cdot X_{r',C} \cdot {}^{r'+g'}\varphi\Big) = \mu\Big(\sum_{g'} e_n(-a,g')X_{r'+g',C} \cdot {}^{r'+g'}\varphi\Big) =$$

$$= e_n(a,g').\mu\Big(\sum_{g'} e_n(-a,g')X_{g',C} \cdot {}^{g'}\varphi\Big).$$ Ce qui montre, grâce à la proposition 4.4 que $\mu\Big(\sum_{g'} e_n(-a,g')X_{g',C} \cdot {}^{g'}\varphi\Big)$ est un multiple de $X_{a,C'}$. Il existe donc une constante $\lambda_a(\varphi)$ telle que la relation (4.21) soit vraie et il est clair que l'application λ_a est une forme linéaire sur $L(\underline{C})$. Pour étudier cette forme il suffit de connaître les constantes $\lambda_a(X_{b,C})$ puisque les fonctions $X_{b,C}$ engendrent $L(\underline{C})$. Nous avons

$$\lambda_a(X_{b,C})X_{a,C} \cdot {}^aR_C^{C'} = \sum_{g'} e_n(-a,g')X_{g',C} \cdot {}^{g'}X_{b,C'}$$

et nous en déduisons en utilisant (4.4)

$$\begin{aligned} \lambda_a(X_{b,C})X_{a,C} \cdot {}^aR_C^{C'} &= \Big(\sum_{g'} e_n(b-a,g')^b X_{g',C}\Big)X_{b,C} \\ &= \lambda_{a-b}(1)X_{a-b,C} \cdot X_{b,C} \cdot {}^aR_C^{C'} \\ &= \lambda_{a-b}(1).e_n(a-b,b)^{\frac{n+1}{2}} \cdot {}^aR_C^{C'} \cdot X_{a,C} \end{aligned}$$

et enfin,

$$\lambda_a(X_{b,C}) = e_n(a,b)^{\frac{n+1}{2}} \cdot \lambda_{a-b}(1) \ .$$

Posons $\varepsilon(r) = \lambda_r(1)$, ce qui donne

$$(4.25) \qquad \varepsilon(r)X_{r,C}.{}^{r}R_{C}^{C'} = \sum_{g'} e_n(-r,g')X_{g',C} \quad \text{pour tout } r \in E_n .$$

Supposons $r \in C$. Alors, $X_{r,C} = 1$ et $e_n(-r,g')X_{g',C} = {}^{r}X_{g',C}$. Il en résulte que $\varepsilon(r){}^{r}R_{C}^{C'} = \sum_{g'} {}^{r}X_{g',C} = {}^{r}R_{C}^{C'}$ et que $\varepsilon(r) = 1$ pour tout $r \in C$.

L'égalité (4.25) s'écrit aussi

$$\varepsilon(r)X_{r,C'} = \mu(\sum_{g'} e_n(-r,g')X_{g',C})$$

et nous venons de voir que l'image de l'espace vectoriel $L(\underline{C},\underline{C}')$ de dimension $n/d(C,C')$ par l'isomorphisme μ contient les $n/d(C,C')$ générateurs $X_{r,C'}$ de $L(\underline{C}',\underline{C})$. Par conséquent, $\mu(L(\underline{C},\underline{C}')) = L(\underline{C}',\underline{C})$. Il en résulte que $\varepsilon(r) = 0$ quand $r \in C'+C$ puisqu'alors $X_{r,C'}$ n'est pas dans $L(\underline{C}',\underline{C})$, d'après proposition 4.4. Enfin, si $r = \overline{r}' + \overline{r}$ avec $\overline{r} \in C$ et $\overline{r}' \in C'$, $\varepsilon(r)X_{r,C} = \sum_{g'} e_n(-\overline{r},g')X_{g',C} = \varepsilon(\overline{r})X_{\overline{r},C}$ et comme $X_{r,C} = e_n(\overline{r},r)^{\frac{n+1}{2}} X_{r,C}$ d'après (4.5), nous obtenons $\varepsilon(r).e_n(\overline{r},\overline{r}')^{\frac{n+1}{2}} = \varepsilon(\overline{r}) = 1$, ce qui prouve (4.23).

4.3 Les constantes $\delta(C_1,\ldots,C_r)$.

Soient $C_1,\ldots,C_r$ des sous-groupes cycliques d'ordre n de E_n. Posons

$$(4.26) \qquad d_{ij} = d(C_i,C_j) \quad \text{et} \quad R_i^j = R_{C_i}^{C_j}$$

Il résulte de la proposition 4.6 que la fonction $R_1^2.R_2^3\ldots R_{k-1}^k.R_k^1$ est une constante non nulle, pour tout k .

Définition 4.12 : Nous posons

$$(4.27) \qquad \delta(C_1,\ldots,C_r) = R_1^2.R_2^3\ldots R_{r-1}^r.R_r^1 \ .$$

Lemme 4.13 : Les formules suivantes permettent de calculer les constantes $\delta(C_1,\ldots,C_r)$ par récurrence :

(4.28) $$\delta(C_1) = n$$

(4.29) $$\delta(C_1,C_2) = n.d_{12}$$

(4.30) $$\delta(C_1,C_2,C_3) = n.\sum_{\substack{(x_1,x_2,x_3)\in C_1\times C_2\times C_3 \\ x_1+x_2+x_3=0}} e_n(x_3,x_1)^{\frac{n+1}{2}}$$

(4.31) $$\delta(C_1,\ldots,C_r) = \frac{\delta(C_1,C_2,C_3)\delta(C_1,C_3,C_4)\ldots\delta(C_1,C_{r-1},C_r)}{\delta(C_1,C_3)\ldots\delta(C_1,C_{r-1})}$$

Preuve : La relation (4.28) résulte de $R_1^1 = \sum_{g_1\in C_1} X_{g_1,C_1}$ et de $X_{g_1,C_1} = 1$ tandis que la relation (4.29) n'est autre que (4.12). Démontrons (4.30).

Nous avons $R_1^2E_2^3 = \sum_{\substack{g_2\in C_2 \\ g_3\in C_3}} X_{g_2,C_1}X_{g_3,C_2} = \sum_{g_2,g_3} \frac{R_1^2R_2^3}{g_{2_{R_1^2}}g_{3_{R_2^3}}} = \sum_{g_2,g_3} \frac{R_1^2\,R_2^3}{g_{3_{R_2^3}}}$

$= \sum_{g_2,g_3} \frac{R_1^2R_2^3}{g_{3_{(R_1^2R_2^3)}}} g_{3_{R_1^2}}$ d'après (4.17). Mais $R_1^2R_2^3$ est égal à un multiple de R_1^3 donc $\frac{R_1^2R_2^3}{g_{3_{(R_1^2R_2^3)}}} = X_{g_3,C_1}$ et $R_1^2R_2^3 = \sum_{g_3} X_{g_3,C_1}\, g_{3_{R_1^2}}$.

Si nous reprenons la formule (4.22) avec $C = C_1$, $C' = C_3$ et $a = 0$, nous obtenons

(4.31) $$R_1^2R_2^3 = \lambda_o(R_1^2)R_1^3$$

En multipliant les deux membres de cette égalité par R_3^1 et en utilisant (4.12) nous obtenons

$$R_1^2R_2^3R_3^1 = n.d_{13}\lambda_o(R_1^2) = \delta(C_1,C_2,C_3) .$$

Mais d'après le théorème 4.11, $\lambda_o(X_{g_2,C_1}) = 0$ quand $g_2 \notin C_1 + C_3$ .Donc,

$$\lambda_o(R_1^2) = \sum_{g_2\in C_2\cap(C_1+C_3)} \lambda_o(X_{g_2,C_1}) .$$

Posons

$$(4.32)\qquad C_{123} = \{(x_1,x_2,x_3)\in C_1\times C_2\times C_3 \mid x_1+x_2+x_3 = 0\}\ .$$

La suite de groupe

$$(4.33)\qquad 0\longrightarrow C_1\cap C_2 \xrightarrow{p} C_{123} \xrightarrow{q} C_2\cap(C_1+C_3) \longrightarrow 0$$

où les homomorphismes p et q sont définis par

$$p(x) = (x,0,-x) \qquad \text{et} \qquad q(x_1,x_2,x_3) = x_2$$

est exacte d'après le théorème 4.11. Si $g_2\in C_2\cap(C_1+C_3)$ désigne l'image par q de (x_1,x_2,x_3) nous avons $\lambda_o(X_{g_2,C_1}) = e_n(x_3,x_1)^{\frac{n+1}{2}}$ et comme g_2 est image de d_{13} éléments de C_{123}, nous obtenons

$$d_{13}\lambda_o(X_{g_2,C_1}) = \sum_{\substack{x\in C_{123}\\ q(x)=g_2}} e_n(x_3,x_1)^{\frac{n+1}{2}} \quad \text{et} \quad d_{13}\lambda_o(R_1^2) = \sum_{x\in C_{123}} e_n(x_3,x_1)^{\frac{n+1}{2}}.$$

qui n'est autre que (4.30). Enfin l'égalité (4.31) modifiée grâce à (4.12) en $R_1^2R_2^3 = \dfrac{\delta(C_1,C_2,C_3)}{\delta(C_1,C_3)}R_1^3$ donne par récurrence

$$(4.34)\qquad R_1^2\ldots.R_{r-1}^r = \frac{\delta(C_1,C_2,C_3)\ldots.\delta(C_1,C_{R-1},C_r)}{\delta(C_1,C_3)\ldots.\delta(C_1,C_r)}R_1^r$$

et en multipliant les deux membres de cette égalité par R_r^1 nous obtenons (4.31).

Nous déduisons immédiatement du lemme 4.13

Corollaire 4.14 : Soit F le corps premier contenu dans k. Alors la constante $\delta(C_1,\ldots,C_r)$ est dans $F(\mu_n)$.

En fait les constantes $\delta(C_1,\ldots,C_r)$ sont des "sommes de Gauss," en effet,

Proposition 4.15 : Soit $\chi : (Z/4Z)^\times \longrightarrow \{\pm 1\}$ le caractère quadratique défini par $\chi(x) = (-1)^{\frac{x-1}{2}}$. Alors

(4.35) $\delta(C_1,\ldots,C_r)^2 = \chi(\frac{n^r}{d_{12}d_{23}\cdots d_{r1}}).d_{12}.d_{23}\cdots d_{r1}.n^r$ et

(4.36) $\delta(C_1,\ldots,C_r).\delta(C_r,\ldots,C_1) = d_{12}.d_{23}\cdots d_{r1}.n^r$

Preuve : La relation (4.36) s'obtient sans peine en multipliant membre à membre (4.27) et $\delta(C_r,\ldots,c_1) = R_2^1R_3^2\ldots R_1^r$ et en utilisant (4.12). Il résulte immédiatement de (4.28) et (4.29) que la relation (4.35) est vraie pour r = 1 et 2. D'autre part, grâce à (4.35) elle est vraie aussi pour r > 3 si elle est vraie pour r = 3, il suffit donc de démontrer (4.36) avec r = 3.

Rappelons que le groupe C_{123} a été défini en (4.32). Notons $\varepsilon : C_{123} \longrightarrow \mu_n$ l'application définie par

$$\varepsilon(x_1,x_2,x_3) = e_n(x_3,x_1)^{\frac{n+1}{2}}$$

C'est une forme quadratique sur C_{123} et

$$\delta(C_1,C_2,C_3) = n \sum_{x\in C_{123}} \varepsilon(x) \qquad \text{d'après (4.30).}$$

Remarquons au passage que la constante $\delta(C_1,\ldots,C_r)$ est par définition, invariante par permutation circulaire sur les groupes $C_1,C_2,\ldots,C_r$ ce qui se voit mal sur la relation (4.31). Par contre, il est aisé de voir directement que (4.30) est invariante par permutation circulaire sur C_1,C_2,C_3. En effet, si $x = (x_1,x_2,x_3)$ est dans C_{123} nous avons $x_1+x_2+x_3 = 0$ et $e_n(x_3,x_1+x_2+x_3) = 1$ d'où nous déduisons $e_n(x_3,x_1) = e_n(x_2,x_3)$ et

$\varepsilon(x_1,x_2,x_3) = \varepsilon(x_2,x_3,x_1) = \varepsilon(x_3,x_1,x_2)$, ce qui montre que la forme quadratique ε est invariante par permutation circulaire. Par contre, comme $\varepsilon(x_3,x_2,x_1) = \varepsilon(x_1,x_2,x_3)^{-1}$ nous voyons que ε se change en son inverse par une transposition des variables. En résumé, si $\sigma \in \mathfrak{S}_3$ opère sur C_{123} par ${}^{\sigma}(x_1,x_2,x_3) = (x_{\sigma(1)},x_{\sigma(2)},x_{\sigma(3)})$ et admet $sg(\sigma)$ pour signature, nous avons

(4.37) $$\varepsilon({}^{\sigma}x) = \varepsilon(x)^{sg(\sigma)}$$

Lemme 4.16 : i) Soit $d = \#(C_1 \cap C_2 \cap C_3)$. Alors,

$$d = (d_{12}, d_{23}) = (d_{23}, d_{31}) = (d_{31}, d_{12}) \tag{4.38}$$

ii) Posons $d_{ij} = d.d'_{ij}$. Le nombre $d.d'_{12}.d'_{23}.d'_{31}$, divise n, la forme ε prend ses valeurs dans $\mu_{d''}$ avec $d'' = \dfrac{n}{d.d'_{12}.d'_{23}.d'_{31}}$ et

$$C_1 \cap (C_2 + C_3) = d'_{32} C_1$$

$$C_2 \cap (C_3 + C_1) = d'_{13} C_2$$

$$C_3 \cap (C_1 + C_2) = d'_{21} C_3 \quad .$$

iii) Il existe $x = (x_1, x_2, x_3) \in C_{123}$ tel que x_2 engendre $C_2 \cap (C_1 + C_3)$ et alors $\varepsilon(x)$ engendre $\mu_{d''}$.

Preuve : i) Montrons par exemple que $d = (d_{12}, d_{23})$. Les groupes C_1, C_2 et C_3 sont cycliques ainsi que leurs sous-groupes. Comme $C_1 \cap C_2$ est d'ordre d_{12} nous avons $C_1 \cap C_2 = (n/d_{12})C_2$. De même, nous avons $C_3 \cap C_2 = (n/d_{23})C_2$. Il en résulte que $C_1 \cap C_2 \cap C_3 = \text{P.P.C.M.}(n/d_{12}, n/d_{23})C_2$ où P.P.C.M. désigne le plus petit commun multiple. Ce qui nous donne $C_1 \cap C_2 \cap C_3 = \dfrac{n}{(d_{12}, d_{23})} C_2$ et comme $C_1 \cap C_2 \cap C_3 = (n/d)C_2$ nous avons bien $d = (d_{12}, d_{23})$.

ii) Les trois nombres d_{ij} divisent n. Il en est de même de leur P.P.C.M. qui n'est autre que $d.d'_{12}.d'_{23}.d'_{31}$. Considérons la suite de groupes

$$0 \longrightarrow C_1 \cap C_2 \cap C_3 \longrightarrow E_n \xrightarrow{\varphi} \mathrm{Hom}(C_1 + C_2 + C_3, \mu_n) \longrightarrow 0$$

où φ est l'homomorphisme $g \longmapsto \chi_g$ (avec les notations habituelles). D'après le théorème 1.8, φ est surjectif et il est clair que $C_1 \cap C_2 \cap C_3$ est son noyau. Par conséquent cette suite est exacte et

$$\#(C_1 + C_2 + C_3) = n^2/d$$

D'autre part, la suite exacte de groupes

$$0 \longrightarrow C_{123} \longrightarrow C_1 \times C_2 \times C_3 \xrightarrow{s} C_1 + C_2 + C_3 \longrightarrow 0$$

où $s(x_1,x_2,x_3) = x_1+x_2+x_3$ montre que $\# C_{123} = n.d.$ Enfin, la suite exacte (4.33) donne $\# C_2 \cap (C_1 + C_3) = nd/d_{13} = n/d'_{13}$. Mais, $C_2 \cap (C_1 + C_3)$ est un sous-groupe cyclique de C_2 donc $C_2 \cap (C_1 + C_3) = d'_{13}C_2$.
Enfin, quand g_1 parcourt C_1 et g_2 parcourt C_2, le nombre $e_n(g_1,g_2)^{\frac{n+1}{2}}$ parcourt $\mu_{n/d_{12}}$ et avec ce que nous venons de voir nous obtenons que $\varepsilon(x)$ est dans $(\mu_{n/d_{12}})^{d'_{13}d'_{23}} = \mu_{d''}$ quand x parcourt C_{123}.
iii) Soit (g_3,g) une base de E_n telle que g_3 soit un générateur de C_3. Alors, $e_n(g_3,g)$ engendre μ_n et il existe a_1,a_2,b_1,b_2 dans $\mathbb{Z}/n\mathbb{Z}$ tels que

$$g_1 = a_1 g + b_1 g_3$$
$$g_2 = a_2 g + b_2 g_3 \ .$$

Comme $e_n(g_3,g_1) = e_n(g_3,g)^{a_1}$ engendre $\mu_{n/d_{13}}$ nous avons $d_{13} = (a_1,n)$. De même, $d_{23} = (a_2,n)$. Quitte à remplacer g_1 et g_2 par d'autres générateurs de C_1 et C_2 nous pouvons supposer que $a_1 = d_{13}$ et $a_1 = d_{23}$.

Alors $d'_{23}g_1 - d'_{13}g_2 + (b_2d'_{13} - b_1d'_{23})g_3 = 0$ et
$x = (x_1,x_2,x_3) = (d'_{23}g_1 \ , \ - d'_{13}g_2, (b_2d'_{13} - b_1d'_{23})g_3)$ est l'élément de C_{123} dont l'existence est affirmée dans le lemme 4.16.

Nous pouvons terminer la démonstration de la proposition 4.15. Soit $x \in C_{123}$ satisfaisant aux conditions iii) du lemme 4.16. D'après tout ce qui précède $\delta(C_1,C_2,C_3) = n.d_{13} \sum_{r \bmod n/d'_{13}} \varepsilon(rx) = n.d_{13} \sum_{r \bmod n/d'_{13}} \varepsilon(x)^r$
Mais l'application $r \longmapsto \varepsilon(x)^{r^2}$ est périodique de période d" et par conséquent

$$\delta(C_1,C_2,C_3) = n.d^2.d'_{12}.d'_{23}.d'_{31} \sum_{r \bmod d''} \varepsilon(x)^{r^2} \tag{4.39}$$

Or il est bien connu [Ei] que

Théorème 4.17 : Soit A un entier positif impair. A tout générateur ζ de μ_A on associe

$$S(\zeta) = \sum_{r \bmod A} \zeta^{r^2}$$

Alors,

$$S(\zeta)^2 = \chi(A).A$$ où χ est le caractère quadratique défini dans l'énoncé de la proposition 4.15 .

Il résulte de ce théorème et de (4.39) que

$$\delta(C_1,C_2,C_3)^2 = \chi(d'').d_{12}.d_{23}.d_{31}.n^3$$ et comme χ est un caractère nous avons $\chi(d'') = \chi[(\frac{n}{d})^2 d'']$ $= \chi(\frac{n^3}{d_{12}d_{23}d_{31}}) = \chi(\frac{n}{d_{12}})\chi(\frac{n}{d_{23}})\chi(\frac{n}{d_{31}})$ ce qui prouve la relation (4.35).

CHAPITRE 5

Etude du plongement de E dans $\mathbb{P}^{n-1}$ associé à une structure de niveau n

Nous supposons dans ce chapitre la courbe elliptique E définie sur un corps k de caractéristique différente de n, munie d'un sous-groupe cyclique C d'ordre n globalement rationnel et d'un point g' primitif d'ordre n rationnel. Nous désignons par C' le groupe engendré g' et nous supposons

$$C \cap C' = \{0\}$$

Avec cette hypothèse le groupe C est isomorphe, en tant que module galoisien, à μ_n. Nous avons de plus un isomorphisme canonique qui associe à $\zeta \in \mu_n$ l'unique élément g_ζ de C tel que

$$e_n(g', g_\zeta) = \zeta \ .$$

Pour alléger l'écriture nous posons pour tout $r \in \mathbb{Z}/n\mathbb{Z}$,

$$X_r = X_{rg',C}$$

où $X_{rg',C}$ est la fonction définie en (4.1) et $\chi_r = \chi_{rg'} \in \mathrm{Hom}(C,\mu_n)$ où $\chi_{rg'}$ est le caractère défini en (3.2).

Lemme 5.1 : Les n fonctions X_r sont définies sur k et forment une base du k-espace vectoriel $L(\underline{C})$.

Preuve : L'hypothèse sur le couple (g',C) fait que χ_1 est un générateur de $\mathrm{Hom}(C,\mu_n)$. Par conséquent, $\chi_r = \chi_1^r$ parcourt $\mathrm{Hom}(C,\mu_n)$ quand r parcourt $\mathbb{Z}/n\mathbb{Z}$. Il en résulte, d'après la proposition 3.1 que les n fonctions X_r forment une base du $k(\mu_n)$-espace vectoriel $k(\mu_n) \otimes_k L(\underline{C})$. Enfin, comme $\mathrm{div}\, X_r$ est stable par l'action de Γ, la

fonction X_r est égale à un multiple constant près à une fonction définie sur k et la relation (4.3) montre qu'en fait X_r est définie sur k. Le lemme en résulte.

Nous avons vu au chapitre 2 qu'un plongement de E dans $\mathbb{P}(L(\underline{C}))$ est associé au diviseur $\underline{C}$. Les fonctions X_r formant une base de $L(\underline{C})$ nous en déduisons un plongement de E dans $\mathbb{P}_k^{n-1}$. Plus précisément

Définition 5.2 : Nous notons π le plongement projectif de E dans $\mathbb{P}_k^{n-1}$ défini sur E - C par

$$\pi(P) = (X_o(P) : X_1(P) : \quad : X_{n-1}(P))$$

où P désigne un point courant de E. Comme $X_o(P) = 1$ pour tout point $P \in E - C$ et comme les fonctions X_r ont un pôle en chaque point de C pour $r \neq 0$, nous voyons que $\pi(C)$ est l'intersection de $\pi(E)$ avec l'hyperplan d'équation $X_o = 0$.

Définition 5.3 : Soit $u \in E_n$. Nous lui associons les éléments $r_u \in \mathbb{Z}/n\mathbb{Z}$ et $\zeta_u \in \mu_n$ uniquement définis par

$$\chi_1^{r_u} = \chi_u \quad \text{et} \quad \zeta_u = e_n(g', u) .$$

Théorème 5.4 : Soit $P \in E$ tel que $\pi(P) = (\alpha_o : \alpha_1 : \ )$ dans $\mathbb{P}^{n-1}$ et soit $u \in E_n$. Posons

$$\alpha'_i = \zeta_u^{-i} \alpha_{i-r_u} \tag{5.1}$$

Alors $\pi(P+u) = (\alpha'_o : \alpha'_1 : \ ) \in \mathbb{P}^{n-1}$, et en posant

$$\alpha''_i = \zeta_u^{-i} \alpha_{-i+r_u} \tag{5.2}$$

nous avons $\pi(-P+u) = (\alpha''_o : \alpha''_1 : \ ) \in \mathbb{P}^{n-1}$.

Preuve : Comme $v = u - r_u g'$ est dans C puisque $e_n(g,v) = 1$ pour tout $g \in C$, il résulte de la formule (4.6) et de la proposition 4.4 que

$$X_i(P+u) = X_i(P + r_u g' + v) = \zeta_u^{-i} \frac{X_{i-r_u}(P)}{X_{-r_u}(P)}$$

d'où

$$\alpha'_i = \zeta_u^{-i} \alpha_{i-r_u} \quad .$$

Quand u = 0 la relation (5.2) résulte de (4.7). Combinée avec (5.1) on obtient le cas général.

Définition 5.5 : Soit T une fonction définie sur k ayant un zéro simple en 0. Nous notons a le point de $\mathbb{P}_k^{n-1}$ défini par $a = (a_0 : a_1 : \quad)$ avec

$$a_i = X_i.T(0) \tag{5.3}$$

Lorsqu'il faudra précisé nous écrirons

$$a_i = a_{ig',C} \quad .$$

Nous voyons immédiatement que a ne dépend pas du choix de T, et que

$$a_{-i} = -a_i \neq o \quad \text{pour } i \neq o \tag{5.4}$$
$$a_o = 0$$

Théorème 5.7 :

i) Soit $r \neq 0$ nous avons

$$X_i(rg') = \frac{a_{i-r}}{a_{-r}} \tag{5.5}$$

ii) Soit $u \in E_n$, nous avons

$$\pi(u) = (\alpha_o : \alpha_1 : \quad)$$

avec

$$\alpha_i = \zeta_u^{-i} a_{i-r_u} \quad . \tag{5.6}$$

Preuve : La formule (5.5) résulte de (4.6). La définition (5.6) donne immédiatement $\pi(0) = a$ et il suffit d'appliquer (5.1) pour obtenir (5.6).

Remarque : Nous verrons ultérieurement que $\frac{1}{a_i}$ pour $i \neq 0$ est une forme modulaire de poids 1 pour $\Gamma(n)$.

5.3 Les équations de $\pi(E)$

Proposition 5.8 : Soient i_1,j_1,i_2,j_2,i_3,j_3 dans $\mathbb{Z}/n\mathbb{Z}$ tels que $i_1 + j_1 = i_2 + j_2 = i_3 + j_3$ alors

$$(5.7) \qquad a_{i_3-i_2}\, a_{j_3-i_2}\, X_{i_1} X_{j_1} + a_{i_1-i_3}\, a_{j_1-i_3}\, X_{i_2} X_{j_2} + a_{i_2-i_1}\, a_{j_2-i_1}\, X_{i_3} X_{j_3} = 0$$

Preuve : Si deux des ensembles $\{i_1,j_1\}$, $\{i_2,j_2\}$, $\{i_3,j_3\}$ sont égaux le membre de gauche de (5.7) est identiquement nul (en tant que polynôme dans les variables X_i) . Dans le cas contraire, le membre de gauche de (5.7) est une fonction qui possède au plus 2n pôles et qui s'annule en 3n points (les translatés des points de C par $i_{1g'}$, $i_{2g'}$ et $i_{3g'}$). Par conséquent elle est nulle.

Corollaire 5.9 : Si $n > 3$, la variété $\pi(E)$ est l'intersection schématique des quadriques de $\mathbb{P}_k^{n-1}$ définies par les équations (5.7).

Preuve : Ce corollaire résulte immédiatement du théorème 3.9 et du corollaire 3.8.

Corollaire 5.10 : Sous les hypothèses de la proposition 5.8 nous avons

$$(5.8) \qquad a_{i_3-i_2}\, a_{j_3-i_2}\, a_{i_1}\, a_{j_1} + a_{i_1-i_3}\, a_{j_1-i_3}\, a_{i_2}\, a_{j_2} + a_{i_2-i_1}\, a_{j_2-i_1}\, a_{i_3}\, a_{j_3} = 0$$

Preuve : Cette relation traduit le fait que $\pi(0) \in \pi(E)$.

Proposition 5.11 : Supposons $n = 3$. Alors les fonctions X_o, X_1, X_2 sont liées par la relation

$$(5.9) \qquad X_o^3 + X_1^3 + X_2^3 + 3(R_C^{C'}(0) - 1)X_o X_1 X_2 = 0$$

où $R_C^{C'}$ est la fonction définie par (4.10) et $\pi(E)$ est la courbe de $\mathbb{P}_k^2$ qui admet (5.9) pour équation.

Preuve : Soient b et b' les constantes telles que

$$X_1 = \frac{a_1}{T} + a_1 b + \ldots \qquad X_2 = \frac{-a_1}{T} + a_1 b' + \ldots$$

les fonctions X_o^3, X_1^3, X_2^3, $X_o X_1 X_2$ sont linéairement dépendantes d'après le théorème 3.11. Il suffit d'écrire le développement de ces fonctions en T pour obtenir (5.9). La dernière affirmation résulte des théorèmes 3.11 et 3.12.

Remarque : Nous pouvons encore écrire l'équation (5.9) sous la forme

$$(X_o + X_1 + X_2)(X_o + \zeta X_1 + \zeta^2 X_2)(X_o + \zeta^2 X_1 + \zeta X_2)$$
$$= -3\, R_C^{C'}(0)\, X_o X_1 X_2$$

soit encore, compte-tenu de (4.22)

$$R_C^{C',3} \prod_{c \in C} X_{c,C'} = -3\, R_C^{C'}(0) \prod_{c' \in C'} X_{c',C} \cdot$$

5.4 La loi de groupe

Lemme 5.12 : Soit $\varphi \in L(2\underline{C}, \chi_r)$ non nulle, telle que $\varphi(P) = 0$. Alors

$$\text{(5.10)} \qquad \text{div } \varphi = P_{\underline{C}} + {}^{-P+rg'}\underline{C} - 2\underline{C}$$

Preuve : Pour simplifier posons ${}^s\Psi = {}^{sg'}\Psi$ pour toute fonction Ψ et tout $s \in \mathbb{Z}/n\mathbb{Z}$. La fonction $X^2_{-r/2} \cdot ({}^{-r/2}\varphi)$ est dans $L(2\underline{C}, \chi_o)$. Or toutes les fonctions de cet espace sont paires puisqu'il a pour base X_o^2 et $X_s X_{-s}$ avec $s \neq o$. A toute fonction Ψ nous associons la fonction Ψ' définie par $\Psi'(x) = \Psi(-x)$. Nous avons

$$X^2_{-r/2} \cdot ({}^{-r/2}\varphi) = (X^2_{-r/2} \cdot ({}^{-r/2}\varphi))' = X^2_{r/2} \cdot ({}^{r/2}(\varphi')) \quad \text{donc}$$
$$-r/2\varphi = \frac{X^2_{r/2}}{X^2_{-r/2}} \cdot {}^{r/2}(\varphi')$$

ce qui donne après translation par $\frac{r}{2}g'$ l'équation fonctionnelle $\varphi = X^2_r({}^r(\varphi))$ soit encore

$$\varphi(x) = X_r^2(x)\ \varphi(-x+rg')$$

pour tout point $x \in E$.

Par conséquent, si Q est un zéro de φ il en est de même de $-Q+rg'$. Enfin, le diviseur de φ étant invariant par translation par les éléments de C nous avons la relation (5.10).

Théorème 5.13 : Soit $P \in E-C$. Posons $\alpha_r = X_r(P)$ (donc $\alpha_o \neq 0$). Soient $i_1,j_1,i_2,j_2,u_1,v_1,u_2,v_2$, r et s dans $\mathbb{Z}/n\mathbb{Z}$ tels que

$$i_1 + j_1 = i_2 + j_2 = s$$

$$u_1 + v_1 = u_2 + v_2 = r + s$$

(5.11)
$$\{i_1,j_1\} \neq \{i_2,j_2\}$$

$$\{u_1,v_1\} \neq \{u_2,v_2\}$$

$$\alpha_{-r-s} \neq 0$$

Alors

(5.12) $X_r(x+P) =$

$$\frac{a_{u_2-u_1}\, a_{v_2-u_1}}{a_{j_2-i_1}\, a_{i_2-i_1}} \cdot \alpha_o \cdot \frac{\alpha_{-i_1}\alpha_{-j_1} X_{i_2+r}(x)X_{j_2+r}(x) - \alpha_{-i_2}\alpha_{-j_2} X_{i_1+r}(x)X_{j_1+r}(x)}{\alpha_{-u_1}\alpha_{-v_1} X_{u_2}(x)X_{v_2}(x) - \alpha_{-u_2}\alpha_{-v_2} X_{u_1}(x)\, X_{v_1}(x)}$$

pour tout $x \in E$.

Preuve : Posons $N = \alpha_{-i_1}\alpha_{-j_1} X_{i_2+r}X_{j_2+r} - \alpha_{-i_2}\alpha_{-j_2} X_{i_1+r}X_{j_1+r}$ et

$D = \alpha_{-u_1}\alpha_{-v_1} X_{u_2}X_{v_2} - \alpha_{-u_2}\alpha_{-v_2} X_{u_1}X_{v_1}$. La fonction N n'est pas identiquement nulle. En effet comme les fonctions $X_{i_2+r}X_{j_2+r}$ et $X_{i_1+r}X_{j_1+r}$ sont linéairement indépendants, pour que N soit nulle il

faudrait avoir

$$\alpha_{-i_1}\alpha_{-j_1} = \alpha_{-i_2}\alpha_{-j_2} = 0.$$

Si α_{-i_1} était nulle par exemple, le point P serait le translaté par un élément de C de $-i_1 g'$ et par conséquent $\alpha_{-i_2}\alpha_{-j_2} \neq 0$. Donc $N \neq 0$.

De plus, d'après (5.2) nous avons $N(-P + rg') = 0$ et comme $N \in L(2\underline{C}, \chi_{s+2r})$ le lemme 5.12 montre que

$$\operatorname{div} N = {}^{-P+r}\underline{C} + {}^{P+r+s}\underline{C} - 2\underline{C}$$

De même nous voyons que $D \neq 0$ et que

$$\operatorname{div} D = {}^{-P}\underline{C} + {}^{P+r+s}\underline{C} - 2\underline{C}$$

Par conséquent

$$\operatorname{div}\frac{N}{D} = {}^{-P+r}\underline{C} - {}^{-P}\underline{C} = \operatorname{div} X_r(x+P) .$$

Si $\alpha_o \neq 0$ le point P n'appartient pas à C et 0 n'est pas un pôle de $\frac{N}{D}$. Par conséquent

$$\frac{N}{D}(0) = \frac{\alpha_{-i_1}\alpha_{-j_1} a_{i_2+r} a_{j_2+r} - \alpha_{-i_2}\alpha_{-j_2} a_{i_1+r} a_{j_1+r}}{\alpha_{-u_1}\alpha_{-v_1} a_{u_2} a_{v_2} - \alpha_{-u_2}\alpha_{-v_2} a_{u_1} a_{v_1}}$$

Mais les relations (5.7) montrent que le numérateur de l'expression précédente est égal à $a_{i_2-i_1} a_{j_2-i_1} \alpha_r \alpha_{-r-s}$ tandis que le dénominateur est égal à $a_{u_2-u_1} a_{v_2-u_1} \alpha_o \alpha_{-r-s}$. Par conséquent,

$$\frac{N}{D}(0) = \frac{\alpha_r}{\alpha_o} \cdot \frac{a_{i_2-i_1} a_{j_2-i_1}}{a_{u_2-u_1} a_{v_2-u_1}}$$

et comme $X_{r(x+P)(o)} = \alpha_r$ nous obtenons (5.12).

Corollaire 5.14 : Avec les notations et les hypothèses du théorème 5.13, si $r \in (\mathbb{Z}/n\mathbb{Z}) - \{0\}$ nous avons

$$X_r(x+P) = \alpha_o \frac{\alpha_{r/2}^2 X_o X_r - \alpha_o \alpha_r X_{r/2}^2}{\alpha_o^2 X_{r/2} X_{-r/2} - \alpha_{r/2}\alpha_{-r/2} X_o^2} \tag{5.13}$$

Preuve Il suffit d'écrire (5.12) avec $i_1 = u_1 = v_1 = 0$, $j_1 = -r$, $i_2 = j_2 = v_2 = -r/2$, $u_2 = r/2$.

5.5 Les dérivations invariantes

Rappelons qu'il existe une dérivation D non nulle sur le corps des fonctions de E, définie à un multiple constant près par l'une des deux propriétés

i) Propriété d'invariance par translation

$$D(\Psi(x+P)) = D\Psi(x+P)$$

pour toute fonction Ψ, tout point P de E ; x désignant un point courant de E.

ii) Si $P \in E$ est tel que $v_p(\Psi) < 0$ alors $v_p(D\Psi) = v_p(\Psi) - 1$.

Si $P \in E$ est tel que $v_p(\Psi) \geq 0$ alors $v_p(D\Psi) \geq 0$.

Une telle dérivation s'appelle une dérivation invariante sur E .

Théorème 5.15 : Soit D une dérivation invariante sur E et T une fonction sur E ayant un zéro simple en O. Posons

$$DT = \alpha + \beta T + o(T)$$

et pour tout $r \neq 0$

$$X_r = \frac{a_r}{T}(1 + b_r T + o(T)) \tag{5.14}$$

Alors

$$DX_r = \alpha(2b_{r/2}X_oX_r - \frac{a_r}{a_{r/2}^2}X_{r/2}^2) - \beta X_o X_r \tag{5.15}$$

Preuve : Les deux propriétés de la dérivation D rappelées au début de ce paragraphe font que

$$DX_r \in L(2\underline{C}, \chi_r)$$

Comme cet espace admet X_oX_r et $X_{r/2}^2$ comme base (quand $r \neq o$) il existe des constantes λ et μ telles que

$$DX_r = \lambda X_o X_r + \mu X_{r/2}^2$$

Or $DX_r = (-\frac{a_r}{T^2} + o(\frac{1}{T}))DT$ et $\lambda X_oX_r + \mu X_{r/2}^2 = \mu \frac{a_{r/2}^2}{T^2} + \frac{2\mu\, a_{r/2}^2 b_{r/2} + \lambda a_r}{T}$

$+ o(\frac{1}{T})$ d'où $\mu.a_{r/2}^2 = -a_r$ et $\lambda a_r + 2\mu a_{r/2}^2 b_{r/2} = o$ ce qui démontre le théorème .

Remarques : La dérivation D étant choisie les quantités $-\frac{\alpha a_r}{a_{r/2}^2}$ et $2\alpha b_{r/2} - \beta$ ne dépendent pas du choix de T. En caractéristique 2 nous avons

$$DX_r = -\beta X_o X_r - \frac{a_r}{a_{r/2}^2} X_{r/2}^2$$

et le coefficient $-\beta$ de X_oX_r ne dépend que de la normalisation de D, mais pas du choix de T, ni de r.

En caractéristique $\neq 2$ nous pouvons choisir T pour que $\alpha = 1$ et $\beta = 0$ (en prenant pour T une fonction impaire par exemple). Dans ce cas, les constantes a_r et b_r ne dépendent plus du choix de T, nous avons

$$DX_r = 2b_{r/2} X_oX_r - \frac{a_r}{a_{r/2}^2} X_{r/2}^2$$

et $b_r = -b_{-r}$, $a_{-r} = -a_r$.

Proposition 5.16 : Si $r \in (\mathbb{Z}/n\mathbb{Z})^x$ nous avons

$$(5.16)\quad n(b_r - b_{-r}) = 2\,\frac{a_{2r}}{a_r^2}\Big[\sum_{i=1}^{(n-3)/2} \frac{a_{2ir}^2}{a_{2ir-r}a_{2ir+r}}\Big] + \frac{a_{2r}^3}{a_r^3 a_{3r}} + \frac{a_r a_{4r}}{a_{2r}^2 a_{3r}} .$$

Preuve : Il suffit de démontrer (5.16) pour r = 1, les calculs étant les mêmes dans le cas général à condition de multiplier tous les indices par r.

Posons, pour tout t, tel que $1 \le t \le n-1$

$$S_t = \frac{X_1^t X_{-t} + X_{-1}^t X_t}{a_t}$$

et pour tout t tel que $2 \le t \le n-2$

$$c_t = \frac{a_t^2}{a_{t-1}a_{t+1}}$$

Lemme 5.17 : Pour $2 \le t \le n-2$ nous avons

$$(5.17)\qquad S_{t+1} = \frac{a_2}{a_1} c_t X_o S_t - X_1 X_{-1} S_{t-1}$$

Preuve : Les formules (5.7) donnent

$$X_{-1}X_{-t+1} = \frac{a_2 a_t}{a_1 a_{t+1}} X_o X_{-t} - \frac{a_{t-1}}{a_{t+1}} X_1 X_{-t-1}$$

$$X_1 X_{t-1} = \frac{a_2 a_t}{a_1 a_{t+1}} X_o X_t - \frac{a_{t-1}}{a_{t+1}} X_{-1} X_{t+1}$$

en substituant dans

$$X_1 X_{-1} S_{t-1} = \frac{X_1^t X_{-1} X_{-t+1} + X_{-1}^t X_1 X_{t-1}}{a_{t-1}}$$

nous trouvons (5.17) sans difficulté.

Lemme 5.18 : Soit u tel que $1 \le u \le \frac{n-1}{2}$. Il existe des constantes $\lambda_o^{(u)}, \lambda_1^{(u)}, \ldots, \lambda_u^{(u)}$ et $\mu_o^{(u)}, \mu_1^{(u)}, \ldots, \mu_u^{(u)}$ telles que

$$S_{2n} = \sum_{i=0}^{u} \lambda_i^{(u)} X_o^{2u+1-2i} (X_1 X_{-1})^i$$

(5.18)

$$S_{2n-1} = \sum_{i=0}^{u} \mu_i^{(u)} X_o^{2u-2i} (X_1 X_{-1})^i$$

Preuve : Grace à la formule de récurrence (5.17) il suffit de prouver (5.18) pour S_1 et S_2 .

Nous avons $S_1 = \frac{X_1 X_{-1} + X_{-1} X_1}{a_1} = \frac{2}{a_1} X_1 X_{-1}$ et $S_2 = \frac{X_1^2 X_{-2} + X_{-1}^2 X_2}{a_2}$.

Les formules (5.7) nous donnent successivement :

$$A = -a_2^2 X_{-1} X_1 + a_1 a_3 X_o^2 + a_1^2 X_{-2} X_2 = 0$$

$$B = a_1^2 X_1 X_{-3} + a_3 a_1 X_{-1}^2 - a_2^2 X_o X_{-2} = 0$$

$$C = -a_2 a_1 X_{-3} X_2 - a_4 a_1 X_{-1} X_o + a_2 a_3 X_1 X_{-2} = 0$$

Calculons $D = a_2^3 X_o A + a_1^2 a_2 X_2 B + a_1^3 X_1 C$. Nous avons

$$D = -(a_2^5 + a_4 a_1^4) X_o X_1 X_{-1} + a_2^3 a_1 a_3 X_o^3 + a_2 a_3 a_1^3 X_{-1}^2 X_2 + a_2 a_3 a_1^3 X_1^2 X_{-2} = 0$$

d'où

$$S_2 = -\frac{a_2}{a_1^2} X_o^3 + \frac{a_2^5 + a_1^4 a_4}{a_1^3 a_2^2 a_3} X_o X_1 X_{-1}$$

Nous avons donc démontré le lemme 5.18 et trouvé

(5.19)

$$\mu_o^{(1)} = 0 \qquad \mu_1^{(1)} = \frac{2}{a_1}$$

$$\lambda_o^{(1)} = -\frac{a_2}{a_1^2} \qquad \lambda_1^{(1)} = \frac{a_2^5 + a_1^4 a_4}{a_1^3 a_2^2 a_3}$$

En posant $t = 2u$ dans (5.17) et en substituant (5.18) nous obtenons

$$\mu_{u+1}^{(u+1)} = - \mu_u^{(u)}$$

d'où $\mu_u^{(u)} = (-1)^{u-1} \mu_1^{(1)}$ et

$$\mu_u^{(u)} = (-1)^{u-1} \frac{2}{a_1} \quad . \tag{5.20}$$

De même, en posant $t = 2n+1$ dans (5.17) et en substituant (5.18) nous obtenons

$$\lambda_{u+1}^{(u+1)} = \frac{a_2}{a_1} c_{2u+1} \mu_{u+1}^{(u+1)} - \lambda_u^{(u)}$$

soit, compte tenu de (5.20) ,

$$(-1)^{u+1} \lambda_{u+1}^{(u+1)} = - 2 \frac{a_2}{a_1^2} c_{2u+1} + (-1)^u \lambda_u^{(u)} \tag{5.21}$$

d'où nous déduisons

$$(-1)^u \lambda_u^{(u)} = - 2 \frac{a_2}{a_1^2} \left[c_3 + c_5 + \ldots + c_{2u-1} \right] - \lambda_1^{(1)} \quad . \tag{5.22}$$

Comme $c_t = c_{n-t}$ nous obtenons

$$(-1)^{\frac{n-1}{2}} \lambda_{\frac{n-1}{2}}^{(\frac{n-1}{2})} = - 2 \frac{a_2}{a_1^2} \left[c_2 + c_3 + \ldots + c_{\frac{n-1}{2}} \right] - \frac{a_2^5 + a_1^4 a_4}{a_1^3 a_2^2 a_3} \quad . \tag{5.23}$$

Mais

$$S_{n-1} = - \frac{X_1^n + X_{-1}^n}{a_1} = \lambda_{\frac{n-1}{2}}^{(\frac{n-1}{2})} X_o (X_1 X_{-1})^{\frac{n-1}{2}} + \ldots + \lambda_o^{(\frac{n-1}{2})} X_o^n$$

d'après (5.18). En développant les deux membres de cette expression au voisinage de 0 grace à (5.14) nous obtenons

$$- n (b_1 - b_{-1}) = \lambda_{\frac{n-1}{2}}^{(\frac{n-1}{2})} (-1)^{\frac{n-1}{2}}$$

d'où la relation (5.16), ce qui achève la démonstration de la proposition 5.16 .

Remarques i) Nous avons en posant $b'_r = b_r - b_{-r}$

$$(b'_{2t+2} - (2t+2)b'_1) - (b'_{2t} - 2tb'_1) = \frac{a_2}{a_1^2} c_{2t+1}$$

et

$$2(b'_2 - 2b'_1) = -\frac{a_2^5 + a_1^4 a_4}{a_1^3 a_2^2 a_3}$$

en effet,

$$S_{2t} = \frac{X_1^{2t} X_{-2t} + X_{-1}^{2t} X_{2t}}{a_{2t}} = \lambda_t^{(t)} X_o (X_1 X_{-1})^t + \ldots + \lambda_o^{(t)} X_o^{2t+1}$$

En prenant le développement en x au voisinage de 0 des deux membres de cette relation nous trouvons

$$2(b'_{2t} - 2tb'_1) = (-1)^t \lambda_t^{(t)}$$

et comme $(-1)^t \lambda_t^{(t)} = -\frac{2a_2}{a_1^2}\left[c_3 + c_5 + \ldots + c_{2t-1}\right] - \lambda_1^{(1)}$ d'après (5.21)

nous obtenons les relations cherchées.

ii) Nous verrons ultérieurement que les expressions $b_r - b_{-r}$ sont des formes modulaires de poids 1 pour $\Gamma(n)$. La formule (5.16) montre comment ces formes et les formes $1/a_r$ sont reliées.

5.6 Cohérence des fonctions $X_{rg',C}$

Soit C_1 un sous-groupe de C. Posons

$$n_1 = \# C_1 \quad , \quad d = \frac{n}{n_1} = [C : C_1]$$

$$g'_1 = dg'.$$

Théorème 5.19 : Pour tout $r_1 \in (\mathbb{Z}/n_1\mathbb{Z}) - \{0\}$ nous avons

$$\frac{X_{r_1 g'_1, C_1}}{n_1 a_{r_1 g'_1, C_1}} = \sum_{r \equiv r_1 \pmod{n_1}} \frac{X_{rg',C}}{n a_{rg',C}} \tag{5.24}$$

Preuve : Il est clair que $X_{r_1 g_1', C_1} \in L(\underline{C})$. Il existe donc des constantes λ_r^s avec $s \in \mathbb{Z}/n\mathbb{Z}$ telles que

$$X_{r_1 g_1', C_1} = \sum_{s \in \mathbb{Z}/n\mathbb{Z}} \lambda_{r_1}^s \, X_{sg', C}$$

Soit $g_1 \in C_1$. Alors $X_{r_1 g_1', C_1}(P - g_1) = e_{n_1}(r_1 g_1', g_1) X_{r_1 g_1', C} =$

$\sum_s \lambda_{r_1}^s \, e_n(sg', g_1) \, X_{sg', C}$. D'où

$$e_{n_1}(r_1 g_1', g_1) \lambda_{r_1}^s = e_n(sg', g_1) \lambda_{r_1}^s$$

pour tout $g_1 \in C_1$. Comme

$$e_n(sg', g_1) = e_{n_1}(s g_1', g_1)$$

d'après le théorème 1.17 nous trouvons

$$e_{n_1}(g_1', g_1)^{r_1 - s} \lambda_{r_1}^s = \lambda_{r_1}^s$$

pour tout $g_1 \in C_1$. Nous pouvons supposer que $C_1 \neq \{0\}$ sinon la formule (5.24) est trivialement vraie. Par conséquent, $n_1 > 1$ et $e_{n_1}(g_1', g_1)$ parcourt μ_{n_1} quand g_1 parcourt C_1. Ceci montre que $\lambda_{r_1}^s = 0$ si $s \not\equiv r_1 \pmod{n_1}$. Donc

$$X_{r_1 g', C_1} = \sum_{r \equiv r_1 (\mathrm{mod}\, n_1)} \lambda_{r_1}^r \, X_{rg', C}$$

Nous pouvons supposer $C \neq C_1$ sinon la relation (5.24) est trivialement vérifiée.

Soit $g \in C - C_1$. Alors

$$(5.25) \qquad {}^{g}X_{r_1 g_1', C_1} = \sum_{r \equiv r_1 (\mathrm{mod}\, n_1)} \lambda_{r_1}^r \, e_n(rg', g) \, X_{rg', C}$$

et la fonction ${}^{g}X_{r_1 g_1', C_1}$ n'a pas de pôle en 0. Multiplions les deux

membres de (5.25) par T et calculons leur valeur en 0. Nous trouvons pour tout $g \in C - c_1$

$$0 = \sum_{r \equiv r_1 (\mathrm{mod}\, n_1)} \lambda_{r_1}^{r} e_n(rg', g) a_{rg', C}$$

Nous pouvons écrire $r = r_1 + tn_1$, alors

$$e_n(rg', g) = e_n(r_1 g', g) e_n(tn_1 g', g)$$

et nous avons

$$0 = \sum_{t \bmod d} \lambda_{r_1}^{r_1 + tn_1} e_n(tn_1 g', g) a_{(r_1 + tn_1)g', C} \tag{5.26}$$

Lorsque g parcourt $C - C_1$, la racine n^{eme} de l'unité, $e_n(n_1 g', g)$, parcourt $\mu_{n_1} - \{1\}$. Les équations (5.26) forment un système dont la solution est

$$\lambda_{r_1}^{r_1 + tn_1} a_{(r_1 + tn_1)g', C} = \text{constante} .$$

Il en résulte que

$$X_{r_1 g_1', C_1} = \text{cte} \times \sum_{r \equiv r_1 (\mathrm{mod}\, n_1)} \frac{X_{rg', C}}{a_{rg', C}}$$

Pour calculer la constante il reste à évaluer le résidu des deux membres de cette égalité en 0 et finalement nous obtenons (5.24).

Remarques : i) Il est facile de vérifier sur la formule (5.24) que $X_{r_1 g_1', C_1}(\frac{r_1}{2} g_1') = -1$.

ii) Si on reprend la formule (5.14) on trouve

$$\frac{b_{r_1 g_1', C_1}}{n_1} = \sum_{r \equiv r_1 (\mathrm{mod}\, n_1)} \frac{b_{rg', C}}{n}$$

5.7 Le groupe $Sp(E_n)$

Définition 5.20 : Nous notons

$$Sp(E_n) = \{\sigma \in Aut(E_n) \mid e_n(g_1,g_2) = e_n(\sigma g_1, \sigma g_2) \text{ pour tous } g_1 \text{ et } g_2 \in E_n\}$$

A tout élément $\sigma \in Aut(E_n)$ nous associons $u_\sigma \in \mathbb{Z}/n\mathbb{Z}$, $v_\sigma \in \mathbb{Z}/n\mathbb{Z}$, $g_\sigma \in C$, $\varphi_\sigma \in Hom(C, \mathbb{Z}/n\mathbb{Z})$ uniquement définis par les équations

$$(5.27) \qquad \begin{cases} \sigma g' = u_\sigma g' + g_\sigma \\ \sigma g = \varphi_\sigma(g) g' + v_\sigma g \quad \text{pour tout } g \in C \end{cases}$$

Lemme 5.21 : La condition nécessaire et suffisante pour que $\sigma \in Aut(E_n)$ soit dans $Sp(E_n)$ est

$$u_\sigma v_\sigma - \varphi_\sigma(g_\sigma) = 1$$

Preuve : Pour tout $g \in C$, nous avons

$$e_n(\sigma g', \sigma g) = e_n(g',g)^{u_\sigma v_\sigma} \, e_n(g', g_\sigma)^{-\varphi_\sigma(g)}$$

Comme $\varphi_\sigma \in Hom(C, \mathbb{Z}/n\mathbb{Z})$ nous avons

$$e_n(g', g_\sigma)^{-\varphi_\sigma(g)} = e_n(g',g)^{-\varphi_\sigma(g_\sigma)}$$

puisque

$$g_\sigma^{\varphi_\sigma(g)} = g^{\varphi_\sigma(g_\sigma)} .$$

Donc $e_n(\sigma g' \sigma g) = e_n(g',g)^{u_\sigma v_\sigma - \varphi_\sigma(g_\sigma)}$, pour tout $g \in C$, d'où la conclusion .

Proposition 5.22 : Soit $\sigma \in Sp(E_n)$. Pour tout $r \in \mathbb{Z}/n\mathbb{Z}$ nous avons

$$(5.28) \qquad X_{r\sigma(g'),\sigma C}\, R_C^{\sigma C} = \sum_{g \in C} e_n(g', g_\sigma)^{(u_\sigma r^2/2) + \varphi_\sigma(g) r} \times e_n(g',g)^{(v_\sigma - \varphi_\sigma(g))/2} X_{u_\sigma r + \varphi_\sigma(g), C}$$

en notant $R_C^{\sigma C}$ la fonction définie par (4.10).

Preuve : Nous tirons de (4.22)

$$X_{\sigma(rg'),\sigma C}\, R_C^{\sigma C} = \sum_{g \in C} e_n(\sigma g', \sigma g)^{-1/2} X_{\sigma g' + \sigma g, C}$$

ce qui, compte-tenu de (5.27) et (4.5) n'est autre que (5.28).

Corollaire 5.23 : Soit g un générateur de C. Posons $u_\sigma = a$, $v_\sigma = d$, $g_\sigma = bg$, $\varphi_\sigma(g) = c$ et $\zeta = e_n(g', g)$. Alors ζ est un générateur de μ_n, la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est dans $SL_2(\mathbb{Z}/n\mathbb{Z})$ et

$$(5.29) \quad X_{\sigma(rg'),\sigma C}\, R_C^{\sigma C} = \sum_{s \in \mathbb{Z}/n\mathbb{Z}} \zeta^{\frac{abr^2 + 2bcrs + cds^2}{2}} X_{(ar+cs)g', C}$$

Preuve : Il est clair que ζ engendre μ_n. Le fait que $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ soit dans $SL_2(\mathbb{Z}/n\mathbb{Z})$ vient du lemme 5.2. Enfin, (5.29) n'est que la traduction de (5.28).

DEUXIEME PARTIE

Dans toute cette partie la lettre n désigne un nombre premier fixé, strictement supérieur à 3. Tous les schémas considérés sont au-dessus de $\mathbb{Z}[1/n]$.

Nous utiliserons un langage imagé, souvent incorrect, mais nous sommes sûrs que le lecteur n'aura aucune peine à faire la traduction en style canonique.

CHAPITRE 6

Le schéma $\mathcal{Q}$

Nous définissons dans ce chapitre :

i) Un schéma $\mathcal{Q}$ qui est le sous-schéma de $\mathbb{P}^{n-1}$ des zéros communs aux polynômes (6.12).

ii) Un groupe étale $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$ qui opère sur $\mathbb{P}^{n-1}$ et laisse stable $\mathcal{Q}$.

iii) Un sous-schéma étale $\mathcal{P}$ de $\mathcal{Q}$, de degré $(n^2 - 1)/2$, qu'on appelle le schéma des pointes, sur lequel $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$ opère transitivement.

6.1 Le groupe $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$

Définition 6.1 : Nous notons $Sp(\mathbb{Z}/n \times \mu_n)$ le schéma en groupes étale au-dessus de $\mathbb{Z}[1/n]$ "formé de l'ensemble des matrices $\begin{pmatrix} u & \zeta \\ \varphi & v \end{pmatrix}$ avec $u \in \mathbb{Z}/n\mathbb{Z}$, $v \in \mathbb{Z}/n\mathbb{Z}$, $\zeta \in \mu_n$, $\varphi \in \mathrm{Hom}(\mu_n, \mathbb{Z}/n\mathbb{Z})$ qui satisfont à la condition

$$uv - \varphi(\zeta) = 1 \ . \text{"} \tag{6.1}$$

La loi de composition est donnée par

$$\begin{pmatrix} u & \zeta \\ \varphi & v \end{pmatrix}\begin{pmatrix} u' & \zeta' \\ \varphi' & v' \end{pmatrix} = \begin{pmatrix} uu' + \varphi'(\zeta) & \zeta'^{u}\,\zeta^{v} \\ u'\varphi + v\varphi' & vv' + \varphi(\zeta') \end{pmatrix} \ . \tag{6.2}$$

L'élément neutre est la matrice $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ et l'inverse de $\begin{pmatrix}u & \zeta\\ \varphi & v\end{pmatrix}$ est $\begin{pmatrix}v & \zeta^{-1}\\ -\varphi & u\end{pmatrix}$.

Proposition 6.2 : i) Soit τ un générateur de $\mu_n(\mathbb{Z}[1/n][\mu_n])$. L'application

$$\theta_\tau : \begin{pmatrix}u & \tau^b\\ \varphi & v\end{pmatrix} \longmapsto \begin{pmatrix}u & b\\ \varphi(\tau) & v\end{pmatrix}$$

est un isomorphisme défini sur $\mathbb{Z}[1/n]$ de $Sp(\mathbb{Z}/n\mathbb{Z}\times\mu_n)$ sur $SL(2,\mathbb{Z}/n\mathbb{Z})$.

ii) Soit $s \in (\mathbb{Z}/n\mathbb{Z})^\times$. Pour tout $\sigma \in Sp(\mathbb{Z}/n\mathbb{Z}\times\mu_n)$ nous avons

$$\theta_{\tau^s}(\sigma) = \begin{pmatrix}s^{-1} & 0\\ 0 & 1\end{pmatrix} \theta_\tau(\sigma) \begin{pmatrix}s & 0\\ 0 & 1\end{pmatrix} \tag{6.3}$$

iii) Si γ est un automorphisme de $\mathbb{Z}[1/n][\mu_n]$ tel que $\gamma\zeta = \zeta^s$ pour tout $\zeta \in \mu_n$ nous avons

$$\gamma\begin{pmatrix}u & \zeta\\ \varphi & v\end{pmatrix} = \begin{pmatrix}u & \zeta^s\\ s^{-1}\varphi & v\end{pmatrix} = \begin{pmatrix}s & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}u & \zeta\\ \varphi & v\end{pmatrix}\begin{pmatrix}s^{-1} & 0\\ 0 & 1\end{pmatrix} \tag{6.4}$$

Corollaire 6.3 : Soit k une $\mathbb{Z}[1/n][\mu_n]$-algèbre à spectre connexe. Le groupe $Sp(\mathbb{Z}/n\mathbb{Z}\times\mu_n)(k)$ est engendré par les matrices de la forme $\begin{pmatrix}1 & \zeta\\ 0 & 1\end{pmatrix}$ et $\begin{pmatrix}0 & \zeta\\ \varphi & 0\end{pmatrix}$.

Preuves : La proposition 6.2 est immédiate. Le corollaire 6.3 résulte du fait que $SL(2,\mathbb{Z}/n\mathbb{Z})$ est engendré par les matrices $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ et $\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$.

Nous verrons (proposition 7.8) que le groupe $Sp(\mathbb{Z}/n\mathbb{Z}\times\mu_n)$ opère sur $\mathbb{Z}/n\mathbb{Z}\times\mu_n$ et que son image dans $Aut(\mathbb{Z}/n\mathbb{Z}\times\mu_n)$ est le sous-groupe qui respecte une forme bilinéaire alternée non dégénérée à valeurs dans μ_n, d'où le nom donné à $Sp(\mathbb{Z}/n\mathbb{Z}\times\mu_n)$.

6.2 Action de $Sp(\mathbb{Z}/n\mathbb{Z}\times\mu_n)$ sur $\mathbb{P}^{n-1}$

Choisissons dans $\mathbb{A}^n$ un système de coordonnées affines indexées par $\mathbb{Z}/n\mathbb{Z}$. Soit $\sigma = \begin{pmatrix}u & \zeta\\ \varphi & v\end{pmatrix}$ dans $Sp(\mathbb{Z}/n\mathbb{Z}\times\mu_n)$. Pour tout

$A = (A(0), A(1), \ )$ dans $\mathbb{A}^n$ posons

$$m_\sigma A = A' = (A'(0), A'(1), \ldots)$$

avec

$$(6.5) \qquad A'(r) = \sum_{\tau \in \mu_n} \zeta^{ur^2 + 2r\varphi(\tau)} \tau^{v\varphi(\tau)} A(ur + \varphi(\tau)).$$

Lemme 6.4 : i) L'application $\sigma \mapsto m_\sigma$ est définie sur $\mathbb{Z}[1/n]$.

ii) Si σ et σ' sont dans $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$ il existe une matrice scalaire $d(\sigma,\sigma')$ telle que

$$m_\sigma \, m_{\sigma'} = d(\sigma,\sigma') m_{\sigma\sigma'}$$

iii) Pour tout $\sigma \in Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$, la matrice m_σ est dans $GL(n, \mathbb{Z}[1/n][\mu_n])$.

Preuve : i) Soit γ un automorphisme de $\mathbb{Z}[1/n][\mu_n]$ tel que $\gamma\zeta = \zeta^s$ pour tout $\zeta \in \mu_n$. Alors, d'après (6.5),

$$\gamma A'(r) = \sum_{\tau \in \mu_n} \zeta^{sur^2 + 2rs\varphi(\tau)} \tau^{sv\varphi(\tau)} A(ur + \varphi(\tau)).$$

En posant $\tau = \nu^s$ dans cette formule nous obtenons

$$\gamma A'(r) = \sum_{\nu \in \mu_n} \zeta^{sur^2 + 2r\varphi(\nu)} \nu^{vs^{-1}\varphi(\nu)} A(ur + s^{-1}\varphi(\nu))$$

et comme $\gamma\sigma = \begin{pmatrix} u & \zeta^s \\ s^{-1}\varphi & v \end{pmatrix}$ nous avons

$$\gamma(m_\sigma A) = m_{\gamma\sigma} A$$

ce qui prouve que l'application $\sigma \mapsto m_\sigma$ est bien définie sur $\mathbb{Z}[1/n]$.

ii) Le groupe $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$ étant engendré par $T = \begin{pmatrix} 1 & \zeta \\ 0 & 1 \end{pmatrix}$ et $S = \begin{pmatrix} 0 & \zeta \\ \varphi & 0 \end{pmatrix}$, il suffit pour prouver l'affirmation ii) de montrer l'existence des matrices scalaires $d(\sigma,T)$ et $d(\sigma,s)$ quand σ est une matrice quelconque de $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$.

Posons $\sigma = \begin{pmatrix} u_1 & \zeta_1 \\ \varphi_1 & v_1 \end{pmatrix}$ et calculons

$$m_\sigma(m_T A) = A' .$$

D'après (6.5) nous avons

$$A'(r) = \sum_{\tau \in \mu_n} \zeta_1^{u_1 r^2 + 2r\varphi_1(\tau)} \tau^{v_1 \varphi_1(\tau)} \zeta^{(u_1 r + \varphi_1(\tau))^2} A(u_1 r + \varphi_1(\tau))$$

$$= \sum_{\tau \in \mu_n} (\zeta_1 \zeta^{u_1})^{u_1 r^2 + 2r\varphi_1(\tau)} \tau^{v_1 \varphi_1(\tau)} \zeta^{\varphi_1(\tau)^2} A(u_1 r + \varphi_1(\tau)).$$

Mais $\zeta^{\varphi_1(\tau)} = \tau^{\varphi_1(\zeta)}$ et

$$A'(r) = \sum_{\tau} (\zeta, \zeta^{u_1})^{u_1 r^2 + 2r\varphi_1(\tau)} \tau^{(v_1 + \varphi_1(\zeta))\varphi_1(\tau)} A(u_1 r + \varphi_1(\tau)).$$

et comme $\sigma T = \begin{pmatrix} u_1 & \zeta^{u_1}\zeta_1 \\ \varphi_1 & v_1 + \varphi_1(\zeta) \end{pmatrix}$ nous constatons que

$$m_\sigma(m_T A) = m_{\sigma T} A$$

ce qui montre l'existence de la matrice $d(\sigma,T)$ qui n'est autre que la matrice identité.

Calculons $m_\sigma(m_s A) = A'$. D'après (6.5) nous avons

$$A'(r) = \sum_{\tau \in \mu_n} \zeta_1^{u_1 r^2 + 2r\varphi_1(\tau)} \tau^{v_1 \varphi_1(\tau)} \sum_{\tau' \in \mu_n} \zeta^{2(u_1 r + \varphi_1(\tau))\varphi(\tau')} A(\varphi(\tau'))$$

Posons dans cette égalité $\tau' = \zeta_1^r \tau''$ alors

$$A'(r) = \sum_{\tau'' \in \mu_n} \zeta^{u_1 r^2} \zeta^{2u_1 r^2 \varphi(\zeta_1) + 2u_1 r \varphi(\tau'')} A(\varphi(\zeta_1^r \tau'')) M(\tau'')$$

où nous avons noté

$$M(\tau'') = \sum_{\tau \in \mu_n} \zeta_1^{2r\varphi_1(\tau)} \tau^{v_1 \varphi_1(\tau)} \zeta^{2\varphi_1(\tau)[r\varphi(\zeta_1) + \varphi(\tau'')]}$$

Comme $\zeta^{\varphi(\zeta_1)} = \zeta_1^{\varphi(\zeta)} = \zeta_1^{-1}$ (puisque $\varphi(\zeta) = -1$) nous pouvons simplifier ces expressions et nous obtenons

$$(6.6) \qquad A'(r) = \sum_{\tau''} \zeta_1^{-u_1 r^2} \zeta^{2u_1 r \varphi(\tau'')} M(\tau'') A(\varphi(\zeta_1^r \tau'')) \quad \text{et}$$

$$M(\tau'') = \sum_{\tau \in \mu_n} \tau^{v_1 \varphi_1(\tau)} \zeta^{2\varphi_1(\tau)\varphi(\tau'')}$$

Nous allons donner une autre expression de $M(\tau'')$. Deux cas sont à envisager.

Premier cas : $v_1 = 0$; alors $\varphi_1(\zeta_1) = -1$ et φ_1 est un isomorphisme entre μ_n et $\mathbb{Z}/n\mathbb{Z}$. Nous avons donc

$$M(\tau'') = \sum_{u \in \mathbb{Z}/n\mathbb{Z}} \zeta^{2\varphi(\tau'')u}$$

ce qui s'écrit encore, compte-tenu de

$$\zeta^{\varphi(\tau'')} = \tau''^{\varphi(\zeta)} = \tau''^{-1},$$

$$M(\tau'') = \sum_{u \in \mathbb{Z}/n\mathbb{Z}} \tau''^{-2u}$$

Il en résulte que

$$M(\tau'') = \begin{cases} 0 & \text{si } \tau'' \neq 1 \\ n & \text{si } \tau'' = 1 \end{cases} \tag{6.7}$$

Deuxième cas : $v_1 \neq 0$. Posons $\tau'' = t^{v_1}$. Alors

$$M(\tau'') = \sum_{\tau \in \mu_n} \tau^{v_1 \varphi_1(\tau)} \zeta^{2v_1 \varphi_1(\tau)\varphi(t)}$$

Faisons dans cette formule le changement de variable $\tau = \theta t$ ce qui donne

$$M(\tau'') = \sum_{\theta \in \mu_n} (\theta t)^{v_1 \varphi_1(\theta t)} \zeta^{2v_1 \varphi_1(\theta t)\varphi(t)}$$

comme $\zeta^{\varphi(t)} = t^{\varphi(\zeta)} = t^{-1}$ nous trouvons

$$M(\tau'') = \sum_{\theta \in \mu_n} \theta^{v_1 \varphi_1(\theta)} \theta^{v_1 \varphi_1(t)} t^{-v_1 \varphi_1(\theta)} t^{-v_1 \varphi_1(t)}$$

et puisque $\theta^{v_1 \varphi_1(t)} = t^{v_1 \varphi_1(\theta)}$ nous obtenons enfin

$$M(\tau'') = \Big(\sum_{\theta\in\mu_n} \theta^{v_1\varphi_1(\theta)}\Big) t^{-v_1\varphi_1(t)} \tag{6.8}$$

Nous pouvons regrouper les résultats (6.7) et (6.8) en une seule expression. Pour cela introduisons

$$G(v_1\varphi_1) = \sum_{\theta\in\mu_n} \theta^{v_1\varphi_1(\theta)} \tag{6.9}$$

Cette expression est une "somme de Gauss", qui n'est jamais nulle, et nous avons démontré que

$$M(\tau'') = \begin{cases} 0 & \text{si } \tau'' \notin \mu_n^{v_1} \\ G(v_1\varphi_1)t^{-v_1\varphi_1(t)} & \text{si } \tau'' = t^{v_1} \text{ avec } t\in\mu_n \end{cases}$$

Si nous reportons ce résultat dans (6.6) nous obtenons

$$A'(r) = \frac{G(v_1\varphi_1)}{(v_1,n)} \sum_{t\in\mu_n} \zeta^{u_1[\varphi(\zeta_1)r^2 + 2rv_1\varphi(t)]} {}_t\varphi_1(\zeta)^{v_1\varphi(t)} A(\varphi(\zeta_1^r t^{v_1}))$$

et comme $\sigma S = \begin{pmatrix} \varphi(\zeta_1) & \zeta^{u_1} \\ v_1\varphi & \varphi_1(\zeta) \end{pmatrix}$ nous avons

$$m_\sigma(m_S A) = d(\sigma, S) m_{\sigma S} A$$

où $d(\sigma,S)$ est la matrice scalaire dont les élements diagonaux valent $\frac{G(v_1\varphi_1)}{(v_1,n)}$.

iii) Le nombre $G(v_1\varphi_1)$ est dans $\mathbb{Z}[\mu_n]$ et nous savons [Ei] que $G(v_1\varphi_1)G(-v_1\varphi_1) = \pm n$. Par conséquent, $G(v_1\varphi_1)$ ainsi que (v_1,n) sont inversibles dans $\mathbb{Z}[1/n][\mu_n]$. Il en résulte, puisque T et S engendrent $Sp(\mathbb{Z}/n\mathbb{Z}\times\mu_n)$ que toutes les matrices scalaires $d(\sigma,\sigma')$ sont dans $GL(n,\mathbb{Z}[1/n][\mu_n])$. Il suffit donc de démontrer que m_T et m_S sont dans $GL(n,\mathbb{Z}[1/n][\mu_n])$.

D'après (6.5), la matrice m_T est une matrice diagonale. En effet, si $m_T A = A'$ nous avons

$$A'(r) = n\zeta^{r^2} A(r) \tag{6.10}$$

d'où

$$\det m_T = n^n \prod_{r=o}^{n-1} \zeta^{r^2} = n^n \zeta^{\sum_{r=o}^{n-1} r^2} .$$

Mais $\sum_{r=o}^{n-1} r^2 = \frac{(n-1)n(2n-1)}{6}$ et comme n est premier à 6 nous avons

$\det m_T = n^n$ ce qui prouve que $m_T \in GL(n, \mathbb{Z}[1/n][\mu_n])$. Calculons maintenant $\det m_S$. Posons $m_S A = A'$. D'après (6.5) nous avons

$$A'(r) = \sum_{\tau \in \mu_n} \zeta^{2r\varphi(\tau)} A(\varphi(\tau))$$

et comme φ est un isomorphisme puisque $\varphi(\zeta) = -1$ nous pouvons récrire cette formule

$$A'(r) = \sum_{t \in \mathbb{Z}/n\mathbb{Z}} \zeta^{2rt} A(t) \tag{6.11}$$

Nous voyons que le coefficient $\alpha_{i,j}$ de la matrice m_S est ζ^{2ij} et que $\det m_S$ est un déterminant de Van der Monde. Si nous notons m'_S la matrice déduite de m_S en changeant ζ en ζ^{-1} nous obtenons

$$\det m_S = \pm \det m'_S$$

et

$$m_S m'_S = n.id$$

Par conséquent, $(\det m_S)^2 = \pm n^n$ et là encore, m_S est dans $GL(n, \mathbb{Z}[1/n][\mu_n])$.

Remarques i) Les relations (6.10) et (6.11) établissent un lien entre les matrices m_σ et la représentation du groupe métaplectique de Weil. La relation (6.10) montre que $T = \begin{pmatrix} 1 & \zeta \\ 0 & 1 \end{pmatrix}$ est associée à l'opérateur de multiplication par la gaussienne $r \longmapsto n\zeta^{r^2}$ alors que (6.11) montre que $s = \begin{pmatrix} 0 & \zeta \\ \varphi & 0 \end{pmatrix}$ est associée à un opérateur de transformation de Fourier.

ii) Le lemme 6.4 est encore vrai si on suppose seulement n impair, pas premier. Nous trouvons encore $d(\sigma,T) = id$ et $d(\sigma,s)$ est la matrice scalaire ayant pour élément diagonal $\frac{G(v_1\varphi_1)}{(v_1,n)}$ où $G(v_1\varphi_1)$ est défini par (6.9) et (v_1,n) est le PGCD de v_1 et n .

Corollaire 6.5 : Si nous notons $\widetilde{m}_\sigma$ l'image de m_σ dans PGL(n), l'application $\sigma \mapsto \widetilde{m}_\sigma$ est un homomorphisme de $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$ dans PGL(n), défini sur $\mathbb{Z}[1/n]$. De plus cet homomorphisme est un monomorphisme.

Preuve : La seule chose à montrer est que $\sigma \mapsto \widetilde{m}_\sigma$ est un monomorphisme. Soit k une $\mathbb{Z}[1/n][\mu_n]$- algèbre et soit $\sigma = \begin{pmatrix} u & \zeta \\ \varphi & v \end{pmatrix} \in Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)(k)$ tel que $\widetilde{m}_\sigma = id$. Alors, d'après (6.5) nous avons

$$ur + \varphi(\tau) = r$$

pour tout $r \in \mathbb{Z}/n\mathbb{Z}$ et tout $\tau \in \mu_n$. En prenant $r = 1$ et $\tau = 1$ nous obtenons $u = 1$ et $\varphi = 0$. Il en résulte que m_σ est la matrice diagonale définie par

$$\alpha_{i,i} = n\zeta^{i^2},$$

pour que $\widetilde{m}_\sigma = id$, il faut que $\zeta = 1$ d'où $\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ qui est, rappelons-le l'élément neutre de $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$.

A partir de maintenant nous n'utiliserons plus les notations m_σ et $\widetilde{m}_\sigma$ et nous noterons σa le transformé du point a de $\mathbf{P}^{n-1}$ par $\widetilde{m}_\sigma$.

6.3 Le schéma $\mathcal{A}$

Considérons les polynômes suivants

$$(6.12)\qquad \begin{cases} \mathcal{R}'_o = A_o \\ \mathcal{R}'_i = A_i + A_{-i} \qquad (i \in \mathbb{Z}/n\mathbb{Z}) \\ \mathcal{R}_I = A_{i_3-i_2} A_{j_3-i_2} A_{i_1} A_{j_1} \\ \qquad + A_{i_1-i_3} A_{j_1-i_3} A_{i_2} A_{j_2} \\ \qquad + A_{i_2-i_1} A_{j_2-i_1} A_{i_3} A_{j_3} \end{cases}$$

où $I = (i_1,j_1,i_2,j_2,i_3,j_3)$ est un sextuplet d'éléments de $\mathbb{Z}/n\mathbb{Z}$ tels que

$$i_1 + j_1 = i_2 + j_2 = i_3 + j_3$$

Définition 6.5 : Nous notons $\mathcal{A}$ le sous-$\mathbb{Z}[1/n]$-schéma de $\mathbb{P}^{n-1}$ défini par l'idéal engendré par les polynômes (6.12).

Remarques : i) Soient u et v dans $\mathbb{Z}/n\mathbb{Z}$ tels que $uv = 1$. Nous verrons (définition 6.11) que le point $a = (a(0) : a(1) : \quad) \in \mathbb{P}^{n-1}(\mathbb{Z}[1/n])$ défini par

$$a(i) = \begin{cases} 0 \quad \text{si} \quad i \neq \pm v/2 \\ a(v/2) = -a(-v/2) = 1 \end{cases}$$

appartient à $\mathcal{A}(\mathbb{Z}[1/n])$.

ii) Si deux des trois ensembles $\{i_1,j_1\}$, $\{i_2,j_2\}$, $\{i_3,j_3\}$ du sextuplet $I = (i_1,j_1,i_2,j_2,i_3,j_3)$ sont égaux, le polynôme $\mathcal{R}_I$ est dans l'idéal engendré par les polynômes $\mathcal{R}'_o$ et $\mathcal{R}_i$.

Proposition 6.6 : Soit a un point de $\mathcal{A}$ et soit $\sigma \in Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$. Alors σa est un point de $\mathcal{A}$. Autrement dit, l'action de $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$ sur $\mathbb{P}^{n-1}$ respecte $\mathcal{A}$.

Preuve : Il suffit de vérifier cette affirmation pour $\sigma = T = \begin{pmatrix} 1 & \zeta \\ 0 & 1 \end{pmatrix}$ et $\sigma = s = \begin{pmatrix} 0 & \zeta \\ \varphi & 0 \end{pmatrix}$. Posons $a = (a(0) : a(1) : \quad)$ et $\sigma a = a' = (a'(0) : a'(1) : \quad)$.

Premier cas : $\sigma = T = \begin{pmatrix} 1 & \zeta \\ 0 & 1 \end{pmatrix}$. Alors d'après (6.5)

$$a'(r) = n\, \zeta^{r^2} a(r) .$$

Il est clair que $a'(0) = 0$ et que $a'(-r) = - a'(r)$.

Soit $I = (i_1, j_1, i_2, j_2, i_3, j_3)$ un sextuplet de $\mathbb{Z}/n\mathbb{Z}$ tel que $i_1 + j_1 = i_2 + j_2 = i_3 + j_3 = \alpha$. Alors

$$(i_3 - i_2)^2 + (j_3 - i_2)^2 + i_1^2 + j_1^2 = i_1^2 + j_1^2 + i_2^2 + j_2^2 + j_2^2 + i_3^2 + j_3^2$$

$$- (j_2^2 + 2i_2 i_3 + 2i_2 j_3 - i_2^2)$$

et comme $j_2^2 + 2i_2 i_3 + 2i_2 j_3 - i_2^2 = (\alpha - i_2)^2 + 2i_2\alpha - i_2^2 = \alpha^2$, nous obtenons

$$(i_3 - i_2)^2 + (j_3 - i_2)^2 + i_1^2 + j_1^2 = \sum_{r=1}^{3} (i_r^2 + j_r^2) - \alpha^2$$

Nous avons le même résultat en effectuant une permutation circulaire sur les indices 1, 2, 3 et par conséquent

$$R_I(a') = \zeta^{\sum_{r=1}^{3} (i_r^2 + j_r^2) - \alpha^2} R_I(a)$$

ce qui montre que a' annule les polynômes (6.9) .

Deuxième cas : $\sigma = S = \begin{pmatrix} 0 & \zeta \\ \varphi & 0 \end{pmatrix}$. Alors, d'après (6.5)

$$a'(r) = \overline{\sum_{\tau \in \mu_n}} \zeta^{2r\varphi(\tau)} a(\varphi(\tau))$$

ou encore, puisque φ est un isomorphisme

$$a'(r) = \overline{\sum_{t \in \mathbb{Z}/n\mathbb{Z}}} \zeta^{2rt} a(t) \quad .$$

Comme $a(0) = 0$ et $a(t) + a(-t) = 0$ nous avons $a'(0) = \sum_t a(t) = 0$.

De même

$$a'(r) + a'(-r) = \sum_t \zeta^{2rt} a(t) + \sum_{t'} \zeta^{-2rt'} a(t')$$

$$= \sum_t \zeta^{2rt} (a(t) + a(-t)) = 0$$

Calculons $\mathcal{R}_I(a')$. En posant

$$B_1 = \sum_{t_1,t_2,t_3,t_4}{}' \zeta^{2[(i_3-i_2)t_1 + (j_3-i_2)t_2 + i_1t_3 + j_1t_4]} a(t_1)a(t_2)a(t_3)a(t_4)$$

$$B_2 = \sum_{t_1,t_2,t_3,t_4}{}' \zeta^{2[(i_1-i_3)t_1 + (j_1-i_3)t_2 + i_2t_3 + j_2t_4]} a(t_1)a(t_2)a(t_3)a(t_4)$$

$$B_3 = \sum_{t_1,t_2,t_3,t_4}{}' \zeta^{2[(i_2-i_1)t_1 + (j_2-i_1)t_2 + i_3t_3 + j_3t_4]} a(t_1)a(t_2)a(t_3)a(t_4)$$

nous avons

$$\mathcal{R}_I(a') = B_1 + B_2 + B_3 .$$

Faisons dans B_1 le changement de variables

$$\begin{aligned} t_1 &= u_3 - u_2 \\ t_2 &= u_1 + v_1 - u_3 - u_2 \\ t_3 &= u_1 \\ t_4 &= v_1 \end{aligned} \qquad (6.13)$$

et posons

$$\begin{aligned} U &= u_1 + v_1 \\ v_2 &= U - u_2 \\ v_3 &= U - v_2 \end{aligned}$$

Le sextuplet $J = (u_1,v_1,u_2,v_2,u_3,v_3)$ est tel que

$u_1 + v_1 = u_2 + v_2 = u_3 + v_3 = U$ et nous obtenons

$$B_1 = \sum_J \zeta^{2[(i_3-i_2)(u_3-u_2) + (j_3-i_2)(v_3-u_2) + i_1u_1 + j_1v_1]} \times$$
$$a(u_3-u_2)a(v_3-u_2)a(u_1)a(v_1) \quad .$$

Or

$$(i_3-i_2)(u_3-u_2) + (j_3-i_2)(v_3-u_2) + i_1u_1 + j_1v_1 =$$
$$i_1u_1 + j_1v_1 + i_2u_2 + j_2v_2 + i_3u_3 + j_3v_3 - \alpha U$$

et par conséquent ,

$$B_1 = \sum_J \zeta^{2[\sum_{r=1}^{3}(i_ru_r + j_rv_r) - \alpha U]} a(u_3-u_2)a(v_3-u_2)a(u_1)a(v_1)$$

Enfin, nous faisons dans B_2 et B_3 les changements de variables déduits de (6.13) par permutation circulaire sur 1,2,3 et nous en déduisons

$$\mathcal{R}_I(a') = \sum_J \zeta^{2[\sum_{r=1}^{3}(i_ru_r + j_rv_r) - \alpha U]} \mathcal{R}_J(a)$$

ce qui montre que $\mathcal{R}_I(a') = 0$ et la proposition est démontrée.

Remarque : Les résultats des paragraphes 6.1, 6.2, 6.3 restent valables si on suppose seulement n impair (mais pas nécessairement premier supérieur à 3).

6.4 Les pointes de $\mathcal{C}$

Définition 6.7 : Nous notons $\begin{bmatrix}1\\0\end{bmatrix} = (a(0) : a(1) : \ )$ le point de $\mathbf{P}^{n-1}$ tel que

(6.14) $$a(i) = \begin{cases} 0 & \text{si } i \neq \pm 1/2 \in \mathbb{Z}/n\mathbb{Z} \\ a(1/2) = -a(-1/2) = 1 \end{cases}$$

Lemme 6.8 : Le point $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ appartient à $\mathcal{A}(\mathbb{Z}[1/n])$.

Preuve : Soit $I = (i_1, j_1, i_2, j_2, i_3, j_3)$ tel que l'un des trois monômes de $R_I(\begin{bmatrix} 1 \\ 0 \end{bmatrix})$ ne soit pas nul. Nous pouvons supposer que c'est

$$a(i_3 - i_2)a(j_3 - i_2)a(i_1)a(j_1).$$

Par conséquent nous avons

$$i_3 - i_2 = \pm 1/2 \qquad j_3 - i_2 = \pm 1/2$$

$$i_1 = \pm 1/2 \qquad j_1 = \pm 1/2 \ .$$

Ces équations définissent 16 systèmes linéaires. Leur solution montre que dans chaque cas deux des trois ensembles $\{i_1, j_1\}$ $\{i_2, j_2\}$ $\{i_3, j_3\}$ sont égaux. Par conséquent (nous l'avons remarqué après la définition 6.5) le polynôme R_I est dans l'idéal engendré par les polynômes R'_o et R_i. Mais comme $a(o) = 0$ et $a(i) + a(-i) = 0$ pour tout $i \in \mathbb{Z}/n\mathbb{Z}$ nous voyons que $\begin{bmatrix} 1 \\ 0 \end{bmatrix} \in \mathcal{A}(\mathbb{Z}[1/n])$.

Définition 6.9 : Nous notons $\mathcal{P}$ l'orbite dans $\mathbb{P}^{n-1}$ de $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ sous l'action de $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$. C'est un sous-schéma étale de $\mathcal{A}$ que nous appelons le schéma des pointes de $\mathcal{A}$.

Si k désigne une $\mathbb{Z}[1/n]$-algèbre nous disons que les éléments de $\mathcal{P}(k)$ sont les pointes de $\mathcal{A}(k)$.

Lemme 6.10 : Le stabilisateur de $\begin{bmatrix} 1 \\ 0 \end{bmatrix} \in \mathcal{A}(k)$ dans $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)(k)$ est l'ensemble des matrices $\sigma = \begin{pmatrix} u & \zeta \\ 0 & u \end{pmatrix}$.

Preuve : Nous pouvons supposer que k a un spectre connexe. Si σ laisse fixe $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ il existe λ inversible tel que

$$\lambda a(r) = \sum_{\tau \in \mu_n} \zeta^{ur^2 + 2r\varphi(\tau)_\tau v\varphi(\tau)} a(ur + \varphi(\tau))$$

Supposons $\varphi \neq 0$. Alors φ est un isomorphisme et il existe $\tau_o \in \mu_n(k)$ tel que $\varphi(\tau_o) = 1$. Nous avons donc

$$\lambda a(r) = \sum_{t \in \mathbb{Z}/n\mathbb{Z}} \zeta^{ur^2 + 2rt\,\tau_o vt^2} a(ur + t)$$

Mais $a(r) \neq 0$ seulement si $r = \pm 1/2$. Par conséquent

$$\lambda a(r) = \left[\zeta^{-ur^2 + r\,\tau_o v(1/2-ur)^2} - \zeta^{-ur^2 - r\,\tau_o v(-1/2-ur)^2}\right] a(1/2)$$

d'où nous tirons

$$(\zeta \tau_o^{-uv})^{2r} = 1 \quad \text{pour tout } r \neq \pm 1/2$$

et

$$\zeta\, \tau_o^{-uv} \neq 1$$

Ces deux égalités étant incompatibles il en résulte $\varphi = 0$ et que $u \in (\mathbb{Z}/n\mathbb{Z})^\times$. Alors

$$\lambda a(r) = n\, \zeta^{ur^2} a(ur)$$

ce qui donne $1/2 = \pm u/2$ et $u = \pm 1$. Réciproquement, si $\varphi = 0$ et $u = v = \pm 1$, il est clair que $\sigma \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$.

Nous en déduisons immédiatement

<u>Corollaire 6.11</u> : <u>Si</u> $\sigma = \begin{pmatrix} u & \zeta \\ \varphi & v \end{pmatrix}$ <u>et</u> $\sigma' = \begin{pmatrix} u & \zeta' \\ \varphi & v' \end{pmatrix}$ <u>sont dans</u> $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)(k)$ <u>nous avons</u> $\sigma \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \sigma' \begin{bmatrix} 1 \\ 0 \end{bmatrix}$.

En effet, $\sigma^{-1}\sigma'$ stabilise $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$.

Soit $(u,\varphi) \in \mathbb{Z}/n\mathbb{Z} \times \mathrm{Hom}(\mu_n, \mathbb{Z}/n\mathbb{Z})(k)$ avec $(u,\varphi) \neq (0,0)$. Il existe $\zeta \in \mu_n(k)$ et $v \in \mathbb{Z}/n\mathbb{Z}$ tels que $\sigma = \begin{pmatrix} u & \zeta \\ \varphi & v \end{pmatrix}$ soit dans $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)(k)$.

D'après le corollaire 6.10, le point $\sigma\begin{bmatrix}1\\0\end{bmatrix}$ de $\mathcal{P}(k)$ ne dépend pas du choix de ζ et v. Ceci nous permet de poser :

Définition 6.12 : Soit $\sigma = \begin{pmatrix} u & \zeta \\ \varphi & v \end{pmatrix} \in Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)(k)$. Nous notons $\begin{bmatrix}u\\\varphi\end{bmatrix}$ le point de $\mathcal{A}(k)$ défini par

$$\begin{bmatrix}u\\\varphi\end{bmatrix} = \sigma\begin{bmatrix}1\\0\end{bmatrix}$$

et nous disons que $\begin{bmatrix}u\\\varphi\end{bmatrix}$ est une représentation de la pointe $\sigma\begin{bmatrix}1\\0\end{bmatrix}$ dans $\mathbb{Z}/n\mathbb{Z} \times \mathrm{Hom}(\mu_n, \mathbb{Z}/n\mathbb{Z})(k)$.

Nous déduisons immédiatement du lemme 6.10.

Proposition 6.13 : i) Nous avons $\begin{bmatrix}u\\\varphi\end{bmatrix} = \begin{bmatrix}u'\\\varphi'\end{bmatrix}$ si et seulement si $u = \varepsilon u'$ et $\varphi = \varepsilon\varphi'$ avec $\varepsilon^2 = 1$. Autrement dit, si k a un spectre connexe, une pointe de $\mathcal{A}(k)$ possède au plus deux représentations dans

$$\mathbb{Z}/n\mathbb{Z} \times \mathrm{Hom}(\mu_n, \mathbb{Z}/n\mathbb{Z})(k) .$$

ii) Si $\begin{pmatrix} u' & \zeta' \\ \varphi' & v' \end{pmatrix} \in Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$ nous avons

$$\begin{pmatrix} u' & \zeta' \\ \varphi' & v' \end{pmatrix}\begin{bmatrix}u\\\varphi\end{bmatrix} = \begin{bmatrix}uu' + \varphi(\zeta')\\ u\varphi' + v\varphi\end{bmatrix} . \tag{6.15}$$

Corollaire 6.14 : Le schéma $\mathcal{P}$ est un $\mathbb{Z}[1/n]$-schéma étale de degré $(n^2-1)/2$. De plus, $\mathcal{P}(\mathbb{Z}[1/n])$ est formé des $(n-1)/2$ pointes du type $\begin{bmatrix}u\\0\end{bmatrix}$. Plus précisément, si $\gamma \in \mathrm{Aut}(\mathbb{Z}[1/n][\mu_n])$ est tel que $\gamma\zeta = \zeta^s$ pour tout $\zeta \in \mu_n$ nous avons

$$\gamma\begin{bmatrix}u\\\varphi\end{bmatrix} = \begin{bmatrix}u\\ s^{-1}\varphi\end{bmatrix} . \tag{6.16}$$

Preuve : D'après la proposition 6.13, si k désigne une $\mathbb{Z}[1/n][\mu_n]$ algèbre à spectre connexe, $\mathcal{P}(k)$ possède deux fois moins d'éléments qu'il y a de couples (u,φ) avec $(u,\varphi) \neq (0,0)$. D'où $\#\mathcal{P}(k) = (n^2-1)/2$. La formule (6.16) résulte de (6.4). Elle montre que les seules pointes $\begin{bmatrix}u\\\varphi\end{bmatrix}$ fixes par Γ sont celles pour lesquelles $\varphi = 0$ (car $n > 3$) et

toujours à cause de la proposition 6.13, il y a (n-1)/2 telles pointes.

Remarque : Il faut noter qu'une pointe de $\mathcal{C}(k)$ n'a jamais une seule représentation dans $\mathbb{Z}/n\mathbb{Z} \times \mathrm{Hom}(\mu_n, \mathbb{Z}/n\mathbb{Z})(k)$. Ou bien elle en a deux, ou bien elle n'en a aucune. Dans ce cas il existe une extension quadratique de k sur laquelle la pointe a deux représentations, et cette extension s'obtient en adjoignant à k les racines $n^{èmes}$ de l'unité.

Définition 6.15 : Nous dirons que les pointes de la forme $\left[\begin{smallmatrix} u \\ 0 \end{smallmatrix}\right]$ sont les pointes rationnelles de $\mathcal{C}$.

Proposition 6.16 : Soient k une $\mathbb{Z}\left[1/n\right]\left[\mu_n\right]$-algèbre et $\left[\begin{smallmatrix} u \\ \varphi \end{smallmatrix}\right]$ une pointe de $\mathcal{C}(k)$. Nous pouvons choisir des coordonnées projectives $(a(0) : a(1) : \quad)$ de $\left[\begin{smallmatrix} u \\ \varphi \end{smallmatrix}\right]$ de la façon suivante .

i) Si $\varphi = 0$

$$a(r) = \begin{cases} 0 & \text{si } r \neq \pm\, 1/2n \\ a(1/2u) = -a(-1/2u) = 1 \end{cases} \tag{6.17}$$

ii) Si $\varphi \neq 0$, il existe un unique générateur $\tau_o \in \mu_n$ tel que $\varphi(\tau_o) = 1$ et

$$a(r) = \tau_o^{ur^2 - r} - \tau_o^{ur^2 + r} \tag{6.18}$$

Preuve : Ces formules résultent immédiatement de (6.5) et (6.14) .

Théorème 6.17 : Soit k une $\mathbb{Z}\left[1/n\right]\left[\mu_n\right]$- algèbre à spectre connexe. Les pointes de $\mathcal{C}(k)$ sont les seuls points de $\mathcal{C}(k)$ dont le stabilisateur dans $\mathrm{Sp}(\mathbb{Z}/n\mathbb{Z} \times \mu_n)(k)$ ait un ordre divisible par n.

Preuve : D'après le lemme 6.9 et la définition 6.11 nous savons que le stabilisateur dans $\mathrm{Sp}(\mathbb{Z}/n\mathbb{Z} \times \mu_n)(k)$ d'une pointe possède 2n éléments. Réciproquement, soit $a \in \mathcal{C}(k)$ ayant dans $\mathrm{Sp}(\mathbb{Z}/n\mathbb{Z} \times \mu_n)(k)$ un stabilisateur dont l'ordre est divisible par le nombre premier n. Alors, il existe dans ce stabilisateur un élément d'ordre n qui est conjugué dans $\mathrm{Sp}(\mathbb{Z}/n\mathbb{Z} \times \mu_n)(k)$ d'une matrice de la forme $\left(\begin{smallmatrix} 1 & \zeta \\ 0 & 1 \end{smallmatrix}\right)$ avec ζ un générateur de μ_n. (Ceci résulte du fait que $\mathrm{Sp}(\mathbb{Z}/n\mathbb{Z} \times \mu_n)(k)$ est isomorphe au groupe $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ pour lequel cette propriété est bien connue). Nous en

déduisons que le point a est le transformé par un élément de $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)(k)$ d'un point de $\mathcal{A}(k)$ laissé fixe par la matrice $\begin{pmatrix} 1 & \zeta \\ 0 & 1 \end{pmatrix}$. Nous sommes donc ramenés à l'étude de ce cas. Supposons donc $a \in \mathcal{A}(k)$ tel que $\sigma a = a$ avec $\sigma = \begin{pmatrix} 1 & \zeta \\ 0 & 1 \end{pmatrix}$. D'après (6.5) il existe une constante λ inversible telle que

$$\lambda a(r) = \zeta^{r^2} a(r)$$

pour tout $r \in \mathbb{Z}/n\mathbb{Z}$. Ceci n'est possible que si tous les $a(r)$ sauf deux, que nous notons $a(i_o)$ et $a(-i_o)$ sont nuls. Par conséquent, a est la pointe $\left[\begin{smallmatrix} 1/2i_o \\ 0 \end{smallmatrix}\right]$ de $\mathcal{A}$ (d'après (6.17)) et le théorème est démontré.

Lemme 6.18 : Soit k une $\mathbb{Z}[1/n]$-algèbre qui soit un corps. Si $a = (a(0) : a(1) : \quad) \in \mathcal{A}(k)$ n'est pas une pointe rationnelle alors

$$a(i) \neq 0 \quad \text{pour tout } i \neq 0 .$$

Preuve : Si a n'est pas une pointe rationnelle d'après (6.17) il existe I et J dans $\mathbb{Z}/n\mathbb{Z}$ tels que $a(I) \neq 0$, $a(J) \neq 0$ et $I \neq \pm J$. Admettons pour un instant le lemme suivant :

Lemme 6.19 : Soit $b = (b(0) : b(1) : \quad) \in \mathcal{A}(k)$. Si b(I) et b(J) sont différents de zéros avec $I \neq \pm J$ alors $b((I+J)/2)$ et $b(I/2)$ ne sont pas nuls.

Par récurrence, il résulte de ce lemme que pour tout $m \geq 0$ et tout r tel que

$$0 \leq r \leq 2^m \quad \text{et} \quad I + r(I-J)^{-2m} \neq 0$$

nous avons $b(I + r(I-J)^{-2m}) \neq 0$. Or, quand $2^m > n$, quel que soit $s \in \mathbb{Z}/n\mathbb{Z}$, il existe un entier r tel que

$$I + r(I-J)2^{-m} = s \qquad (\text{car } I - J \neq 0)$$

Par conséquent, pour tout $s \in \mathbb{Z}/n\mathbb{Z} - \{0\}$, nous avons $b(s) \neq 0$ ce qui démontre le lemme 6.18 en prenant $b = a$.

Démonstration du lemme 6.19 : Posons $\rho = (I + J)/2$ et supposons $b(\rho) = 0$. A tout élément t de $\mathbb{Z}/n\mathbb{Z}$ associons le sextuplet

$$\mathcal{J} = (i_1, j_1, i_2, j_2, i_3, j_3)$$

défini par les équations

$$i_1 = I + t\rho \qquad j_1 = I + (t-2)\rho$$

$$i_2 = -\rho \qquad j_2 = 2I + (2t-1)\rho$$

$$i_3 = I + (t-1)\rho \qquad j_3 = I + (t-1)\rho$$

Nous avons $i_1 + j_1 = i_2 + j_2 = i_3 + j_3$ et

$$0 = R_{\mathcal{J}}(b) = b(I + t\rho)^3 b(I + (t-2)\rho) + b(-I - (t+1)\rho) b(I + (t-1)\rho)^3$$

soit encore

$$b(I + t\rho)^3 b(I + (t-2)\rho) = b(I + (t+1)\rho) b(I + (t-1)\rho)^3 ,$$

pour tout $t \in \mathbb{Z}/n\mathbb{Z}$.
Comme $b(I)b(J) = -b(I)\, b(I-2\rho) \neq 0$ nous voyons par récurrence sur t que

$$b(I + t\rho) \neq 0 \quad \text{pour tout } t$$

et comme $I + t\rho$ parcourt $\mathbb{Z}/n\mathbb{Z}$ puisque $\rho \neq 0$ nous avons $b(i) \neq 0$ pour tout $i \in \mathbb{Z}/n\mathbb{Z}$ ce qui est en contradiction avec $b(0) = 0$. Donc $b(\rho) = b((I+J)/2) \neq 0$.

Maintenant nous pouvons remplacer J par -J et refaire le raisonnement précédent. Nous obtenons que $b(I-J)/2) \neq 0$. Enfin, comme $I/2 = ((I+J)/2 + (I-J)/2)/2$ nous avons aussi $b(I/2)$ ce qui prouve le lemme.

Nous en tirons immédiatement le corollaire suivant :

Corollaire 6.20 : Soit $i \in \mathbb{Z}/n\mathbb{Z} - \{0\}$. L'ouvert de $\mathcal{C}$ défini par la condition a(r) inversible est le complémentaire dans $\mathcal{C}$ des $(n-3)/2$ sections $\left[{}^{u}_{0}\right]$ où $u \neq \pm 1/2r$.

CHAPITRE 7

Le schéma $\mathcal{V}$.

Nous désignons par (A(o):A(1): :A(n-1),X(o):X(1): :X(n-1)) les coordonnées projectives d'un point de $\mathbb{P}^{n-1} \times \mathbb{P}^{n-1}$.

7.1 Le schéma $\mathcal{V}$

A tout sextuplet $I=(i_1,j_1,i_2,j_2,i_3,j_3)$ d'éléments de $\mathbb{Z}/n\mathbb{Z}$ tels que

$$i_1+j_1 = i_2+j_2 = i_3+j_3$$

nous associons le polynôme de $\mathbb{Z}[1/n]$ $[A(i),X(j)]$

$$\begin{aligned}\mathcal{S}_I = {} & A(i_3-i_2)A(j_3-i_2)X(i_1)X(j_1) \\ & + A(i_1-i_3)A(j_1-i_3)X(i_2)X(j_2) \\ & + A(i_2-i_1)A(j_2-i_1)X(i_3)X(j_3)\end{aligned} \tag{7.1}$$

Définition 7.1 : Nous notons $\mathcal{V}$ le sous-schéma de $\mathbb{P}^{n-1} \times \mathbb{P}^{n-1}$, au-dessus de $\mathbb{Z}[1/n]$, des zéros communs aux polynômes (7.1) et (6.12).
La première projection $\mathbb{P}^{n-1} \times \mathbb{P}^{n-1} \longrightarrow \mathbb{P}^{n-1}$ induit un morphisme que nous noterons p de $\mathcal{V}$ dans $\mathcal{A}$. Soit k une $\mathbb{Z}[1/n]$-algèbre, la fibre $\mathcal{V}_a$ en un point a = (a(o):a(1):) de $\mathcal{A}(k)$ est le sous-schéma de $\mathbb{P}^{n-1}(k)$ défini par les relations

$$\begin{aligned}& a(i_3-i_2)a(j_3-i_2)X(i_1)X(j_1) \\ & + a(i_1-i_3)a(j_1-i_3)X(i_2)X(j_2) \\ & + a(i_2-i_1)a(j_2-i_1)X(i_3)X(j_3) = 0\end{aligned}$$

Remarque : Si deux des trois ensembles, $\{i_1,j_1\}$, $\{i_2,j_2\}$, $\{i_3,j_3\}$ sont égaux, le polynôme $\mathcal{S}_I$ est dans l'idéal engendré par les polynômes R'_o et R_i de (6.12)

7.2 Le groupe $\mathcal{V}_n$

On vérifie immédiatement

Lemme 7.2 : Soit k une $\mathbb{Z}[1/n]$-algèbre et soient $r \in \mathbb{Z}/n\mathbb{Z}$ et $\zeta \in \mu_n(k)$. Pour tout point $a = (a(0) : a(1) : \quad)$ de $\mathcal{A}(k)$ le point $(a, (\alpha(0) : \alpha(1) : \quad))$ de $\mathcal{A} \times \mathbb{P}^{n-1}$ avec

$$\alpha(i) = \zeta^{-i} a(i-r) \tag{7.2}$$

est dans $\mathcal{V}_a(k)$.

Définition 7.3 : Nous notons s le $\mathcal{A}$-morphisme de schéma de $\mathcal{A} \times \mathbb{Z}/n\mathbb{Z} \times \mu_n$ dans $\mathcal{V}$ défini par

$$(a, r, \zeta) \xrightarrow{s} (a, (\alpha(0) : \alpha(1) : \quad))$$

avec $\alpha(i) = \zeta^{-i} a(i-r)$.

Théorème 7.4 : Le morphisme s est une immersion fermée. En particulier, si k désigne une $\mathbb{Z}[1/n]$-algèbre non nulle, les sections de $\mathcal{V} \xrightarrow{p} \mathcal{A}$ définies par

$$a \xrightarrow{(r,\zeta)} s(a, r, \zeta)$$

ne se rencontrent pas.

Preuve : Supposons qu'il existe $a = (a(o) : a(1) : \quad)$ dans $\mathcal{A}(k)$, (r, ζ) et (r_1, ζ_1) dans $(\mathbb{Z}/n\mathbb{Z} \times \mu_n)(k)$ tels que

$$s(a, r, \zeta) = s(a, r_1, \zeta_1) .$$

Ceci signifie qu'il existe λ inversible tel que

$$\zeta^{-i} a(i-r) = \lambda \zeta_1^{-i} a(i-r_1) \tag{7.3}$$

pour tout $i \in \mathbb{Z}/n\mathbb{Z}$.

En posant $\rho = r-r_1$ et en changeant d'indice dans (7.3) nous obtenons

$$(\zeta/\zeta_1)^{-i-r}a(i) = \lambda\ a(i+\rho)$$

et plus généralement

$$(7.4) \qquad (\zeta/\zeta_1)^{-t(i+r)-\frac{t(t-1)\rho}{2}}a(i) = \lambda^t a(i+t\rho)$$

pour tous i et t dans $\mathbb{Z}/n\mathbb{Z}$.

Posons d'abord i = 0 ce qui nous donne

$$a(t\rho) = 0 \qquad \text{pour tout } t \in \mathbb{Z}/n\mathbb{Z}.$$

Si ρ n'était pas nul, nous en déduirions a(i) = 0 pour tout i ce qui est impossible, par conséquent $\rho = 0$ et la relation (7.4) devient

$$(7.5) \qquad (\zeta/\zeta_1)^{-t(i+r)}a(i) = \lambda^t a(i)$$

pour tout $t \in \mathbb{Z}/n\mathbb{Z}$ et tout $i \in \mathbb{Z}/n\mathbb{Z}$. Il existe i_o tel que $a(i_o)$ soit inversible ainsi que $a(-i_o) = -a(i_o)$. Nous avons

$$(\zeta/\zeta_1)^{-t(i_o+r)} = \lambda^t \qquad \text{et}$$
$$(\zeta/\zeta_1)^{-t(-i_o+r)} = \lambda^t$$

pour tout $t \in \mathbb{Z}/n\mathbb{Z}$ d'où nous déduisons

$$(\zeta/\zeta_1)^{2i_o t} = 1 \quad \text{pour tout } t.$$

Comme $2i_o \neq 0$ il en résulte que $\zeta/\zeta_1 = 1$ ce qui montre que $(r,\zeta) = (r_1,\zeta_1)$.

<u>Définition</u> 7.5 : Nous notons $\mathscr{V}_n$ le sous-schéma de $\mathscr{V}$ image de l'immersion s. Nous le munissons d'une structure de $\mathcal{O}$-schéma en groupe, image de celle de $\mathbb{Z}/n\mathbb{Z} \times \mu_n$. La loi de composition, notée additivement, est donnée par

$$s(a,r,\zeta) + s(a,r_1,\zeta_1) = s(a,r+r_1,\zeta\zeta_1)$$

Nous notons 0 la section $a \longmapsto s(a,0,1)$, g' la section $a \longmapsto s(a,1,1)$ et g_ζ la section $a \longmapsto s(a,0,\zeta)$ de sorte que la section $rg' + g_\zeta$ n'est autre que

$$a \longmapsto s(a,r,\zeta).$$

Il nous arrivera souvent d'écrire

$$s(a,r,\zeta) = (rg'+g_\zeta)_a \quad .$$

Enfin, nous munissons le schéma $\mathbb{Z}/n\mathbb{Z} \times \mu_n$ d'une forme ε_n, bilinéaire, alternée, non dégénérée, à valeurs dans le schéma en groupes μ_n, en posant

$$\varepsilon_n((r,\zeta) , (r_1,\zeta_1)) = \zeta_1^r \zeta^{-r_1}$$

Nous en déduisons sur le $\mathcal{C}$-schéma $\mathcal{V}_n$ une forme e_n, bilinéaire, alternée, non dégénérée, à valeurs dans le $\mathcal{C}$-schéma en groupes $\mathcal{C} \times \mu_n$.
Nous avons

$$e_n(s(a,r,\zeta), s(a,r_1,\zeta_1)) = (a, \zeta_1^r \zeta^{-r_1}) \tag{7.6}$$

Lemme 7.6 : Soit k une $\mathbb{Z}[1/n]$-algèbre qui soit un corps. Soit $a \in \mathcal{C}(k)$ et supposons que a ne soit pas une pointe rationnelle.
Si $P = (a,(\alpha(o):\alpha(1): \quad))$ appartenant à $\mathcal{V}_a(k)$ est tel que $\alpha(r) = 0$, il existe $\zeta \in \mu_n(k)$ tel que $P = (rg' + g_\zeta)_a$

Preuve : Montrons qu'il est impossible de trouver i_1 et i_2 avec $i_1 \neq i_2$ tels que $\alpha(i_1) = \alpha(i_2) = 0$. Si de tels i_1 et i_2 existaient, nous aurions

$$a(i_2-i_1)\ a(i_3+j_3-i_2-i_1)\ \alpha(i_3)\ \alpha(j_3) = 0$$

pour tous i_3 et j_3 dans $\mathbb{Z}/n\mathbb{Z}$. en effet, il suffit de considérer le sextuplet $I = (i_1,j_1,i_2,j_2,i_3,j_3)$ où

$$j_1 = i_3+j_3-i_1$$
$$j_2 = i_3+j_3-i_2$$
et i_3 et j_3 sont quelconques

et d'écrire que $\mathcal{Y}_I(P) = 0$.

Comme nous avons supposé que a n'est pas une pointe rationnelle, nous savons d'après le lemme 6.18 que $a(i) \neq 0$ pour tout $i \neq 0$.
Par conséquent, $\alpha(i_3)\alpha(j_3) = 0$ pour tous i_3 et j_3 dans $\mathbb{Z}/h\mathbb{Z}$ tels que $i_3+j_3-i_1-i_2 \neq 0$ (puisque dans ce cas $a(i_3+j_3-i_1-i_2)a(i_1-i_1) \neq 0$).
Soit i_3 tel que $\alpha(i_3) \neq 0$. Alors $\alpha(j_3) = 0$ pour tout j_3 tel que $j_3 \neq i_1+i_2-i_3$. En particulier, si i_3 était différent de $(i_1+i_2)/2$ nous aurions $i_3 \neq i_1+i_2-i_3$ et $\alpha(i_3) = 0$ ce qui est faux; donc $i_3 = (i_1+i_2)/2$.
Nous avons démontré que si i_1 et i_2 sont tels que $\alpha(i_1) = \alpha(i_2) = 0$ avec $i_1 \neq i_2$ alors $\alpha(j) = 0$ pour tout $j \neq (i_1+i_2)/2$. Il est facile d'en déduire que $\alpha(j) = 0$ pour $j \in \mathbb{Z}/n\mathbb{Z}$; ce qui est exclu.
Par conséquent, le nombre r mentionné dans l'énoncé du lemme est le seul élément de $\mathbb{Z}/n\mathbb{Z}$ tel que $\alpha(r) = 0$.

Soit $I = (r, j, i_2+r, j_2+r, i_3+r, j_3+r)$ un sextuplet d'éléments de $\mathbb{Z}/n\mathbb{Z}$ tels que

$$j = i_2+j_2+r = i_3+j_3+r$$

La relation $\mathcal{Y}_I(P) = 0$ nous donne

$$a(i_2)\, a(j_2)\, \alpha(i_3+r)\, \alpha(j_3+r) = a(i_3)\, a(j_3)\, \alpha(i_2+r)\, \alpha(j_2+r) \tag{7.7}$$

et cette égalité est vraie pour tous i_2, j_2, i_3, j_3 dans $\mathbb{Z}/n\mathbb{Z}$ tels que

$$i_2+j_2 = i_3+j_3 \ .$$

Nous en déduisons

$$a(i)\ a(2)\ \alpha(r+1)\ \alpha(i+r+1) = a(1)\ a(i+1)\ \alpha(i+r)\ \alpha(r+2)$$

pour tout $i \in \mathbb{Z}/n\mathbb{Z}$, et puisque $\alpha(r)$ est le seul α à être nul nous en tirons

$$\frac{\alpha(i+r+1)}{a(i+1)} = \frac{a(1)}{a(2)} \cdot \frac{\alpha(r+2)}{\alpha(r+1)} \cdot \frac{\alpha(i+r)}{a(i)}$$

puis, par récurrence sur i,

$$\frac{\alpha(i+r)}{a(i)} = \frac{\alpha(r+1)}{a(1)} \cdot \left(\frac{\alpha(r+2)}{\alpha(r+1)} \cdot \frac{a(1)}{a(2)} \right)^{i-1}$$

pour tout entier i tel que $1 \leq i \leq n-1$, ceci nous donne, à un multiple constant non nul près,

$$\alpha(r+i) = \zeta^{-i} a(i) \tag{7.8}$$

pour tout i tel que $1 \leq i \leq n-1$ avec

$$\zeta = \frac{\alpha(r+2)}{\alpha(r+1)} \cdot \frac{a(1)}{a(2)} \quad .$$

Si nous reportons (7.8) dans (7.7) avec des valeurs convenables de i_2, j_2, i_3, j_3 nous trouvons $\zeta^n = 1$, ce qui montre que $\zeta \in \mu_n(k)$ et que la relation (7.8) est vraie pour tout $i \in \mathbb{Z}$. Nous en tirons

$$\alpha(i) = \zeta^{-i} a(i-r) \ ,$$

pour tout $i \in \mathbb{Z}/n\mathbb{Z}$ ce qui est une autre façon d'écrire $P = (rg' + g_\zeta)_a$.

7.3 Actions de $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$ sur $\mathcal{V}$.

Faisons agir $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$ sur $\mathbb{P}^{n-1} \times \mathbb{P}^{n-1}$ en opérant sur chaque facteur comme il a été dit en (6.5). Nous avons vu que cette action laisse stable $\mathcal{A} \times \mathbb{P}^{n-1}$; nous allons voir qu'elle laisse stable $\mathcal{V} \subset \mathcal{A} \times \mathbb{P}^{n-1}$ ce qui nous montre que $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$ opère sur le morphisme $\mathcal{V} \xrightarrow{p} \mathcal{A}$.

Proposition 7.7 : Soit k une $\mathbb{Z}[1/n]$-algèbre et soient $a \in \mathcal{A}(k)$, $\sigma \in Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)(k)$ et $P \in \mathcal{V}_a(k)$.
Alors le point σP défini par (6.5) appartient à $\mathcal{V}_{\sigma a}(k)$.

Preuve : Il suffit de recopier mutatis mutandis la démonstration de la proposition 6.6

Nous en déduisons que $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$ opère sur les sections de $\mathcal{V} \xrightarrow{p} \mathcal{A}$. En particulier, faisons agir la matrice $\sigma = \begin{pmatrix} u & \xi \\ \varphi & v \end{pmatrix}$ de $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$ sur $\mathbb{Z}/n\mathbb{Z} \times \mu_n$ par

$$(7.9) \qquad (r,\zeta) \xmapsto{\sigma} (r,\zeta)\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix} = (ur + 2^{-1}\varphi(\zeta), \zeta^v \xi^{2r})$$

Alors,

Proposition 7.8 : Cette opération donne un isomorphisme entre $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$ et le sous-groupe des automorphismes de $\mathbb{Z}/n\mathbb{Z} \times \mu_n$ qui respectent la forme bilinéaire ε_n.

Il est clair que cette opération donne une injection de $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$ dans le groupe des automorphismes de $\mathbb{Z}/n\mathbb{Z} \times \mu_n$ et la condition (6.1) permet d'en déterminer l'image.

Proposition 7.9 : L'immersion s du corollaire 7.3 est compatible avec l'action de $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$ sur $\mathbb{Z}/n\mathbb{Z} \times \mu_n$, $\mathcal{A}$ et $\mathcal{V}$. Autrement dit, $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$ opère sur $\mathcal{V}_n$ de façon compatible avec le morphisme $\mathcal{V}_n \longrightarrow \mathcal{A}$ et

$$(7.10) \qquad \sigma^{-1}(rg' + g_\zeta)_{\sigma a} = \left((ur + 2^{-1}\varphi(\zeta))g' + g_{\zeta^v \xi^{2r}} \right)_a$$

Enfin, l'action de $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$ respecte la forme e_n .

Preuve : Pour démontrer cette proposition, il suffit de vérifier (7.10) et pour vérifier (7.10) il suffit de considérer les cas où $\sigma = T = \begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix}$ et $\sigma = S = \begin{pmatrix} 0 & \xi \\ \varphi & 0 \end{pmatrix}$.

Soit $a = (a(o):a(1):\quad)$ un point de $\mathcal{C}$.

Posons $\sigma a = (a'(o):a'(1):\quad)$

puis $(rg'+g_\zeta)_{\sigma a} = (\sigma a,(\alpha'(o):\alpha'(1):\quad))$

et $\sigma^{-1}(rg'+g_\zeta)_{\sigma a} = (a,(\alpha(o):\alpha(1):\quad))$

Premier cas : $\sigma = T = \begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix}$. La formule (6.5) nous donne successivement

$$a'(i) = \xi^{i^2} a(i)$$

$$\alpha'(i) = \zeta^{-i}\, \xi^{(i-r)^2} a(i-r)$$

$$\alpha(i) = \xi^{r^2}(\zeta\xi^{2r})^{-i} a(i-r)$$

et cette dernière relation signifie que

$$T^{-1}(rg'+g_\zeta)_{Ta} = (rg'+g_{\xi^{2r}\zeta})_a$$

ce qui prouve (7.10) dans ce cas.

Deuxième cas : $\sigma = S = \begin{pmatrix} 0 & \xi \\ \varphi & 0 \end{pmatrix}$. La formule (6.5) nous donne successivement

$$a'(i) = \sum_{\tau\in\mu_n} \xi^{2i\varphi(\tau)} a(\varphi(\tau))$$

$$\alpha'(i) = \zeta^{-i}\left(\sum_\tau \xi^{2(i-r)\varphi(\tau)} a(\varphi(\tau))\right)$$

$$\alpha(i) = \sum_{\tau'\in\mu_n} \xi^{-2i\varphi(\tau')}\left(\zeta^{\varphi(\tau')}\sum_{\tau\in\mu_n} \xi^{2(-\varphi(\tau')-r)\varphi(\tau)} a(\varphi(\tau))\right)$$

Nous pouvons récrire cette égalité

$$a(i) = \sum_\tau \xi^{-2r\varphi(\tau)} a(\varphi(\tau))\left[\sum_{\tau'} \xi^{-2i\varphi(\tau')-2\varphi(\tau)\varphi(\tau')}\zeta^{\varphi(\tau')}\right]$$

La quantité entre crochets est nulle sauf si $\xi^{-2i-2\varphi(\tau)}\zeta = 1$ et vaut n dans ce cas.

Comme $\varphi(\xi) = -1$ nous avons $\xi^{-\varphi(\tau)} = \tau$ et

$\alpha(i) = \xi^{r\varphi(\zeta)}\xi^{-2ir} a(i-2^{-1}\varphi(\zeta))$ ce qui signifie

$$S^{-1}(rg'+g_{\zeta})_{Sa} = (2^{-1}\varphi(\zeta)g'+g_{\xi 2r})_a$$

et prouve (7.10) dans ce cas.

Remarque : Nous pouvons illustrer la formule (7.10) par

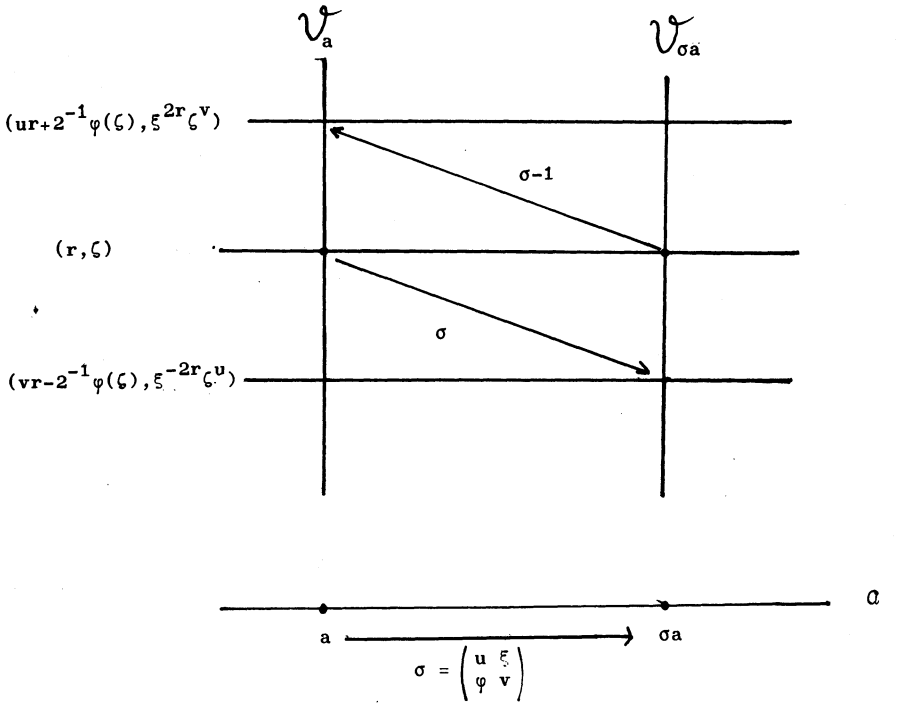


Tableau (7.11) .

Si a est un point de $\mathcal{Q}$ et si σ est une matrice de $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$ qui stabilise a , la matrice σ opère sur la fibre $\mathcal{V}_a$.

Théorème 7.11 : La matrice $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ de $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$ opère trivialement sur $\mathcal{Q}$ et opère sur $\mathcal{V}$ en envoyant le point $P = (a,(\alpha(o):\alpha(1): \quad))$ de $\mathcal{V}$ sur le point noté $(-P) = (a,(\alpha'(o):\alpha'(1) \quad))$ défini par

$$\alpha'(i) = \alpha(-i)$$

pour tout $i \in \mathbb{Z}/n\mathbb{Z}$.

Preuve : Il suffit d'écrire (6.5) avec $\sigma = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

CHAPITRE 8

Les fibres singulières de $\mathcal{V}$

Nous étudions maintenant les fibres de $\mathcal{V}$ au-dessus des pointes de $\mathbb{C}$. Au chapitre 9 nous verrons que ce sont les seules fibres singulières de $\mathcal{V}$ ce qui justifie le titre donné au présent chapitre.

8.1 Les n-gones

Définition 8.1 : Nous appelons n-gone un sous-$\mathbb{Z}[1/n]$-schéma de $\mathbb{P}^{n-1}$ qui soit sur $\mathbb{Z}[1/n][\mu_n]$ la réunion de n droites projectives $(\Delta_i)_{i \in \mathbb{Z}/n\mathbb{Z}}$ telles que

$$\Delta_i \cap \Delta_j = \emptyset \quad \text{si} \quad i-j \notin \{0,1,-1\}$$

et $\Delta_i \cap \Delta_{i+1}$ soit une section.

Un n-gone est une courbe propre et plate de genre arithmétique 1 au-dessus de $\mathbb{Z}[1/n]$.

Définition 8.2 : Soient i et $j \in \mathbb{Z}/n\mathbb{Z}$ tels que $i \neq j$. Nous notons $D_{i,j}$ la droite de $\mathbb{P}^{n-1}$ définie par les (n-2) équations

$$X_s = 0 \quad \text{avec} \quad s \neq i \text{ et } j \; . \tag{8.1}$$

Lemme 8.3 : La réunion des n droites $\Delta_i = D_{i-1/2,i+1/2}$ où i parcourt $\mathbb{Z}/n\mathbb{Z}$ est un n-gone. Son idéal est engendré par les monômes X_iX_j tels que $i-j \notin \{0,1,-1\}$.

Preuve : La droite Δ_i est l'ensemble des points de $\mathbf{P}^{n-1}$ de coordonnées projectives $(\alpha(0) : \alpha(1) : \quad)$ telles que

$$\alpha(r) = 0 \qquad \text{si} \quad r \neq i \pm 1/2$$

Par conséquent, $\Delta_i \cap \Delta_{i+1}$ est réduit au point que nous noterons $M_{i+1/2}$ (le point M_j a pour coordonnées projectives $(\alpha(0) : \alpha(1) : \quad)$ avec $\alpha(r) = 0$ si $r \neq j$ et, $\alpha(j)$ inversible). De plus, $\Delta_i \cap \Delta_j$ est vide si $i-j \notin \{0,1,-1\}$.

Notons I l'idéal engendré par les monômes $X_u X_v$ tels que $u-v \notin \{0,1,-1\}$. L'idéal I_i qui définit la droite Δ_i est engendré par les X_u tels que $u \neq i \pm 1/2$. Par conséquent, $X_u X_v \in I_i$ si $u - v \notin \{0,1,-1\}$. et nous avons $I \subset \bigcap_i I_i$. Réciproquement, soit $P \in \bigcap_i I_i$. Les monômes de P qui ne sont pas dans I_i sont de la forme

$$(8.2) \qquad X_{i-1/2}^a \ , \quad X_{i+1/2}^a \ , \quad X_{i-1/2}^a X_{i+1/2}^b$$

Comme l'idéal I_i ne contient pas de combinaison linéaire de ces polynômes autre que 0, et comme P est dans I_i nous voyons que P ne contient pas de monôme de la forme (8.2). Le raisonnement étant valable pour tout $i \in \mathbb{Z}/n\mathbb{Z}$, le polynôme P est combinaison linéaire de monômes appartenant à I et nous avons $\bigcap_i I_i \subset I$. Il en résulte que $I = \bigcap_i I_i$ et le lemme 8.3 est démontré.

8.2 La fibre $\mathcal{V}_{\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]}$.

Théorème 8.4 : Le schéma $\mathcal{V}_{\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]}$ est le n-gone défini au lemme 8.3.

Preuve : Le schéma $\mathcal{V}_{\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]}$ est le sous-schéma de $\mathbf{P}^{n-1}$ défini par les équations

$$a(i_3-i_2)a(j_3-i_2)X(i_1)X(j_1)$$
$$+ a(i_1 - i_3)a(j_1 - i_3)\ X(i_2)\,X(j_2)$$
$$+ a(i_2 - i_1)\,a(j_2 - i_1)\,X(i_3)\,X(j_3) = 0 \quad ,$$

où $a(r) = 0$ quand $r \neq \pm 1/2$. Celles qui ne se réduisent pas à l'idendité $0 = 0$ ont au moins un de leurs trois monômes différents de zéro. Si nous supposons que c'est le premier, ce que nous pouvons toujours faire, nous trouvons que ce sont les équations

$$(8.2) \qquad a_{1/2}^2 X_u X_v + a((-u+v-1)/2)a((-u+v+1)/2) X((u+v)/2)^2 + a((u-v)/2)a((-u+v)/2)X((u+v-1)/2)X((u+v+1)/2)=0$$

obtenues en résolvant les quatre systèmes

$$i_3-i_2 = \pm 1/2 , \quad i_3 - j_2 = \pm 1/2 , \quad i_1 = u, \quad j_1 = v .$$

Si $u - v \in \{0,1,-1\}$ le membre de gauche de (8.2) est identiquement nul. Par contre, si $u - v \notin \{0,1,-1\}$ l'équation (8.2) se réduit à

$$(8.3) \qquad X_u X_v = 0$$

ce qui montre que $\mathcal{V}_{\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]}$ est le n-gone défini au lemme 8.3.

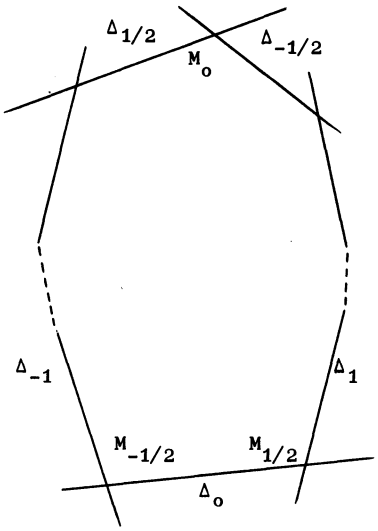
Il résulte de ce théorème que $\mathcal{V}_{\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]}$ est la réunion des n droites Δ_i d'équations $X_u = 0$ pour tout $u \neq i \pm 1/2$ et que $\mathcal{V}_{\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]}$ possède n points singuliers $(M_j)_{j \in \mathbb{Z}/n\mathbb{Z}}$ ayant pour coordonnées projectives $(\alpha_j(0) : \alpha_j(1) : \quad)$ avec

$$(8.4) \qquad \alpha_j(r) = 0 \quad \text{si } r \neq j \quad \text{et}$$

$$\alpha_j(j) \text{ est inversible .}$$

Enfin, $M_{i+1/2}$ est l'intersection de Δ_i et Δ_{i+1} .

<u>Remarque</u> : Toutes les composantes de $\mathcal{V}_{\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]}$ sont rationnelles sur $\mathbb{Z}[1/n]$.



(8.5) <u>La fibre de</u> $\mathcal{V}_{\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]}$ <u>au-dessus d'un point de</u> $\mathbb{Z}\left[1/n\right]$.

Nous notons $\tilde{\mathcal{V}}_{\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]}$ l'ouvert de $\mathcal{V}_{\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]}$ complémentaire des n points singuliers.

<u>Proposition 8.5</u> : i) $(\mathcal{G}_n)_{\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]} \subset \tilde{\mathcal{V}}_{\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]}$.

ii) <u>Soient</u> k <u>une</u> $\mathbb{Z}\left[1/n\right]$ - <u>algèbre à spectre connexe</u> $r \in \mathbb{Z}/n\mathbb{Z}$ <u>et</u> $\zeta \in \mu_n(k)$. <u>Le point</u> $(rg' + g_\zeta)_{\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]}$ <u>de</u> $(\mathcal{G}_n)_{\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]}(k)$ <u>est dans</u> $\Delta_r(k)$.

<u>Preuve</u> : On obtient cette proposition en reportant les coordonnées de $(rg' + g_\zeta)_{\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]}$ données par la définition 7.3 dans les équations de Δ_i, et en comparant ces coordonnées à celles des points singuliers de $\mathcal{V}_{\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]}$ données par (8.4).

Définition 8.6 : Nous notons $C(\begin{bmatrix}1\\0\end{bmatrix})$ le sous-schéma en groupe de $(\mathcal{V}_n)_{\begin{bmatrix}1\\0\end{bmatrix}}$ égal à

$$\Delta_o \cap (\mathcal{V}_n)_{\begin{bmatrix}1\\0\end{bmatrix}} .$$

Le groupe $C(\begin{bmatrix}1\\0\end{bmatrix})$ est isomorphe à μ_n et la proposition 8.5 affirme que la droite Δ_r contient le translaté de $C(\begin{bmatrix}1\\0\end{bmatrix})$ par $(rg')_{\begin{bmatrix}1\\0\end{bmatrix}}$.

Soit k une $\mathbb{Z}[1/n]$-algèbre et soit $\sigma = \begin{pmatrix} u & \zeta \\ 0 & u \end{pmatrix}$ un point de $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)(k)$. Comme la matrice σ laisse fixe $\begin{bmatrix}1\\0\end{bmatrix} \in \mathcal{C}(k)$ elle opère sur $\mathcal{V}_{\begin{bmatrix}1\\0\end{bmatrix}}(k)$.

Nous verrons comment au chapitre 9. En attendant énonçons

Proposition 8.8 : i) Si $u = 1$, σ opère sur $\mathcal{V}_{\begin{bmatrix}1\\0\end{bmatrix}}(k)$ en envoyant chaque composante $\Delta_i(k)$ sur elle-même.

ii) $u = -1$, σ opère sur $\mathcal{V}_{\begin{bmatrix}1\\0\end{bmatrix}}(k)$ en envoyant $\Delta_i(k)$ sur $\Delta_{-i}(k)$.

Preuve : Pour démontrer cette proposition il suffit de prendre un point P de $\mathcal{V}_{\begin{bmatrix}1\\0\end{bmatrix}}(k)$ porté par Δ_i et de regarder quelle est son image par σ en utilisant (6.5).

8.3 Les fibres singulières

Théorème 8.9 : Soit a une pointe de $\mathcal{C}$. Le schéma $\mathcal{V}_a$ est un n-gône. Si la matrice σ de $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$ est telle que $a = \sigma\begin{bmatrix}1\\0\end{bmatrix}$ les composantes de $\mathcal{V}_a$ sont les n droites $\sigma\Delta_i$.

Preuve : Soit k une $\mathbb{Z}[1/n]$-algèbre et soit a une pointe de $\mathcal{C}(k)$. S'il existe $\sigma \in Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)(k)$ telle que

$$a = \sigma\begin{bmatrix}1\\0\end{bmatrix}$$

nous avons $\mathcal{V}_a(k) = \sigma\, \mathcal{V}_{\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]}(k)$ et le théorème est démontré dans ce cas. Le cas général s'en déduit par descente.

Définitions 8.10 : i) Nous tirons de la proposition 8.8 et du théorème 8.9 que la composante $\sigma\Delta_o$ de $\mathcal{V}_a$ ne dépend pas du choix ni de l'existence de la matrice σ telle que $a = \sigma\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$. Nous la notons $\mathcal{V}_a^\circ$.

ii) Soit k une $\mathbb{Z}[1/n][\mu_n]$-algèbre .

Nous appelons numérotage de $\mathcal{V}_a(k)$ une bijection ν entre l'ensemble des composantes de $\mathcal{V}_a(k)$ et $\mathbb{Z}/n\mathbb{Z}$ telle que

$$(8.6) \qquad \begin{cases} \nu(\mathcal{V}_a^\circ(k)) = 0 \\ \nu(\mathcal{C}) - \nu(\mathcal{C}') = \pm 1 \quad \text{si} \quad \mathcal{C} \cap \mathcal{C}' \neq \emptyset \end{cases}$$

Il est clair qu'il existe deux numérotages de $\mathcal{V}_a(k)$ et deux seulement et ces deux numérotages sont opposés l'un de l'autre.

iii) A tout numérotage de $\mathcal{V}_a(k)$ nous associons un numérotage des points singuliers en posant

$$(8.7) \qquad \nu(M) = \frac{\nu(\mathcal{C}) + \nu(\mathcal{C}')}{2} \qquad \text{si } M = \mathcal{C} \cap \mathcal{C}' .$$

Corollaire 8.11 : A chacune des deux représentations $\left[\begin{smallmatrix}u\\\varphi\end{smallmatrix}\right]$ de la pointe a dans $\mathbb{Z}/n\mathbb{Z} \times \mathrm{Hom}(\mu_n, \mathbb{Z}/n\mathbb{Z})(k)$ est associé de façon canonique l'un des deux numérotages de $\mathcal{V}_a(k)$ et cette correspondance est bijective .

Preuve : Soit $\left[\begin{smallmatrix}u\\\varphi\end{smallmatrix}\right]$ une représentation dans $\mathbb{Z}/n\mathbb{Z} \times \mathrm{Hom}(\mu_n, \mathbb{Z}/n\mathbb{Z})(k)$ de la pointe a et soient $\sigma = \left(\begin{smallmatrix}u & \zeta\\ \varphi & v\end{smallmatrix}\right)$ et $\sigma' = \left(\begin{smallmatrix}u & \zeta'\\ \varphi & v'\end{smallmatrix}\right)$ dans $\mathrm{Sp}(\mathbb{Z}/n\mathbb{Z} \times \mu_n)(k)$. La proposition 8.8 nous montre que $\sigma\Delta_i(k) = \sigma'\Delta_i(k)$ quel que soit $i \in \mathbb{Z}/n\mathbb{Z}$ et l'application $\nu : \sigma\Delta_i(k) \mapsto i$ est le numérotage de $\mathcal{V}_a(k)$ associé à la représentation $\left[\begin{smallmatrix}u\\\varphi\end{smallmatrix}\right]$. Nous voyons immédiatement que le numérotage associé à $\left[\begin{smallmatrix}-u\\-\varphi\end{smallmatrix}\right]$ est $-\nu$, ce qui démontre le corollaire.

Théorème 8.13 : Soit ν un numérotage de $\mathcal{V}_a(k)$. L'application notée $\bar{\nu}$ qui associe à chaque point de $(\mathcal{V}_n)_a(k)$ le numéro de sa composante est un homomorphisme surjectif de $(\mathcal{V}_n)_a(k)$ sur $\mathbb{Z}/n\mathbb{Z}$. Plus précisément,

si ν est associé à la représentation $\left[\begin{smallmatrix} u \\ \varphi \end{smallmatrix}\right]$ de a nous avons

$$(8.8) \qquad \bar{\nu}((rg' + g_\zeta)_a) = ur + 2^{-1}\varphi(\zeta)$$

Preuve . Prouvons (8.8). Soit $(rg' + g_\zeta)_a$ un point de $(\mathscr{V}_n)_a(k)$ et soit $\sigma = \left(\begin{smallmatrix} u & \xi \\ \varphi & v \end{smallmatrix}\right)$ dans $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)(k)$ telle que $\sigma\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] = a$. Alors la proposition 7.9 montre que

$$(rg' + g_\zeta)_a = \sigma(((ur + 2^{-1}\varphi(\zeta))g' + g_{\zeta^v \xi 2r})\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]) .$$

et comme $((ur + 2^{-1}\varphi(\zeta))g' + g_{\zeta^v \xi 2r})\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$ est porté par $\Delta_{ur+2^{-1}\varphi(\zeta)}(k)$ nous voyons que $(rg' + g_\zeta)_a$ est porté par $\sigma\Delta_{ur+2^{-1}\varphi(\zeta)}(k)$ ce qui prouve (8.8). Il est clair que $\bar{\nu}$ est un homomorphisme de $(\mathscr{V}_n)_a(k)$ dans $\mathbb{Z}/n\mathbb{Z}$, et la surjectivité de $\bar{\nu}$ résulte du fait que, soit u, soit φ, n'est pas nul.

Comme à la définition 8.6 nous notons C(a) le sous-schéma de $(\mathscr{V}_n)_a$ défini par

$$C(a) = \mathscr{V}_a^\circ \cap (\mathscr{V}_n)_a .$$

Le corollaire précédent montre que chaque composante de $\mathscr{V}_a(k)$ contient le translaté de C(a)(k) par un élément de $(\mathscr{V}_n)_a(k)$. De plus, C(a)(k) est le noyau de l'homomorphisme $\bar{\nu}$ associé à l'une quelconque des représentations de a.

Il est commode de regrouper sur un tableau les résultats obtenus dans ce chapitre. Nous désignons encore par k une $\mathbb{Z}[1/n][\mu_n]$-algèbre, par a une pointe de $\mathcal{Q}(k)$, par $\sigma = \left(\begin{smallmatrix} u & \xi \\ \varphi & v \end{smallmatrix}\right)$ une matrice dans $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)(k)$ telle que $a = \sigma\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$, par ν le numérotage de $\mathscr{V}_a(k)$ associé à la représentation $\left[\begin{smallmatrix} u \\ \varphi \end{smallmatrix}\right]$. De plus, nous notons $\mathcal{C}_i$ la composante de $\mathscr{V}_a(k)$ telle que $\nu(\mathcal{C}_i) = i$ et par M_i le point singulier de $\mathscr{V}_a(k)$ tel que $\nu(M_i) = i$. Nous avons $M_i = \mathcal{C}_{i-1/2}(k) \cap \mathcal{C}_{i+1/2}(k)$.

	$\varphi = 0$	$\varphi \neq 0$ et $\varphi(\tau) = 1$
Coordonnées projectives $(a(0) : a(1) : \quad)$ de a	$a(i) = \begin{cases} 0 & \text{si } i \neq \pm 1/2u \\ a(1/2u) = -a(-1/2u) & \text{inversible} \end{cases}$	$a(i) = \tau^{ui^2-i} - \tau^{ui^2+i}$
Equations de $\mathcal{C}_i$	$X_r = 0$ pour tout $r \neq i/u \pm 1/2u$	$\sum_{t \in \mathbb{Z}/n\mathbb{Z}} \tau^{ut^2 - 2rt} X(t) = 0$ pour tout $r \neq i \pm 1/2$
Coordonnées projectives $(m_i(0) : m_i(1) : \quad)$ de M_i	$m_i(r) = \begin{cases} 0 & \text{si } r \neq i/u \\ & \text{inversible si } r = i/u \end{cases}$	$m_i(r) = \tau^{ur^2 - 2ri}$
Coordonnées projectives $(\alpha(0) : \alpha(1) : \quad)$ de $(rg' + g_\zeta)_a$	$\alpha(i) = \begin{cases} 0 & \text{si } i \neq r \pm 1/2u \\ -\zeta^{+1/2u} & \text{si } i = r - 1/2u \\ \zeta^{-1/2u} & \text{si } i = r + 1/2u \end{cases}$	$\alpha(i) = \zeta^{-i}(\tau^{ui^2-2uir-i} - \tau^{ui^2-2uir+i})$
Groupe $C(a) = \operatorname{Ker} \bar{\nu}$	L'ensemble des $(g_\zeta)_a$ où ζ parcourt μ_n.	L'ensemble des $(-2^{-1}\varphi(\zeta)g' + g_{\zeta u})_a$ où ζ parcourt μ_n.
$(\mathcal{P}_n)_a \cap \mathcal{C}_i$	L'ensemble des translatés de $((i/u)g')_a$ par C(a)	L'ensemble des translatés de $(ivg' + g_{\zeta^{-2i}})_a$ par C(a)

Tableau (8.9)

8.4 Les ouverts Ω_i de $\mathcal{V}$

Nous démontrerons au chapitre que le morphisme $\mathcal{V} \xrightarrow{p} \mathcal{C}$ est lisse sauf aux points singuliers des fibres $\mathcal{V}_a$ au-dessus des pointes a de $\mathcal{C}$, en sorte que $\mathcal{V}_a$ est lisse lorsque a n'est pas une pointe de a.

D'ici-là, nous dirons qu'un point M de $\mathcal{V}$ est extraordinaire quand p(M) est une pointe de $\mathcal{C}$ et quand M est un point singulier de $\mathcal{V}_{p(M)}$. Tous les autres points de $\mathcal{V}$ seront dits ordinaires et nous noterons $\tilde{\mathcal{V}}$ le sous-schéma de $\mathcal{V}$ formé des points ordinaires.

Définition 8.14 : Nous noterons $\Omega(r)$ l'ouvert de $\mathcal{V}$ défini par la condition

$$X(r) \text{ inversible}$$

Les $\Omega(r)$ forment un recouvrement de $\mathcal{V}$ par des ouverts affines.

Le lemme 7.6 et les résultats du paragraphe précédent nous permettent d'énoncer les deux théorèmes suivants :

Théorème 8.15 : Soient a un point de $\mathcal{C}$ et P un point de $\mathcal{V}_a$. Nous avons les quatre possibilités suivantes (qui s'excluent mutuellement) :

i) a n'est pas une pointe rationnelle de $\mathcal{C}$.

α) P n'est pas dans $(\mathcal{O}_n)_a$. Alors

$$P \in \bigcap_i \Omega(i)$$

β) $P = (rg' + g_\zeta)_a$. Alors

$$P \in \bigcap_{i \neq r} \Omega(i) \quad \text{et} \quad P \notin \Omega(r).$$

ii) a est une pointe rationnelle de $\mathcal{C}$ et ν est le numérotage de $\mathcal{V}_a$ associé à la représentation $\begin{bmatrix} u \\ 0 \end{bmatrix}$ de a.

α) P est sur la composante dont le numéro est r et n'est pas un point singulier. Alors

$$P \in \Omega\left(\frac{r+1/2}{u}\right) \cap \Omega\left(\frac{r-1/2}{u}\right) \text{ et } P \notin \Omega(i) \text{ pour } i \neq \frac{r \pm 1/2}{u}.$$

β) P est le point singulier de numéro r. Alors $P \in \Omega(r/u)$ et $P \notin \Omega(i)$ pour $i \neq r/u$.

Théorème 8.16 : Le complémentaire de $\Omega(r)$ dans $\mathcal{V}$ est la réunion

i) de l'image dans $\mathcal{V}$ des sections de la forme $a \mapsto (rg' + g_\zeta)_a$ où ζ parcourt μ_n ;

ii) pour chaque pointe rationnelle a, de n-2 composantes de $\mathcal{V}_a$ définies de la façon suivante. Si $\left[\begin{smallmatrix} u \\ 0 \end{smallmatrix}\right]$ est la représentation de a associée au numérotage ν de $\mathcal{V}_a$, ce sont celles dont le numéro diffère de ur $\pm$ 1/2.

Définition 8.17 : Nous notons $\mathcal{B}$ le sous-schéma de $\mathcal{A}$ complémentaire des pointes rationnelles ; d'après le lemme 6.18 c'est le sous-schéma affine de $\mathcal{A}$ défini par les conditions

$$a(i) \text{ inversible } \forall\, i \neq 0.$$

Nous posons $\mathcal{W} = p^{-1}(\mathcal{B})$; c'est un sous-schéma de $\mathcal{V}$ et nous notons

$$\omega(r) = \mathcal{W} \cap \Omega(r).$$

C'est l'ouvert de $\mathcal{W}$ défini par la condition X(r) inversible et, d'après le théorème 8.16, c'est le complémentaire dans $\mathcal{W}$ des sections de la forme

$$a \mapsto (rg' + g_\xi)_a.$$

Enfin, nous notons $\tilde{\mathcal{W}}$ le complémentaire dans $\mathcal{W}$ des points extraordinaires.

CHAPITRE 9

Quotient de $\mathcal{V}$ par μ_n.

9.1 Action de $\mathcal{G}_n$ sur $\mathcal{V}$.

Nous vérifions immédiatement

Lemme 9.1 : *Soient k une $\mathbb{Z}[1/n]$-algèbre, $r \in \mathbb{Z}/n\mathbb{Z}$ et $\zeta \in \mu_n(k)$. L'automorphisme de $k[A(i),X(j)]$ défini par*

$$\begin{cases} A(i) \mapsto A(i) \\ X(j) \mapsto \zeta^{-j} X(j-r) \end{cases} \tag{9.1}$$

laisse stable l'idéal engendré par les polynômes (6.12) et (7.1).

Nous en déduisons une action de $\mathcal{G}_n$ sur $\mathcal{V}$ que nous notons additivement. Plus précisément, si $a \in \mathcal{A}(k)$ et $P = (a,(\alpha(0) : \alpha(1) : \quad)) \in \mathcal{V}_a(k)$ nous notons $(rg' + g_\zeta)_a + P$ le point de $\mathcal{V}_a(k)$ défini par

$$(rg' + g_\zeta)_a + P = (a,(\alpha'(0) : \alpha'(1) : \quad))$$

avec

$$\alpha'(i) = \zeta^{-i}\, \alpha(i-r). \tag{9.2}$$

Théorème 9.2 : *Cette action induit l'action par translation sur $\mathcal{G}_n \subset \mathcal{N}$. Autrement dit,*

$$(rg' + g_\zeta)_a + (r_1 g' + g_{\zeta_1})_a = ((r+r_1)g' + g_{\zeta\zeta_1})_a \tag{9.3}$$

De plus les actions de $\mathcal{G}_n$ et $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$ sont liées par

$$\sigma(P + u) = \sigma(P) + \sigma(u) \tag{9.4}$$

pour tous $P \in \mathcal{V}(k)$, $u \in (\mathcal{V}_n)_{p(P)}(k)$ et $\sigma \in Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)(k)$.

Preuve : La relation (9.3) s'obtient en appliquant (9.2) aux coordonnées de $(rg' + g_\zeta)_a$ données par (7.2). Pour démontrer (9.4) nous traiterons les deux cas :

$$\sigma = T = \begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad \sigma = S = \begin{pmatrix} 0 & \xi \\ \varphi & 0 \end{pmatrix} .$$

Soient $\sigma = \begin{pmatrix} u & \xi \\ \varphi & v \end{pmatrix} \in Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)(k)$, $a \in \mathcal{C}(k)$,
$P = (a, (\alpha(0) : \alpha(1) : \quad)) \in \mathcal{V}_a(k)$, $r \in \mathbb{Z}/n\mathbb{Z}$ et $\zeta \in \mu_n(k)$. Nous posons

$$\sigma(rg' + g_\zeta)_a + P = (\sigma a, (\beta(0) : \beta(1) : \quad)) \in \mathcal{V}_{\sigma a}(k)$$

et

$$\sigma(P) + \sigma((rg' + g_\zeta)_a) = (\sigma a, (\gamma(0) : \gamma(1) : \quad)) \in \mathcal{V}_{\sigma a}(k).$$

D'après (6.5), (9.2) et (7.10) nous avons

$$(9.5) \quad \beta(i) = \sum_{\tau \in \mu_n} \xi^{ui^2 + 2i\varphi(\tau)} \tau^{v\varphi(\tau)} \zeta^{-(ui + \varphi(\tau))} \alpha(ui + \varphi(\tau) - r)$$

et

$$(9.6) \quad \gamma(i) = \xi^{2ri} \zeta^{-ui} \Big(\sum_{\tau' \in \mu_n} \xi^{u(i - vr + 2^{-1}\varphi(\zeta))^2 + 2(i - vr + 2^{-1}\varphi(\zeta))\varphi(\tau')} \times$$

$$\tau'^{v\varphi(\tau')} \alpha(u(i - vr + 2^{-1}\varphi(\zeta)) + \varphi(\tau')) \Big)$$

Premier cas : $\sigma = T = \begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix}$. Nous tirons de (9.5) et (9.6)

$$\beta(i) = \xi^{i^2} \zeta^{-i} \alpha(i - r) \quad \text{et}$$

$$\gamma(i) = \xi^{2ri} \zeta^{-i} \xi^{(i-r)^2} \alpha(i-r).$$

Nous voyons que $\beta(i)$ et $\gamma(i)$ différent d'un multiple constant inversible et (9.4) est démontré dans ce cas .

Deuxième cas : $\sigma = S = \begin{pmatrix} 0 & \xi \\ \varphi & 0 \end{pmatrix}$.

Nous tirons de (9.5) et (9.6)

$$\beta(i) = \sum_{\tau \in \mu_n} \xi^{2i\varphi(\tau)} \zeta^{-\varphi(\tau)} \alpha(\varphi(\tau)-r)$$

et

$$\gamma(i) = \xi^{2ir} \sum_{\tau' \in \mu_n} \xi^{2(i+2^{-1}\varphi(\zeta))\varphi(\tau')} \alpha(\varphi(\tau')).$$

En utilisant le fait que $\varphi(\xi) = -1$ et en multipliant ces relations par un élément de k inversible, indépendant de i nous obtenons

$$\beta(i) = \sum_{t \in \mathbb{Z}/n\mathbb{Z}} \xi^{2it} \zeta^{-t} \alpha(t-r)$$

et

$$\gamma(i) = \xi^{2ir} \sum_{t \in \mathbb{Z}/n\mathbb{Z}} \xi^{2i(t-r)} \zeta^{r-t} \alpha(t-r) ,$$

ce qui montre que $\beta(i)$ et $\gamma(i)$ diffèrent d'un multiple constant inversible et (9.4) est démontré dans ce cas. En vertu du corollaire 6.3 ceci suffit pour prouver le théorème.

Théorème 9.3 : Soit k une $\mathbb{Z}[1/n][\mu_n]$-algèbre. Les seuls points de $\mathcal{V}(k)$ dont le stabilisateur sous l'action de $(\mathcal{V}_n)(k)$ n'est pas trivial sont les points extraordinaires de $\mathcal{V}(k)$. Si a est une pointe de $\mathcal{A}(k)$ et si M est un point extraordinaire de $\mathcal{V}_a(k)$, le stabilisateur de M est le groupe $C(a)(k)$.

Preuve : Soit $P \in \mathcal{V}(k)$ et supposons que

$$(rg' + g_\zeta)_{p(P)} + P = P$$

avec $\zeta \in \mu_n(k)$. Cette égalité signifie, si $P = (p(P), (\alpha(0) : \alpha(1) : \quad))$, qu'il existe $\lambda \in k$, inversible, tel que

$$\zeta^{-i} \alpha(i-r) = \lambda \, \alpha(i)$$

pour tout $i \in \mathbb{Z}/n\mathbb{Z}$.

Nous en déduisons par récurrence sur l'entier t ,

$$\alpha(i-tr) = (\zeta^i\lambda)^t\, \zeta^{-r\frac{t(t-1)}{2}}\, \alpha(i) \tag{9.7}$$

pour tous i et t dans $\mathbb{Z}/n\,\mathbb{Z}$.
Si r = 0 cette égalité se réduit à

$$\alpha(i) = (\zeta^i\lambda)^t\, \alpha(i) ,$$

et si P est un point ordinaire de $\mathcal{V}(k)$, il existe d'après le théorème (8.15) s et s' dans $\mathbb{Z}/n\mathbb{Z}$, distincts, tels que $\alpha(s)$ et $\alpha(s')$ soient inversibles. Ce qui nous donne

$$\zeta^s\lambda = \zeta^{s'}\lambda = 1 ,$$

d'où $\zeta = \lambda = 1$ et $(r,\zeta) = (0,1)$.

Si $r \neq 0$, l'égalité (9.7) donne

$$\alpha(-tr) = \lambda^t\, \zeta^{-r\frac{t(t-1)}{2}}\, \alpha(0). \tag{9.8}$$

Nous en déduisons, puisqu'il existe $i \in \mathbb{Z}/n\mathbb{Z}$ tel que $\alpha(i)$ soit inversible, que $\alpha(j)$ est inversible quelque soit j. Soit τ un générateur de $\mu_n(k)$. Définissons u et j dans $\mathbb{Z}/n\mathbb{Z}$ par les équations

$$\zeta = \tau^{-2ru}$$

$$\lambda^2\zeta^r = \tau^{4rj} .$$

Nous tirons de (9.8)

$$\alpha(i) = \tau^{ui2-2ij}\alpha(0) \tag{9.9}$$

pour tout $i \in \mathbb{Z}/n\mathbb{Z}$. En nous reportant au tableau (8.9) nous voyons que si $\varphi \in \mathrm{Hom}(\mu_n, \mathbb{Z}/n\mathbb{Z})(k)$ est tel que $\varphi(\tau) = 1$ et si $v \in \mathbb{Z}/n\mathbb{Z}$ et $\xi \in \mu_n(k)$ sont tels que $\sigma = \begin{pmatrix} u & \xi \\ \varphi & v \end{pmatrix}$ soit dans $\mathrm{Sp}(\mathbb{Z}/n\mathbb{Z} \times \mu_n)(k)$, le point P est le transformé par σ d'un point singulier de $\mathcal{V}_{\begin{bmatrix}1\\0\end{bmatrix}}(k)$ et que P est un point extraordinaire de $\mathcal{V}(k)$.

Nous venons donc de montrer que les points ordinaires de $\mathcal{V}(k)$ ont un stabilisateur trivial sous l'action de $\mathcal{V}_n(k)$.

Si P est un point extraordinaire de $\mathcal{V}(k)$, grâce au théorème 9.2, nous pouvons supposer que $p(P) = \begin{bmatrix}1\\0\end{bmatrix}$ et les relations (9.2) et le tableau (8.9) montrent que

$$P = (rg' + g_\xi)_{\begin{bmatrix}1\\0\end{bmatrix}} + P$$

si et seulement si $r = 0$ ce qui démontre le théorème.

Nous utilisons les notations du chapitre 8(théorème 8.13).

Proposition 9.4 : Soient k une $\mathbb{Z}[1/n][\mu_n]$-algèbre, a une pointe de $\mathcal{C}(k)$ et ν un numérotage de $\mathcal{V}_a(k)$. L'élément $u \in (\mathcal{V}_n)_a(k)$ opère sur $\mathcal{V}_a(k)$ en envoyant

i) la composante $\mathcal{C}$ sur la composante $\mathcal{C}'$ telle que

$$\nu(\mathcal{C}') = \nu(\mathcal{C}) + \bar{\nu}(u) \tag{9.10}$$

ii) le point singulier M sur le point singulier M' tel que

$$\nu(M') = \nu(M) + \bar{\nu}(u) \ . \tag{9.11}$$

En particulier $(\mathcal{V}_n)_a(k)$ opère transitivement sur les points singuliers de $\mathcal{V}_a(k)$.

Preuve : Grâce au théorème 9.2, il suffit de vérifier cette proposition lorsque $a = \begin{bmatrix}1\\0\end{bmatrix}$. Dans ce cas nous pouvons choisir ν tel que $\nu(\Delta_i) = i$ et alors $\nu(rg' + g_\zeta)_{\begin{bmatrix}1\\0\end{bmatrix}} = r$.

Si $P = (\begin{bmatrix}1\\0\end{bmatrix}, (\alpha(0) : \alpha(1) : \quad))$ est sur $\Delta_i(k)$ nous avons $\alpha(j) = 0$ pour $j \neq i \pm 1/2$.

Posons $$(rg' + g_\zeta)_{\begin{bmatrix}1\\0\end{bmatrix}} + P = \left(\begin{bmatrix}1\\0\end{bmatrix}, (\alpha'(0) : \alpha'(1) : \quad) \right) .$$

alors les formules (9.2) montrent que $\alpha'(j) = 0$ pour $j \neq r\ r+i \pm 1/2$ ce qui signifie que $(rg' = g_\zeta)_{\begin{bmatrix}1\\0\end{bmatrix}} + P \in \Delta_{i+r}(k)$. Il suffit de reprendre

la définition de $\bar{\nu}$ pour obtenir (9.10).
Soit M un point singulier de $\mathcal{V}_a(k)$ tel que $M = \mathcal{C} \cap \mathcal{C}'$.
Alors $M+u \in (\mathcal{C}+u) \cap (\mathcal{C}'+u)$, c'est un point singulier, et (9.11) résulte de (9.10). Enfin, la relation (9.11) et le fait que $\bar{\nu}$ est surjective montrent que $(\mathcal{V}_n)_a(k)$ opère transitivement sur l'ensemble des n points singuliers de $\mathcal{V}_a(k)$.

Corollaire 9.5 : Soit $a = \begin{bmatrix} u \\ \varphi \end{bmatrix}$ une pointe de $\mathcal{A}(k)$ et soit M un point singulier de $\mathcal{V}_a(k)$.

i) si $\varphi = 0$, $M + (g_\zeta)_a = M$ pour tout $\zeta \in \mu_n(k)$

ii) si $\varphi \neq 0$, $M + (g_\zeta)_a$ parcourt l'ensemble des points singuliers de $\mathcal{V}_a(k)$ quand ζ parcourt $\mu_n(k)$

Preuve : Il suffit d'appliquer (9.11) en remarquant que $\bar{\nu}((g_\zeta)_a) = 0$ si $\varphi = 0$ et $\bar{\nu}((g_\zeta)_a)$ parcourt $\mathbb{Z}/n\mathbb{Z}$ quand ζ parcourt $\mu_n(k)$ si $\varphi \neq 0$.

Définition 9.6 : Soit a une pointe de $\mathcal{A}(k)$.
Nous notons G(a)(k) le stabilisateur de a dans $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)(k)$ et G'(a)(k) le sous-groupe de G(a)(k) qui laisse stable les composantes de $\mathcal{V}_a(k)$.

Si k est à spectre connexe nous savons que G'(a)(k) est cyclique d'ordre n, d'indice 2 dans G(a)(k). De plus, $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in G(a)(k) - G'(a)(k)$ (cela résulte des propositions 7.11 et 8.8).

Proposition 9.7 : A chaque composante $\mathcal{C}$ de $\mathcal{V}_a(k)$ est associé un homomorphisme $\lambda_{\mathcal{C}}$ de G'(a)(k) dans C(a)(k) tel que $\sigma \in G'(a)(k)$ opère sur $\mathcal{C}$ par

$$P \xrightarrow{\sigma} (P + \lambda_{\mathcal{C}}(\sigma))$$

De plus, si ν désigne un numérotage de $\mathcal{V}_a(k)$ et $\lambda_i = \lambda_{\mathcal{C}_i}$ l'homomorphisme associé à la composante $\mathcal{C}_i$ telle que $\nu(\mathcal{C}_i) = i$ nous avons

$$\lambda_i = (\lambda_1)^i$$

et λ_1 est un isomorphisme.

Preuve : Grâce à la proposition 7.7 il suffit de vérifier le cas $a = \begin{bmatrix}1\\0\end{bmatrix}$ Le choix de ν n'ayant pas d'importance nous posons $\nu(\Delta_i) = i$. Soit $P = (\begin{bmatrix}1\\0\end{bmatrix}, (\alpha(0):\ \alpha(1):\ \ ))$ dans $\Delta_i(k)$ et soit $\sigma = \begin{pmatrix}1 & \zeta\\ 0 & 1\end{pmatrix} \in G'(a)(k)$.

Nous avons

$$\sigma P = (\begin{bmatrix}1\\0\end{bmatrix}, (\alpha'(0):\ \alpha'(1):\ \ ))$$

avec $\alpha'(r) = \zeta^{r^2}\alpha(r)$. Par conséquent $\alpha'(r) = 0$ si $r \neq i \pm 1/2$ et

$$\alpha'(i - 1/2) = \zeta^{(i-1/2)^2}\alpha(i - 1/2)$$
$$\alpha'(i + 1/2) = \zeta^{(i+1/2)^2}\alpha(i + 1/2).$$

A un facteur près, inversible et indépendant de r, nous avons

$$\alpha'(r) = \zeta^{2ir}\alpha(r) \quad \text{et par conséquent}$$
$$\sigma P = (g_{\zeta^{-2i}})\begin{bmatrix}1\\0\end{bmatrix} + P$$

L'application $\begin{pmatrix}1 & \zeta\\ 0 & 1\end{pmatrix} \longmapsto (g_{\zeta^{-2i}})\begin{bmatrix}1\\0\end{bmatrix}$ est l'homomorphisme λ_i. La proposition ne fait que traduire les propriétés immédiates de l'application $i \longmapsto \lambda_i$.

9.3 Quotient de $\mathcal{W}$ par μ_n.

Rappelons que les schémas $\mathcal{B}$ et $\mathcal{W} = \mathcal{V}_{\mathcal{B}}$ ont été définis page 8.10

Nous désignons par k une $\mathbb{Z}[1/n]$-algèbre et par $\mathcal{J}$ l'idéal de $k[X_0,\ldots,X_{n-1}]$ engendré par les polynômes (7.1).

Soit L la sous-algèbre de $k[X_0,\ldots,X_{n-1}]/\mathcal{J}$ engendrée par l'image des monômes de la forme

$$m = X(0)^u\, X(-1)^v\, X(1)^w\, X(\alpha_1)\ldots X(\alpha_r) \tag{9.12}$$

avec $r \geq 0$, $u \geq 0$, $v \geq 0$, $w \geq 0$, $\alpha_i \neq 0,1,-1$ et

$$u + v + w + r \equiv 0 \pmod 3$$
$$u + v + w + \sum_{i=1}^{r} \alpha_i \equiv 0 \pmod n$$

En outre nous posons $r(m) = r$.

Proposition 9.8 : L'algèbre L est engendrée par l'image des monômes

$$X = X(0)\,X(-1)\,X(1) \qquad Y = X(-1)^2\,X(2) \qquad Z = X(0)^3 \tag{9.13}$$

Preuve : Soit M la sous-algèbre de $k[X_0,\ldots X_{n-1}]/\mathcal{J}$ engendrée par l'image de X,Y et Z. En comparant (9.13) à (9.12) nous remarquons que les images de X,Y et Z sont dans L. Par conséquent, $M \subset L$ et il nous faut démontrer que tout élément de L est dans M.

Soient α et β dans $\mathbb{Z}/n\mathbb{Z}$. Dans $k[X_0,\ldots,X_{n-1}]/\mathcal{J}$ nous avons les relations

$$\left\{\begin{array}{l} X(\alpha)X(\beta) = \dfrac{a(\alpha)a(\beta)}{a(-1)a(\alpha+\beta+1)}\,X(-1)X(\alpha+\beta+1) \\ \qquad\qquad - \dfrac{a(\alpha-1)a(\beta+1)}{a(-1)a(\alpha+\beta+1)}\,X(0)X(\alpha+\beta) \\ \text{si} \quad \alpha+\beta+1 \neq 0 \end{array}\right. \tag{9.14}$$

$$\left\{\begin{array}{l} X(\alpha)X(\beta) = \dfrac{a(\alpha)a(\beta)}{a(1)a(\alpha+\beta-1)}\,X(1)X(\alpha+\beta-1) \\ \qquad\qquad - \dfrac{a(\alpha-1)a(\beta-1)}{a(1)a(\alpha+\beta-1)}\,X(0)X(\alpha+\beta) \\ \text{si} \quad \alpha+\beta-1 \neq 0 \end{array}\right. \tag{9.15}$$

Il en résulte que tout monôme m de $k[X_0,\ldots,X_{n-1}]$ donné par (9.12), tel que $r(m) \geq 2$ est équivalent modulo $\mathcal{J}$ à une combinaison linéaire d'autres monômes m' de L tels que $r(m') < r(m)$. Par récurrence sur r(m) nous voyons que L est engendrée par les images des monômes m tels que $r(m) \leq 1$ c'est-à-dire par les images des monômes de la forme $m = X(0)^u X(-1)^v X(1)^w X(\alpha)$.

Définition 9.9 : Soit $m = X(\alpha_1)\ldots X(\alpha_r)$ dans $k[X_0,\ldots,X_{n-1}]$. Nous posons

$$m' = X(-\alpha_1)\ldots X(-\alpha_r) \tag{9.16}$$

et nous notons opp l'automorphisme $m \overset{\text{opp}}{\longmapsto} m'$.

L'idéal $\mathcal{J}$ de $k[X_0,\ldots,X_{n-1}]$ est stable par l'action de opp, qui s'étend donc en un automorphisme de $k[X_0,\ldots,X_{n-1}]/\mathcal{J}$. De plus, il est immédiat que L est stable par l'action de opp.

Lemme 9.10 : L'algèbre M est stable par l'automorphisme opp.

Preuve : Nous avons $X' = X$, $Z' = Z$ et $Y' = X(1)^2X(-2)$. Pour démontrer que l'image de Y' est dans M nous pouvons recopier le début de la démonstration du lemme 5.18 puisqu'elle n'utilise rien d'autre que les relations $\mathcal{S}_I = 0$.

Ainsi nous obtenons dans $k[X_0,\ldots,X_{n-1}]/\mathcal{J}$ la relation

$$Y' = -Y + \frac{a(2)^5 + a(4)a(1)^4}{a(1)^3a(2)a(3)}\,X - \frac{a(2)^2}{a(1)^2}\,Z \tag{9.17}$$

et le lemme est démontré.

Définition 9.11 : Soit t un entier ≥ 0. Nous notons $\varepsilon(t)$ l'unique entier défini par les conditions

$$0 \leq \varepsilon(t) < 3 \tag{9.18}$$

$$\varepsilon(t) + t + 1 \equiv 0 \pmod 3,$$

et nous posons

$$\varphi(t) = X(0)^{\varepsilon(t)}X(-1)^tX(t). \tag{9.19}$$

Lemme 9.12 : Quel que soit $t \geq 0$ les images des monômes $\varphi(t)$ et $\varphi(t)\circ$ opp sont dans M.

Preuve : D'après le lemme 9.10 il suffit de démontrer que les images des monômes $\varphi(t)$ sont dans M. Nous allons procéder par récurrence sur t. Nous constatons que

$$\varphi(0) = Z \quad , \quad \varphi(1) = X \quad , \quad \varphi(2) = Y \ . \tag{9.20}$$

Pour simplifier l'écriture nous allons employer la même notation pour désigner un monôme et son image dans $k[X_o,\ldots,X_{n-1}]/J$.
Soit $t > 2$ et faisons l'hypothèse que quel que soit l'entier r avec $0 \leq r < t$ nous avons $\varphi(r) \in M$. Nous allons montrer qu'alors $\varphi(t) \in M$.

Supposons d'abord $t \equiv 2 \pmod n$ c'est-à-dire $t = 2 + kn$ avec $k \geq 1$. Nous avons

$$\varphi(t) = X(0)^{\varepsilon(2+kn)}\, X(-1)^{kn}\, \varphi(2)$$

et comme $\varepsilon(kn + 2) = 2(kn - 1)$ nous obtenons

$$\varphi(t) = \varphi(2)\, \varphi(kn) \tag{9.21}$$

et par conséquent $\varphi(t) \in M$.

Nous pouvons donc maintenant supposer $t \not\equiv 2 \pmod n$.

Nous avons

$$X(-1)X(t) = \frac{a(2)a(t-1)}{a(1)a(t-2)}\, X(0)\, X(t-1) - \frac{a(t)}{a(t-2)}\, X(1)\, X(t-2)$$

et par conséquent,

$$\varphi(t) = X(0)^{\varepsilon(t)}X(-1)^{t}X(t) = \frac{a(2)a(t-1)}{a(1)a(t-1)}\, X(0)^{\varepsilon(t)+1}X(-1)^{t-1}X(t-1)$$

$$- \frac{a(t)}{a(t-2)}\, X(0)^{\varepsilon(t)}X(1)X(-1)^{t-1}X(t-2)$$

Comme $\varepsilon(t)+1 \equiv \varepsilon(t-1) \pmod 3$ et comme $\varepsilon(t)+1 \geq \varepsilon(t-1)$, il existe un entier $s \in \{0,1\}$ tel que $\varepsilon(t) + 1 = \varepsilon(t-1) + 3s$.
Il en résulte que

$$\varphi(t) = \frac{a(2)a(t-1)}{a(1)a(t-2)} Z^s\varphi(t-1) - \frac{a(t)}{a(t-2)} X(0)^{\varepsilon(t)}X(1)X(-1)^{t-1}X(t-2)$$

Nous sommes donc ramenés à démontrer que

$$\psi = X(0)^{\varepsilon(t)}X(-1)^{t-1}X(1)X(t-2)$$

est dans M.
Deux cas sont à envisager.

Premier cas : $t \equiv 0$ ou $1 \pmod 3$.
Alors $\varepsilon(t) > 0$, $\varepsilon(t)-1 = \varepsilon(t-2)$ et

$$\psi = (X(0)X(-1)X(1))\cdot(X(0)^{\varepsilon(t)-1}X(-1)^{t-2}X(t-2))$$

soit encore

$$\psi = \varphi(1)\varphi(t-2) \quad \text{et} \quad \varphi(t) \in M.$$

Deuxième cas : $t \equiv 2 \pmod 3$.

Nous avons $\varepsilon(t) = 0$ et

$$\psi = X(1)X(-1)^{t-1}X(t-2).$$

Supposons d'abord $t \not\equiv 3 \pmod n$. Alors

$$X(1)X(t-2) = \frac{a(1)a(t-4)}{a(2)a(t-3)} X(0)X(t-1) + \frac{a(1)a(t-2)}{a(2)a(t-3)} X(2)X(t-3) ,$$

d'où

$$\psi = \frac{a(1)a(t-4)}{a(2)a(t-3)} X(0)X(-1)^{t-1}X(t-1) + \frac{a(1)a(t-2)}{a(2)a(t-3)} X(-1)^{t-1}X(2)X(t-3)$$

et comme $\varepsilon(t-1) = 1$, $\varepsilon(t-3) = 0$ et $t > 3$(puisque $t > 2$ et $t \equiv 2 \bmod 3$) nous obtenons enfin

$$\psi = \frac{a(1)a(t-4)}{a(2)a(t-3)} \varphi(t-1) + \frac{a(1)a(t-2)}{a(2)a(t-3)} \varphi(2)\ \varphi(t-3)$$

et $\varphi(t) \in M$.

Reste un dernier cas à examiner,c'est celui où
$t \equiv 3(\bmod n)$, $t \equiv 2(\bmod 3)$, $t > 2$.
Nous avons

$$\psi = X(1)^2 X(-1)^{t-1}$$

et avec nos hypothèses $t \geq 3$ + $n \geq 8$.(puisque $n \geq 5$).
Comme

$$X(-1)^2 = \frac{a(2)^2}{a(1)a(3)} X(0)X(-2) - \frac{a(1)}{a(3)} X(1)X(-3)$$

nous en déduisons

$$\psi = \frac{a(2)^2}{a(1)a(3)} X(0)X(1)^2X(-2)X(-1)^{t-3} - \frac{a(1)}{a(3)} X(1)^3X(-3)X(-1)^{t-3} .$$

Nous remarquons que $X(0)X(-1)^{t-3} = \varphi(t-4)$ puisque $\varepsilon(t-4) = 1$ et $X(t-4) = X(-1)$, que $X(1)^2X(-2) = Y'$ et que $X(-3)X(-1)^{t-6} = \varphi(t-6)$ puisque $X(t-3) = X(-3)$ et $\varepsilon(t-6) = \varepsilon(t) = 0$.

Nous en déduisons que

$$\psi = \frac{a(2)^2}{a(1)a(3)} Y'\varphi(t-4) - \frac{a(1)}{a(3)} (X(1)X(-1))^3\varphi(t-6).$$

Il suffit donc de voir que $(X(1)X(-1))^3 \in M$.
Nous avons

$$X(1)X(-1) = \frac{a(1)a(3)}{a(2)^2} X(0)^2 + \frac{a(1)^2}{a(2)^2} X(2)X(-2)$$

et par conséquent

$$(X(1)X(-1))^3 = \frac{a(1)a(3)}{a(2)^2} X(0)^2X(1)^2X(-1)^2 + \frac{a(1)^2}{a(2)^2} X(1)^2X(2)X(-2)X(-1)^2$$

soit encore

$$(X(1)X(-1))^3 = \frac{a(1)a(3)}{a(2)^2} X^2 + \frac{a(1)^2}{a(2)^2} YY'$$

et le lemme 9.12 est démontré.
Fin de la démonstration de la proposition 9.8 .

Nous devons montrer que les images des monômes

$$m = X(0)^uX(-1)^vX(1)^w X(\alpha)$$

avec $u \geq 0$, $v \geq 0$ et $w \geq 0$, qui sont dans L sont aussi dans M.
Compte-tenu de ce que les images de $X(0)^3$ et $X(0)X(-1)X(1)$ sont dans M nous pouvons supposer

$$0 \leq u < 3 \quad \text{et}$$
$$\inf(u,v,w,) = 0 \ .$$

Si l'un des deux entiers v et w est nul, le monôme m est de la forme $\varphi(t)$ ou $\varphi'(t)$, et est dans M. Nous pouvons donc supposer u = 0.
Comme $X(1)^3X(-1)^3$ est dans M nous pouvons supposer en outre que

$$0 \leq \inf(v,w) < 3 \ .$$

Si $m = X(1)X(-1)^v$ nous avons $m = \varphi(v)$ et par conséquent $m \in M$.

Les seuls cas restant à examiner sont donc

$$m_1 = X(1)^2X(-1)^v$$
$$m_2 = X(1)X(-1)^vX(v-1)$$
$$m_3 = X(1)^2X(-1)^vX(v-2) \ ,$$

leur appartenance à M entrainant celle de m'_1 , m'_2 et m'_3 .

Cas $m = m_1$.
Nous avons

$$X(1)^2 = \frac{a(2)}{a(1)a(3)} X(0)X(2) - \frac{a(1)}{a(3)} X(-1)X(3)$$

d'où

$$m_1 = \frac{a(2)}{a(1)a(3)} X(0)X(-1)^v X(2) - \frac{a(1)}{a(3)} X(-1)^{v+1}X(3)$$

mais $v \equiv 1 \pmod 3$ et $v \equiv 2 \pmod n$
par conséquent

$$m_1 = \frac{a(2)}{a(1)a(3)} \varphi(v) - \frac{a(1)}{a(3)} \varphi(v+1)$$

et $m_1 \in M$.

Cas $m = m_2$. Il y a deux possibilités à envisager.
Première hypothèse $v \equiv -1 \pmod n$. Alors

$$m_2 = X(1)X(-1)^v X(-2) \qquad \text{et}$$

$$X(1)X(-2) = \frac{a(1)a(4)}{a(2)a(3)} X(0)X(-1) + \frac{a(1)}{a(3)} X(2)X(-3) .$$

Par conséquent

$$m_2 = \frac{a(1)a(4)}{a(2)a(3)} X(0)X(-1)^{v+1} + \frac{a(1)}{a(3)} X(2)X(-1)^v X(-3).$$

Mais $v > 2$ puisque $v > 0$ et $v \equiv -1(n)$.

De plus, $v \equiv 1(3)$. Il en résulte que

$$m_2 = \frac{a(1)a(4)}{a(2)a(3)} \varphi(v) + \frac{a(1)}{a(3)} \varphi(2)\varphi(v-2) ,$$

ce qui montre que $m_2 \in M$.

Deuxième hypothèse $v \not\equiv -1(n)$. Alors

$$X(1)X(v-1) = \frac{a(2)a(v)}{a(1)a(v+1)} X(0)X(v) - \frac{a(v-1)}{a(v+1)} X(-1)X(v+1)$$

et

$$m_2 = \frac{a(2)a(v)}{a(1)a(v+1)} X(0)X(v)X(-1)^v - \frac{a(v-1)}{a(v+1)} X(v+1)X(-1)^{v+1} .$$

Comme $v \equiv 1 \pmod 3$, nous en tirons

$$m_2 = \frac{a(2)a(v)}{a(1)a(v+1)} \varphi(v) - \frac{a(v-1)}{a(v+1)} \varphi(v+1)$$

et $m_2 \in M$.

Cas $m = m_3$. Deux possibilités sont à envisager.
Nous avons $m = X(1)^2X(-1)^vX(v-2)$.

Première hypothèse $v \equiv 0 \pmod n$. Alors

$$m_3 = X(1)^2X(-1)^vX(-2) .$$

Mais $\varepsilon(v-1) = 0$ puisque $v \equiv 0 \pmod 3$, donc

$$m_3 = \varphi'(2)\varphi(v-1) \quad \text{et } m_3 \in M.$$

Deuxième hypothèse $v \not\equiv 0 \pmod n$. Alors

$$X(1)X(v-2) = \frac{a(2)a(v-1)}{a(1)a(v)} X(0)X(v-1) - \frac{a(v-2)}{a(v)} X(-1)X(v)$$

et

$$m_3 = \frac{a(2)a(v-1)}{a(1)a(v)} X(0)X(1)X(-1)^vX(v-1) - \frac{a(v-2)}{a(v)} X(1)X(-1)^{v+1}X(v)$$

ou encore

$$m_3 = \frac{a(2)a(v-1)}{a(1)a(v)} \varphi(1)\varphi(v-1) - \frac{a(v-2)}{a(v)} X(1)X(-1)^{v+1}X(v).$$

Mais nous venons de voir que les monômes de la forme $m_2 = X(1)X(-1)^{v+1}X(v)$ sont dans M donc $m_3 \in M$. Ceci achève la démonstration de la proposition 9.8

Théorème 9.13 : X,Y et Z sont liées par la relation

$$(9.22)\quad Y^2Z - \frac{a(2)^5+a(4)a(1)^4}{a(1)^3a(2)a(3)}\,XYZ + \frac{a(2)^2}{a(1)^2}\,YZ^2 = -\frac{a(2)^2}{a(1)^2}\,X^3 + \frac{a(3)}{a(1)}\,X^2Z$$

Preuve : La relation (9.17) nous donne

$$(9.23)\quad -Y'YZ = Y^2Z - \frac{a(2)^5+a(4)a(1)^4}{a(1)^3a(2)a(3)}\,XYZ + \frac{a(2)^2}{a(1)^2}\,YZ^2 .$$

Or

$$Y'YZ = X(1)^2X(-1)^2X(0)^3X(2)X(-2)$$

et nous avons

$$X(2)X(-2) = \frac{a(2)^2}{a(1)^2}\,X(1)X(-1) - \frac{a(3)}{a(1)}\,X(0)^2$$

donc

$$(9.24)\quad -Y'YZ = -\frac{a(2)^2}{a(1)^2}\,X^3 + \frac{a(3)}{a(1)}\,X^2Z$$

ce qui, combiné avec (9.23), nous donne (9.22).

9.3. La courbe $\mathfrak{Y}$

Définition 9.14 : Nous notons $\mathfrak{Y}$ la courbe définie au-dessus de $\mathfrak{B}$ par l'équation (9.22). C'est un sous-schéma de $\mathfrak{B} \times \mathbf{P}^2$.
Nous notons O et P les sections de $\mathfrak{Y}$ dont les coordonnées projectives (X:Y:Z) sont données par

$$(9.25)\qquad O = (0:1:0)$$
$$P = (0:0:1)$$

Ces sections sont contenues dans l'ouvert de lissité $\mathfrak{Y}^{reg}$ de $\mathfrak{Y}$. On

munit $\mathfrak{J}^{reg}$ d'une structure de schéma en groupes commutatifs en prenant 0 pour élément neutre et en posant la condition

" A + B + C = 0 si et seulement si A,B et C sont alignés ".

Les fibres géométriques de $\mathfrak{J}^{reg}$ sont soit des courbes lisses de genre 1 (courbes elliptiques) soit de type $\mathbb{G}_m$ ou $\mathbb{G}_a$

Nous avons vu, théorème 9.3 et corollaire 9.5, que μ_n opère librement sur $\mathcal{W}$ La proposition 9.8 et le théorème 9.13 nous permettent de définir un monomorphisme de $\mathcal{W}/\mu_n$ dans $\mathfrak{J}$.
Nous notons θ le morphisme correspondant de $\mathcal{W}$ dans $\mathfrak{J}$. Autrement dit, θ est défini par les relations (9.13).

Posons pour tout entier m

$$\begin{aligned} \alpha_m &= a(m-1)a(m)a(m+1) \\ \beta_m &= a(m-1)^2a(m+2) \\ \gamma_m &= a(m)^3 \end{aligned} \tag{9.26}$$

Proposition 9.15 : Pour tout entier $m \geq 0$ nous avons

$$mP = (\alpha_m : \beta_m : \gamma_m) \ , \tag{9.27}$$

(En particulier nP = 0). De plus

$$\theta(rg'+g_\zeta) = -rP. \tag{9.28}$$

Preuve : Nous remarquons que (9.27) est vraie pour m = 0 et 1.
Calculons les coordonnées projectives du point 2P. La tangente à $\mathfrak{J}$ en P a pour équation Y = 0. Elle recoupe $\mathfrak{J}$ au point -2P qui a pour coordonnées

$$(a(-3)a(-2)a(-1) \ : \ 0 \ : \ a(-2)^3) \ .$$

Au passage nous voyons que (9.27) est vraie pour m = -2. Sur la courbe $\mathfrak{J}$, l'opposé du point de coordonnées $(\alpha:\beta:\gamma)$ a pour coordonnées

$$(9.29)\qquad \left(\alpha : \frac{a(2)^5+a(4)a(1)^4}{a(1)^3\,a(2)a(3)}\,\alpha - \frac{a(2)^2}{a(1)^2}\,\gamma - \beta : \gamma\right).$$

Par conséquent,

$$2P = (a(1)a(2)a(3) : a(1)^2a(4) : a(2)^3)$$

et (9.27) est vraie pour m = 2.

Soit $Q=(\alpha : \beta : \gamma)$ un point de $\mathfrak{I}$ différent de O et P. La droite passant par P et Q a pour équation $\alpha Y - \beta X = 0$. Elle recoupe $\mathfrak{I}$ au point

$$(9.30)\qquad -(P+Q) = (\alpha\beta\gamma : \beta^2\gamma : \alpha^3)$$

Nous déduisons de (9.30), (9.29) et (9.22)

$$(9.31)\qquad P + Q = \left(\alpha\beta\gamma : \frac{a(2)^2}{a(1)^2}\,\beta\gamma^2 - \frac{a(3)}{a(1)}\,\alpha^2\gamma : \alpha^3\right).$$

Nous pouvons maintenant démontrer (9.27) par récurrence sur m.

Soit m un entier tel que $2 \leq m < n$ et supposons (9.27) vraie pour m. Nous avons $mP \neq P$ et $mP \neq O$ car la première coordonnée de mP n'est pas nulle. La relation (9.31) nous donne

$$(m+1)P = \left(\alpha_m\beta_m\gamma_m : \frac{a(2)^2}{a(1)^2}\,\beta_m\,\gamma_m^{\,2} - \frac{a(3)}{a(1)}\,\alpha_m^{\,2}\gamma_m : \alpha_m^{\,3}\right).$$

Nous obtenons immédiatement

$$\alpha_m\beta_m\gamma_m = a(m-1)^3a(m)^3\alpha_{m+1}$$
$$\alpha_m^{\,3} = a(m-1)^3a(m)^3\gamma_{m+1}.$$

D'autre part,

$$\frac{a(2)^2}{a(1)^2}\,\beta_m\gamma_m^{\,2} - \frac{a(3)}{a(1)}\,\alpha_m^{\,2}\gamma_m =$$

$$(9.32)\qquad \frac{a(m-1)^2a(m)^5}{a(1)^2}\left[a(2)^2a(m+2)a(m) - a(1)a(3)a(m+1)^2\right]$$

Mais par un choix convenable du sextuplet I, la relation $\mathcal{R}_I = 0$ nous donne

$$a(2)^2 a(m+2)a(m) - a(1)a(3)a(m+1)^2 = a(1)^2 a(m-1)a(m+3) ,$$

et en reportant cette égalité dans (9.32) nous obtenons

$$\frac{a(2)^2}{a(1)^2} \beta_m \gamma_m^2 - \frac{a(3)}{a(1)} \alpha_m^2 \gamma_m = a(m-1)^3 a(m)^3 \beta_m \quad .$$

Il en résulte, si $m \neq 0$ et 1, ce que nous avons supposé, que

$$(m+1)P = (\alpha_{m+1} : \beta_{m+1} : \gamma_{m+1}) \quad .$$

Nous en déduisons par récurrence sur m que

$$nP = (\alpha_n : \beta_n : \gamma_n) = (\alpha_o : \beta_o : \gamma_o) = 0 \quad .$$

Par conséquent P est un point d'ordre n sur $\mathfrak{J}$, et la relation (9.27) qui a maintenant un sens si l'on prend m dans $\mathbb{Z}/n\mathbb{Z}$ est démontrée.

Enfin, la relation (9.28) résulte de (9.27) et de (9.13).

Corollaire 9.16 : Les fibres géométriques de $\mathfrak{J}$ ne sont jamais de type $\mathbf{G}_a$.

Preuve : Un groupe de type $\mathbf{G}_a$ ne possède pas de point d'ordre n non trivial.

Proposition 9.17 : Les relations suivantes

$$\varphi_o = 1 \quad , \varphi_1 = \frac{X}{Z} \quad , \varphi_2 = \frac{Y}{Z} \tag{9.33}$$

$$\varphi_{2+\ell n} = \varphi_2 (\varphi_{n-1})^{\ell} \tag{9.34}$$

$$a(t-1)\varphi_{t+1} = \frac{a(2)a(t)}{a(1)} \varphi_t - a(t+1) \frac{X}{Z} \varphi_{t-1} \quad , \tag{9.35}$$

permettent d'associer à chaque entier m positif un $\mathcal{B}$-morphisme φ_m de $\mathfrak{J}$ dans $\mathcal{B} \times \mathbf{P}^1$.

Preuve : L'équation 9.22 de la courbe $\mathfrak{Y}$ montre que φ_o, φ_1 et φ_2 sont des $\mathfrak{B}$-morphismes. Les relations de récurrence (9.35) et (9.34) permettent de construire les autres φ_m.

Nous remarquons que les relations (9.33) et (9.35) ne suffisent pas à déterminer les fonctions φ_m quand $m \equiv 2 (\text{mod } n)$; c'est pourquoi nous avons introduit la relation complémentaire (9.34).

Lemme 9.18 : Pour tous entiers t et $\ell \geq 0$ nous avons

$$\varphi_{t+\ell n} = \varphi_t (\varphi_{n-1})^{\ell} \quad . \tag{9.36}$$

Preuve : Nous voyons immédiatement que (9.36) est vraie pour $\ell = 0$.
De plus, il suffit de prouver cette relation pour $0 \leq t < n$; c'est-à-dire que nous devons montrer que pour tout entier positif m nous avons

$$\varphi_m = \varphi_m - \left[\frac{m}{n}\right] n \, (\varphi_{n-1})^{\left[\frac{m}{n}\right]} \quad . \tag{9.37}$$

Nous procédons par récurrence. Soit s supérieur ou égal à n et supposons que (9.37) est vraie pour tout entier m tel que $0 \leq m < s$.
Si $s \equiv 2 \pmod n$ la relation (9.37) résulte immédiatement de (9.34).
Supposons donc $s \not\equiv 2 \pmod n$. Nous avons, d'après (9.34)

$$\varphi_s = \frac{a(2)a(s-1)}{a(1)a(s-2)} \varphi_{s-1} - \frac{a(s)}{a(s-2)} \frac{X}{Z} \varphi_{s-2} \quad . \tag{9.38}$$

Posons $s = \ell n + r$ avec $0 \leq r < n$; autrement dit

$$\ell = \left[\frac{s}{n}\right] \qquad \text{et} \qquad r = s - n\left[\frac{s}{n}\right] \quad .$$

Si $s \equiv \pmod n$, avec l'hypothèse de récurrence, nous avons

$$\varphi_{s-1} = \varphi_{n-1} (\varphi_{n-1})^{\ell-1} = \varphi_{n-1}^{\ell} \quad \text{et}$$

$$\varphi_{s-2} = \varphi_{n-2} (\varphi_{n-1})^{\ell-1} \quad .$$

et en reportant dans (9.38) nous obtenons

$$\varphi_s = (\varphi_{n-1})^{\ell} \quad ,$$

qui n'est autre que (9.37).

Si $s \equiv 1 \pmod n$, nous avons, d'après l'hypothèse de récurrence,

$$\varphi_{s-1} = (\varphi_{n-1})^{\ell} \quad \text{et}$$

$$\varphi_{s-2} = (\varphi_{n-1})^{\ell} .$$

En reportant dans (9.38) nous obtenons

$$\varphi_s = \frac{X}{Z}(\varphi_{n-1})^{\ell} = \varphi_1(\varphi_{n-1})^{\ell}$$

qui n''st autre que (9.37).

Si $s \equiv r \pmod n$ avec $2 < r < n$, nous avons d'après l'hypothèse de récurrence

$$\varphi_{s-1} = \varphi_{r-1}(\varphi_{n-1})^{\ell}$$

$$\varphi_{s-2} = \varphi_{r-2}(\varphi_{n-1})^{\ell} .$$

En reportant dans (9.38) nous obtenons

$$\varphi_s = (\varphi_{n-1})^{\ell}\left[\frac{a(2)a(s-1)}{a(1)a(s-1)}\ \varphi_{r-1} - \frac{a(s)\ X}{a(s-2)Z}\ \varphi_{r-2}\right] .$$

Mais le terme entre crochets n'est autre que φ_r, ce qui prouve (9.37) dans ce cas et achève la démonstration du lemme 9.18 .

Lemme 9.19 : Soient $r \in \mathbb{Z}/n - \{0\}$ et t un entier positif. Alors

$$\varphi_t(rP) = \frac{a(r-1)^t a(r+t)}{a(r)^{t+1}} \tag{9.39}$$

Preuve : Il résulte de (9.33) et de (9.27) que cette relation est vraie pour $t = 0,1,2$. Supposons-la vraie pour $t = 0,1,2,\ldots,m$ avec $2 \leq m \leq n$. La relation (9.35) nous donne

$$\varphi_{m+1}(rP) = \frac{a(2)a(m)a(r-1)^m a(r+m)}{a(1)a(m-1)a(r)^{m+1}} - \frac{a(m+1)a(r-1)^m a(r+1)a(r+m-1)}{a(m-1)a(r)^{m+2}}$$

et comme

$$a(2)a(r)a(m)a(r+m) - a(m+1)a(r+1)a(r+m-1)a(1) = a(1)a(r-1)a(m-1)a(r+m+1)$$

nous obtenons, après simplification par $a(m-1)$,

$$\varphi_{m+1}(rP) = \frac{a(r-1)^{m+1}a(r+m+1)}{a(r)^{m+2}}$$

Nous en déduisons que (9.39) est vraie quel que soit m tel que $0 \leq m \leq n$. En particulier,

$$\varphi_{n-1}(rP) = \frac{a(r-1)^n}{a(r)^n} \quad , \tag{9.40}$$

ce qui, combiné avec (9.36), donne (9.39) pour tout entier $t \geq 0$.

Lemme 9.20 : Pour tout entier $t \geq 0$, nous avons sur $\mathfrak{I}$,

$$\operatorname{div} \varphi_t = t\{P\} + \{-tP\} - (t+1)\{0\} \quad . \tag{9.41}$$

Preuve : Il est clair que (9.41) est vraie pour $t = 0,1,2$. D'autre part, grâce à (9.36), il suffit de prouver (9.41) pour $0 \leq t < n$. Supposons donc (9.41) vraie pour $t = 0,1,2,\ldots,m$ avec $2 \leq m \leq n$. La relation (9.35) nous montre que φ_{m+1} n'a pour pôles, qu'un pôle d'ordre $m+2$ en 0, et possède un zéro d'ordre au moins m en P. De plus, $\varphi_{m+1}(-(m+1)P) = 0$ d'après (9.39). Par conséquent, il existe un point Q de $\mathfrak{I}$ tel que

$$\operatorname{div} \varphi_{m+1} = m\{P\} + \{-(m+1)P\} + \{Q\} - (m+2)\{0\}$$

et le théorème d'Abel montre que $Q = P$, ce qui prouve (9.41) pour $t = m+1$, et par récurrence pour tout m.

Théorème 9.21 : Soit $I = (i_1,j_1,i_2,j_2,i_3,j_3)$ un sextuplet d'entiers tels que

$$i_1+j_1 = i_2+j_2 = i_3+j_3 \quad .$$

Alors les fonctions $\varphi_{i_1},\varphi_{j_1},\varphi_{i_2},\varphi_{j_2},\varphi_{i_3},\varphi_{j_3}$ sont liées par la relation

$$(9.42)\qquad a(i_3-i_2)a(j_3-i_2)\varphi_{i_1}\varphi_{j_1} + a(i_1-i_3)a(j_1-i_3)\varphi_{i_2}\varphi_{j_2} + a(i_2-i_1)a(j_2-i_1)\varphi_{i_3}\varphi_{j_3} = 0$$

Preuve : Posons $r = i_1+j_1$. Alors

$$\operatorname{div}\varphi_{i_1}\varphi_{j_1} = r\{P\} + \{-i_1P\} + \{-j_1P\} - (r+2)\{0\} .$$

Sur $\mathfrak{J}$, le diviseur

$$r\{P\} + 2\{-(r/2)P\} - (r+2)\{0\}$$

est principal, c'est le diviseur d'une fonction que nous notons ψ. Nous avons

$$\operatorname{div}\left(\frac{\varphi_{i_1}\varphi_{j_1}}{\psi}\right) = \{-i_1P\} + \{-j_1P\} - 2\{-(r/2)P\} .$$

Par conséquent, les trois fonctions

$$\frac{\varphi_{i_1}\varphi_{j_1}}{\psi} , \frac{\varphi_{i_2}\varphi_{j_2}}{\psi} , \frac{\varphi_{i_3}\varphi_{j_3}}{\psi}$$ qui n'ont pour pôles qu'un pôle

double au point $-(r/2)P$ sont linéairement dépendantes. Le lemme 9.19 nous permet de trouver les coefficients de dépendance et nous obtenons ainsi la relation (9.42).

Soit H l'ouvert de $\mathfrak{J}$ défini par la condition :

φ_{n-1} inversible.

Il résulte du lemme 9.20 que H est le complémentaire de 0 et P.

Lemme 9.23 : Le morphisme $\theta : \mathcal{W} \to \mathfrak{J}$ induit un épimorphisme de l'ouvert $\omega(0) \cap \omega(-1)$ de $\mathcal{W}$ sur l'ouvert H de $\mathfrak{J}$.

Preuve : Soient k une $\mathbb{Z}[1/n]$-algèbre, $a \in \mathcal{B}(k)$,
$Q = (X(0) : X(1) : \quad : X(n-1)) \in \mathcal{W}_a(k)$. Supposons Q dans $\omega(0)_a(k)$. Alors

$$\varphi_t(\theta(Q)) = \frac{X(-1)^t X(t)}{X(0)^{t+1}} \quad . \tag{9.43}$$

En effet, cette relation est vraie pour t = 0,1,2 et comme les quantités $\varphi_t(\theta(Q))$ et $\frac{X(-1)^t X(t)}{X(0)^{t+1}}$ vérifient les mêmes relations de récurrence en t elles sont égales quel que soit t.

Il en résulte, si $Q \in \omega(0) \cap \omega(1)_a(k)$ que

$$\frac{X(t)}{X(0)} = \left(\frac{X(0)}{X(-1)} \right)^t \varphi_t(\theta(Q))$$

et

$$\left(\frac{X(-1)}{X(0)} \right)^n = \varphi_{n-1}(\theta(Q)) \ .$$

Par conséquent, θ envoie $\omega(0) \cap \omega(-1)_a(k)$ dans H(k).

Réciproquement, considérons le révêtement étale H' de H défini comme le sous-schéma de $H \times \mathbb{P}^1$ d'équations

$$Y(-1)^n = \varphi_{n-1} Y(0)^n \tag{9.44}$$

$$Y(t) = Y(0) \left(\frac{Y(0)}{Y(-1)} \right)^t \varphi_t \qquad \text{pour } 1 \leq t \leq n-2 \tag{9.45}$$

où $(Y(0) : Y(1) : \quad)$ sont les coordonnées homogènes dans $\mathbb{P}^{n-1}$ indexées par $\mathbb{Z}/n\mathbb{Z}$. Le théorème (9.21) nous montre que si $I = (i_1, j_1, i_2, j_2, i_3, j_3)$ est un sextuplet d'éléments de $\mathbb{Z}/n\mathbb{Z}$ tels que

$$i_1 + j_1 = i_2 + j_2 = i_3 + j_3$$

nous avons $\mathcal{G}_I = 0$ (en désignant par $\mathcal{G}_I$ le polynôme (7.1)). Nous voyons donc que θ induit un isomorphisme de $\omega(0) \cap \omega(-1)$ sur H'.

Lemme 9.24 : Soit $Q \in \omega(0) \cap \omega(-1)_a(k)$. Alors, pour tout entier r nous avons

$$\theta((-rg')_a + Q) = rP + \theta(Q) \ . \tag{9.46}$$

Preuve : Il suffit de démontrer (9.46) avec r = 1.
Soient (X(0):X(1):) les coordonnées projectives de Q et (X : Y : Z) celles de θ(Q). La formule (9.31) nous montre que

$$P+\theta(Q) = (XYZ : \frac{a(2)^2}{a(1)^2} YZ^2 - \frac{a(3)}{a(1)} X^2Z : X^3).$$

Or

$$XYZ = X(0)^3X(-1)^3X(0)X(1)X(2)$$

$$X^3 = X(0)^3X(-1)^3 X(1)^3$$

D'autre part,

$$\frac{a(2)^2}{a(1)^2} YZ^2 - \frac{a(3)}{a(1)} X^2Z = \frac{X(0)^5X(-1)^2}{a(1)^2} \left[a(2)^2X(2)X(0) - a(3)a(1)X(1)^2\right]$$

et le terme entre crochets est égal à

$$a(1)^2X(-1)X(3)$$ ce qui prouve,

puisque $X(0)^3X(-1)^3$ est inversible que

$$P+\theta(Q) = (X(0)X(1)X(2) : X(0)^2X(3) : X(1)^3) = \theta(-g'+Q).$$

Nous tirons de ce lemme que θ induit un épimorphisme de $\omega(-r) \cap \omega(-1-r)$ sur rP + H pour tout r et, comme les ouverts $\omega(-r) \cap \omega(-1-r)$ recouvrent $\mathcal{W}$ tandis que les ouverts rP + H recouvrent $\mathfrak{I}$ nous avons démontré

Théorème 9.25 : $\mathcal{W}$ est le revêtement principal de groupe μ_n de $\mathfrak{I}$ donné par (9.44) et (9.45), le groupe μ_n opérant sur $\mathcal{W}$ par

$$Y(i) \longmapsto \zeta^{-i}Y(i).$$

Théorème 9.26 :

i) Le schéma $\mathcal{C}$ est une courbe elliptique généralisée au-dessus de $\mathfrak{A}$, munie de la section 0 comme section neutre (au sens de [De-Ra]).

ii) Les fibres géométriques de $\mathcal{C}$ sont

a) des courbes lisses de genre 1 (courbes elliptiques) au dessus des points de $\mathfrak{A}$ qui ne sont pas des pointes.

b) des n-gones au-dessus des pointes de $\mathfrak{A}$.

iii) $\tilde{\mathcal{V}}$ est l'ouvert de lissité de $\mathcal{V}/\mathcal{A}$

iv) $\mathcal{V}_n$ est le noyau de la multiplication par n sur $\tilde{\mathcal{V}}$ et l'action de $\mathcal{V}_n$ sur $\mathcal{V}$ définie par (9.1) est la translation.

Preuve : Il résulte du théorème 9.25 que $\mathcal{W}$ est une courbe elliptique généralisée au-dessus de $\mathcal{B}$. Soit k un corps algébriquement clos où n est inversible et soit $a \in \mathcal{B}(k)$. Deux cas sont possibles.

i) $\mathcal{J}_a(k)$ est lisse alors d'après le théorème 9.25, $\mathcal{W}_a(k)$ est une courbe lisse de genre 1.

ii) $\mathcal{J}_a(k)$ est une cubique à point double ordinaire. Alors la translation par P sur $\mathcal{J}_a(k)$ n'opère pas librement (elle laisse fixe le point singulier). Il résulte alors de (9.44) que le groupe $\mathcal{V}_n$ n'opère pas librement sur $\mathcal{W}$ et d'après le théorème 9.3 nous en déduisons que $\mathcal{W}_a(k)$ possède des points extraordinaires. Les seules fibres géométriques de $\mathcal{W}$ qui sont singulières sont donc celles qui sont au-dessus des pointes de $\mathcal{B}$.
Il n'y a plus qu'à utiliser l'action de $Sp(\mathbb{Z}/n\,\mathbb{Z} \times \mu_n)$ sur $\mathcal{V}$ et sur $\mathcal{A}$ pour obtenir les affirmations i), ii) et iii) du théorème 9.26.

Le sous-schéma $\mathcal{V}_n$ de $\tilde{\mathcal{V}}$ opère sur $\mathcal{V}$ par (9.1). Or les automorphismes de $\mathcal{V}$ sont de la forme

$$P \to u(P) + Q$$

où u désigne un automorphisme de $\mathcal{V}$ dont la restriction à $\tilde{\mathcal{V}}$ respecte la loi de groupe. Comme $n > 3$ le seul automorphisme du groupe $\tilde{\mathcal{V}}$ qui soit d'ordre n est l'identité. Il en résulte qu'un point g de $\mathcal{V}_n$ opère sur $\mathcal{V}$ par $P \to P+Q(g)$ et comme $O \to g$ nous avons $Q(g) = g$. Nous en déduisons que $\mathcal{V}_n$ est contenu dans le noyau de la multiplication par n sur $\tilde{\mathcal{V}}$ et comme il a même degré il lui est égal, ce qui achève la démonstration de ce corollaire.

CHAPITRE 10

Conclusion.

10.1 La catégorie $\mathcal{C}(n)$.

Définition 10.1 : Nous notons $\mathcal{C}(n)$ la catégorie dont les objets sont les triplets, (S,E,λ) formés

i) d'un schéma S sur $\mathbb{Z}[1/n]$

ii) d'une courbe elliptique généralisée E au-dessus de S dont les fibres singulières sont des n-gônes

iii) d'un isomorphisme λ entre le schéma $S \times \mathbb{Z}/n\mathbb{Z} \times \mu_n$ et le noyau E_n de la multiplication par n sur l'ouvert de lissité $\tilde{E}$ de E/S conservant la forme bilinéaire ε_n définie au paragraphe 7.2.

Nous notons g'_E la section de E_n qui est le générateur canonique du sous-groupe de E_n isomorphe par λ à $S \times \mathbb{Z}/n\mathbb{Z}$ et C_E le sous-groupe de E_n isomorphe par λ à $S \times \mu_n$.

Les morphismes sont les couples de morphismes (φ,f) rendant cartésien le diagramme

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & E' \\ \downarrow & & \downarrow \\ S & \xrightarrow{f} & S' \end{array}$$

tels que

$$\varphi(g'_E) = g'_{E'}$$
$$\varphi(C_E) = C_{E'} \quad .$$

Le corollaire 9.27 montre que le triplet $(\mathcal{A}, \mathcal{V}, s)$ où s désigne l'immersion fermée définie au corollaire 7.3 est un objet de catégorie $\mathcal{E}(n)$. Nous voyons que $g'_{\mathcal{V}}$ n'est autre que la section $a \longmapsto (g')_a$ et que $C_{\mathcal{V}}$ est la réunion des sections $a \longmapsto (g_\zeta)_a$.

10.2 Les courbes avec μ_n bien réparti.

Dans la première partie de cette thèse, nous avons vu que si $(\mathrm{Spec}(k), E, \lambda)$ désigne un objet de $\mathcal{E}(n)$ tel que E soit une courbe elliptique (lisse) définie au-dessus d'un corps k où n est inversible, il existe un morphisme canonique de $(\mathrm{Spec}(k), E, \lambda)$ dans $(\mathcal{A}, \mathcal{V}, s)$.

Rappelons que ce morphisme est obtenu à l'aide des fonctions $(X_0, X_1, \ldots, X_{n-1})$ définies par

$$(10.1) \qquad \begin{cases} \operatorname{div} X_r = {}^{r g'_E}\underline{C}_E - \underline{C}_E \\ X_r(\frac{r}{2} g') = \begin{cases} -1 & \text{si } r \neq 0 \\ 1 & \text{sinon} \end{cases} \end{cases}$$

et des constantes $(a_0, a_1, \ldots, a_{n-1})$ définies par

$$(10.2) \qquad a_r = X_r.T(0)$$

où T désigne une fonction sur E possédant un zéro simple à l'origine 0 de E.

Cette construction d'un morphisme canonique de (S, E, λ) dans $(\mathcal{A}, \mathcal{V}, s)$ s'étend sans difficulté au cas où E est une courbe elliptique généralisée au-dessus d'une base S, telle que pour tout point géométrique $\overline{s}$ de S pour lequel la fibre $E_{\overline{s}}$ soit singulière, le groupe $(C_E)_{\overline{s}}$ ne soit pas contenu dans la composante neutre de $E_{\overline{s}}$ ce que, pour abréger, nous appelons une bonne répartition de μ_n. En effet, dans ce cas nous pouvons toujours trouver des fonctions X_r satisfaisant à (10.1), une fonction T et définir des a_r par (10.2). Nous avons encore un morphisme

de la catégorie $\mathcal{E}(n)$ de (S,E,λ) dans $(\mathcal{A}, \mathcal{V}, s)$ construit à l'aide des X_r et des a_r.

Théorème 10.2 : Soit (S,E,λ) dans $\mathcal{E}(n)$ tel que E ait un μ_n bien réparti; alors il existe un unique morphisme de (S,E,λ) dans $(\mathcal{A}, \mathcal{V}, s)$.

Preuve : Nous venons de voir qu'il existe un morphisme de (S,E,λ) dans $(\mathcal{A}, \mathcal{V}, s)$. Comme E a un μ_n bien réparti, en fait ce morphisme va de (S,E,λ) dans $(\mathcal{B}, \mathcal{W}, s)$ puisque $\mathcal{B}$ est précisément l'ouvert de $\mathcal{A}$ dont les fibres ont un μ_n bien réparti. L'unicité du morphisme vient du fait que sur le schéma $\mathcal{W}$ défini par (7.1), les fonctions X_r/X_o sont précisément celles qui vérifient (10.1) ce qui implique que nécessairement tout morphisme de (S,E,λ) dans $(\mathcal{B}, \mathcal{W}, s)$ se construit à l'aide des fonctions X_r sur E satisfaisant (10.1).

Dans [De-Ra] un objet $(\mathcal{M},\mathcal{E},\rho)$ de $\mathcal{E}(n)$ est construit possédant les propriétés suivantes.

i) $\mathcal{M}$ et $\mathcal{E}$ sont lisses sur $\mathbb{Z}[1/n]$ et $\mathcal{M}$ est une courbe projective
ii) Pour tout objet (S,E,λ) de $\mathcal{E}(n)$ il existe un unique morphisme de $\mathcal{E}(n)$ de (S,E,λ) dans $(\mathcal{M},\mathcal{E},\rho)$.

$\mathcal{M}$ est le "schéma des modules de la catégorie $\mathcal{E}(n)$".

Désignons par $\mathcal{M}'$ l'ouvert de $\mathcal{M}$ et par $\mathcal{E}'$ l'ouvert de $\mathcal{E}$ au-dessus de $\mathcal{M}'$ tels que les fibres de $\mathcal{E}'$ aient un μ_n bien réparti. L'ouvert $\mathcal{M}'$ est le complémentaire d'un ensemble fini de points dans $\mathcal{M}$.

Le théorème 10.2 montre qu'il existe un morphisme unique de $(\mathcal{M}',\mathcal{E}',\rho)$ dans $(\mathcal{B}, \mathcal{W}, s)$ et la propriété d'universalité de $(\mathcal{M},\mathcal{E},\rho)$ montre qu'il existe un morphisme unique de $(\mathcal{B}, \mathcal{W}, s)$ dans $(\mathcal{M}',\mathcal{E}',\rho)$. Nous pouvons reformuler le théorème 10.2 .
Théorème 10.3 : Les objets $(\mathcal{M}',\mathcal{E}',\rho)$ et $(\mathcal{B}, \mathcal{W}, s)$ de $\mathcal{E}(n)$ sont isomorphes.

10.3 Les courbes avec μ_n mal réparti

Nous avons

$$\begin{array}{ccc} \mathcal{E}' & \xrightarrow{\varphi} & \subset \mathcal{V} \\ \downarrow & & \downarrow \\ \mathcal{M}' & \xrightarrow{f} & \subset \mathcal{A} \ . \end{array}$$

Le schéma $\mathcal{M}$ étant une courbe, il est bien connu qu'on peut prolonger f de façon unique en un morphisme de $\mathcal{M}$ dans $\mathcal{A}$. Il faut voir que φ se prolonge en un morphisme de $\mathcal{E}$ dans $\mathbf{P}^{n-1}$ ce qui donnera, puisque est fermé dans $\mathbf{P}^{n-1}$ un prolongement de φ en un morphisme de $\mathcal{E}$ dans Pour cela, compte-tenu du corollaire 2.6 de [De-Ra] page 159 il suffit de voir qu'il existe un morphisme de la "courbe de Tate à n côtés"

$$(S,E,\lambda) = (\text{Spec } \mathbf{Z}[1/n][[q^{1/n}]] \ , \ \mathbf{G}_m q^{1/n}/q^{\mathbf{Z}} \ , \ \lambda)$$

dans $(\mathcal{A}, \mathcal{V}, s)$. Pour simplifier, mais cela ne change rien à la méthode nous pouvons supposer que λ est l'isomorphisme tel que g'_E soit la section "$q^{1/n}$" et C_E soit le sous-groupe "μ_n" de E.(Il faudrait considérer aussi le cas où $g'_E = q_n^{a/n}$ avec $a \neq 0$).
Nous renvoyons à [De-Ra] pages 149 et suivantes pour ce qui concerne la courbe de Tate.

Nous posons $q_n = q^{1/n}$ de sorte que $q_n^n = q$ et nous désignons par z le point courant de $\mathbf{G}_m$.

Définition 10.4 : Soit $r \in \mathbf{Z}/n\mathbf{Z}$. Nous notons $\overline{r}$ l'unique élément de $\mathbf{N}$ défini par

$$(10.3) \qquad \begin{cases} \overline{r} \equiv -r \pmod{n} \\ 0 \leq \overline{r} < n \end{cases}$$

et nous posons

$$(10.4) \qquad \varepsilon(r) = \frac{\overline{r}(n-r)}{2}$$

Nous voyons immédiatement que

$$(10.5)\qquad \begin{cases} \varepsilon(-r) = \varepsilon(r) \\ 0 \leq \varepsilon(r) \leq (n^2-1)/8 \\ \varepsilon(1/2) = \varepsilon(-1/2) = (n^2-1)/8 \\ \varepsilon(r) \neq \varepsilon(r') \quad \text{si} \quad r \neq \pm r' \end{cases}$$

Théorème 10.5 Au-dessus de $S[1/q_n]$ la courbe E est lisse et les fonctions X_r définies par (10.1) admettent le développement

$$(10.6)\qquad X_r(z) = \frac{(-z)^r}{1-z^n} \cdot \frac{1}{q_n^{\varepsilon(r)}} \cdot \frac{\prod_{m>0,\, m\equiv r(n)} (1-q^m z^{-n}) \prod_{m\geq 0,\, m\equiv -r(n)} (1-q^m z^n)}{\prod_{m>0,\, m\equiv 0(n)} (1-q^m z^{-n})(1-q^m z^n)}$$

Preuve : Si r = 0, le membre de droite de (10.6) est égal à 1 ce qui est bien la valeur de $X_o(z)$. Supposons donc $r \neq 0$.

Rappelons [La] que la fonction T définie sur $\mathbb{G}_m$ par le développement

$$(10.7)\qquad T(z,q) = (1-z) \prod_{m>0} (1-q^m z)(1-q^m z^{-1})$$

vérifie les deux relations

$$(10.8)\qquad \begin{aligned} T(qz,q) &= -z^{-1}T(z,q) \\ T(z^{-1},q) &= -z^{-1}T(z,q) \end{aligned}$$

et que toute fonction sur la courbe de Tate s'écrit à une constante près sous la forme

$$z^u \cdot \frac{\prod_{i=1}^{r} T(z/a_i,q)}{\prod_{i=1}^{r} T(z/b_i,q)}$$

avec $\prod_{i=1}^{r} a_i / \prod_{i=1}^{r} b_i = q^{-u}$

La première des deux équations (10.1) montre alors qu'il existe $\alpha(r)$ tel que

$$X_r(z) = \alpha(r)\, z^{-r} \prod_{\zeta \in \mu_n} \frac{T(z/q_n^r \zeta, q)}{T(z/\zeta, q)}$$

$$= \alpha(r)\, z^{-r} . \frac{T(z^n/q^r, q^n)}{T(z^n, q^n)}$$

La deuxième équation (10.1) nous permet de calculer $\alpha(r)$. Considérons deux cas :

Premier cas : r est pair. Posons $s = r/2$.
Nous avons $X_r(q_n^s) = -1$ ce qui donne

$$\alpha(r)\, q_n^{-r^2/2} \frac{T(q^{-s}, q^n)}{T(q^s, q^n)} = -1 .$$

Mais, d'après (10.8)

$$T(q^{-s}, q_n) = -q^{-s} T(q^s, q^n)$$

d'où

$$X_r(z) = q_n^{r(n+r)/2}\, z^{-r} \frac{T(s^n/q^r, q^n)}{T(z^n, q^n)}$$

Il suffit alors d'utiliser (10.7) pour obtenir (10.6).

Deuxième cas : r est impair. Posons $s = \frac{n+r}{2}$
Nous avons

$$X_r(q_n^s) = -1 \quad \text{ce qui donne}$$

$$\alpha(r)\, q_n^{-r(n+r)/2} \frac{T(q^{\frac{n-r}{2}}, q^n)}{T(q^{\frac{n+r}{2}}, q^n)} = -1 .$$

Mais d'après (10.8),

$$T(q^{\frac{n-r}{2}}, q^n) = T(q^{\frac{n+r}{2}}, q^n) \qquad \text{d'où}$$

$$X_r(z) = -q_n^{r(n+r)/2}\, z^{-r}\, \frac{T(z^n/q^r, q^n)}{T(z^n, q^n)}$$

et on obtient (10.6) en utilisant (10.7).

La courbe de Tate E est recouverte par les cartes locales $(U_i)_{i \in \mathbb{Z} + 1/2}$, définies par

$$U_i = S[z_{i-1/2}, t_{i+1/2}]/(z_{i-1/2} \cdot t_{i+1/2} - q_n). \tag{10.9}$$

Ces cartes sont recollées de sorte que l'ouvert

$$\mathcal{C}_i = U_{i-1/2} \cap U_{i+1/2} \subset U_{i+1/2} \text{ soit } U_{i+1/2}[1/z_i] \simeq S[z_i, z_i^{-1}]$$

et $$\mathcal{C}_i \subset U_{i-1/2} \text{ soit } U_{i-1/2}[1/t_i] \simeq S[t_i, t_i^{-1}] ,$$

ces ouverts étant identifiés par la condition

$$z_i \cdot t_i = 1 \tag{10.10}$$

Proposition 10.6 Le morphisme

$$\begin{array}{ccc} \mathcal{E}' = \mathcal{E}[1/q_n] & \longrightarrow & \mathcal{V} \\ \downarrow & & \downarrow \\ S' = S[1/q_n] & \longrightarrow & \mathcal{A} \end{array}$$

se prolonge en un morphisme

$$\begin{array}{ccc} \mathcal{E} & \longrightarrow & \mathcal{V} \\ \downarrow & & \downarrow \\ S & \longrightarrow & \mathcal{A} \end{array}$$

Preuve : Considérons le morphisme p_i défini sur la carte $U_{i+1/2}$ par

$$(z_i,t_{i+1}) \qquad (\psi_o(z_i,t_{i+1}),\dots,\psi_{n-1}(z_i,t_{i+1}))$$

avec

$$(10.11)\quad \psi_r(z_i,t_{i+1}) = z_i^{\frac{s(s+1)}{2}}\, t_{i+1}^{\frac{s(s-1)}{2}}\, (-1)^{\overline{(r-i)}} \prod_{\substack{m>0\\ m\equiv r-i\,(n)}} (1-z_i^{(m-1)n} t_{i+1}^{mn}) \cdot \prod_{\substack{m\geq 0\\ m\equiv i-r\,(n)}} (1-z_i^{(m+1)n} t_{i+1}^{mn})$$

où $s = \overline{(r-i)} - \frac{n-1}{2}$.

Au-dessus de $S[1/q_n]$ nous avons la relation $z_o = z_i q_n^i$ (d'après (10.9) et (10.10)) et compte-tenu de (10.6) nous trouvons

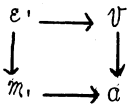
$$\psi_r(z_i,t_{i+1}) = z_i^{\frac{n^2-1}{8}} - \frac{n-1}{2}\, t_{i+1}^{\frac{n^2-1}{8}} \prod_{\substack{m>0\\ m\equiv -i\,(n)}} (1-q^m z_o^{-n}) \prod_{\substack{m\geq 0\\ m\equiv i\,(n)}} (1-q^m z_o^n) X_r(z_o)$$

Ceci nous montre qu'au-dessus de $S[1/q_n]$, le morphisme p_i n'est autre que le morphisme de $E[1/q_n]$ dans $\mathcal{V}$ obtenu à l'aide des fonctions X_r. Sur la fibre spéciale nous avons

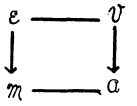
$$\psi_r = \begin{cases} (-1)^{\frac{n-1}{2}} & \text{pour } \overline{(r-i)} = \frac{n-1}{2} \\ z_i (-1)^{\frac{n+1}{2}} & \text{pour } \overline{(r-i)} = \frac{n+1}{2} \\ t_{i+1} (-1)^{\frac{n-3}{2}} & \text{pour } \overline{(r-i)} = \frac{n-3}{2} \\ 0 & \text{dans les autres cas.} \end{cases}$$

donc p_i définit bien un plongement de $U_{i+1/2}$ dans $\mathbb{P}^n$ (puisqu'on peut développer en série z_i et t_{i+1} à l'aide des $\psi_r(z_i,t_{i+1})$) et nous avons vu au passage que p_i et p_j, pour $i \neq j$, coincident au-dessus de l'ouvert $U_{i+1/2} \cap U_{j+1/2}$ qui est contenu dans $E[1/q_n]$. Nous en déduisons la proposition 10.6.

Il résulte de cette proposition que nous pouvons prolonger le morphisme



en un morphisme



Le groupe $Sp(\mathbb{Z}/n\mathbb{Z} \times \mu_n)$ opère sur l'ensemble de la situation et comme nous avons vu au paragraphe 10.2 que $(\mathcal{M}', \mathcal{E}', \rho)$ et $(\mathcal{B}, \mathcal{W}, s)$ sont isomorphes, nous obtenons

Théorème 10.6 : Les objets $(\mathcal{M}, \mathcal{E}, \rho)$ et $(\mathcal{A}, \mathcal{V}, s)$ de la catégorie $\mathcal{E}(n)$ sont isomorphes. En particulier $(\mathcal{A}, \mathcal{V}, s)$ est universel, les schémas $\mathcal{V}$ et $\mathcal{A}$ sont lisses sur $\mathbb{Z}[1/n]$ et $\mathcal{A}$ est une courbe projective.

APPENDICE

$H^2(\mathbb{Z}/n_1\mathbb{Z}\times\ldots\times\mathbb{Z}/n_r\mathbb{Z},k^\times)$ avec action triviale.

Soient $n_1,n_2,\ldots,n_r$ des entiers. Nous considérons un groupe

$$G = G_1 \times G_2 \times\ldots\times G_r$$

tel que G_i soit isomorphe à $\mathbb{Z}/n_i\mathbb{Z}$. Nous supposons que

$$1\leq n_r \mid n_{r-1} \mid \ldots \mid n_1 ,$$

et nous posons $n = n_1$. Si de plus $r = 1$ nous posons $n_2 = 1$. La loi de composition de G est notée additivement.

Soit k un corps, $k^\times$ son groupe multiplicatif, $\overline{k}$ une clôture algébrique de k et

$$\mu_n = \{x \in \overline{k}^\times \mid x^n = 1\} .$$

Considérons une extension centrale

$$0 \longrightarrow k^\times \longrightarrow E \xrightarrow{\pi} G \longrightarrow 0$$

de $k^\times$ par G et notons σ une section ensembliste de π.

Si g et g' sont dans G le commutateur $\sigma(g)\sigma(g')\sigma(g)^{-1}\sigma(g')^{-1}$ de $\sigma(g)$ et $\sigma(g')$ est un élément de $k^\times$ qui ne dépend pas du choix de σ. Nous posons

$$\langle g,g'\rangle = \sigma(g)\sigma(g')\sigma(g)^{-1}\sigma(g')^{-1}$$

Lemme A.1 : L'application $\langle\ ,\ \rangle : G\times G \longrightarrow A$ est une forme bilinéaire alternée à valeurs dans μ_{n_2}.

Preuve : Il est clair que $< , >$ est alternée. Soient g, g_1 et g_2 dans G. Alors

$$\sigma(g)\sigma(g_1)\sigma(g)^{-1} = <g,g_1>\sigma(g_1)$$
$$\sigma(g)\sigma(g_2)\sigma(g)^{-1} = <g,g_2>\sigma(g_2)$$

d'où

$$\sigma(g)\sigma(g_1)\sigma(g_2)\sigma(g)^{-1} = <g,g_1><g,g_2>\sigma(g_1)\sigma(g_2) \ .$$

Mais $\sigma(g_1)\sigma(g_2) = \alpha(g_1,g_2)\sigma(g_1 + g_2)$ avec $\alpha(g_1,g_2)$ dans le centre de E. Par conséquent,

$$\sigma(g)\sigma(g_1 + g_2)\sigma(g)^{-1} = <g,g_1><g,g_2>\sigma(g_1 + g_2) \ .$$

Ceci montre que

$$<g,g_1 + g_2> = <g,g_1><g,g_2>$$

et en utilisant le fait que $< , >$ est alterné nous obtenons

$$<g_1,g><g_2,g> = <g_1 + g_2,g> \ .$$

D'autre part, si nous écrivons

$$g = \sum_{i=1}^{r} g_i \quad \text{et} \quad g' = \sum_{i=1}^{r} g_i'$$

avec g_i et g_i' dans G_i , nous obtenons par linéarité et compte-tenu du fait que $< , >$ est alternée

$$<g,g'> = \prod_{i \neq j} <g_i,g_j'>$$

et comme $<g,g'>^d = 1$ si $dg = 0$ nous voyons que $<g_i,g_j'> \in \mu_{n_2}$ pour tous couples i et j et plus généralement, $<g,g'> \in \mu_{n_2}$.

Nous avons posé $n = n_1$ et par conséquent, $ng = 0$ pour tout $g \in G$. Ceci montre que l'élément $\sigma(g)^n$ de E est en fait dans $k^\times$ pour tout $g \in G$. De plus son image $v(g)$ dans $k^\times/k^{\times n}$ ne dépend pas du choix de σ.

Lemme A.2 : Pour tous g et g' dans G nous avons

$$v(g)v(g') = <g,g'>^{\frac{n(n-1)}{2}} v(g+g') \quad . \tag{A.1}$$

Preuve : Pour tous g et g' dans G nous avons d'une part

$$\sigma(g)\sigma(g') = \alpha(g,g')\sigma(g+g') \tag{A.2}$$

avec $\alpha(g,g')$ dans $k^\times$, d'autre part

$$\sigma(g)\sigma(g') = <g,g'>\sigma(g')\sigma(g) \quad . \tag{A.3}$$

Par récurrence sur l'entier s nous obtenons

$$\sigma(g)^s\sigma(g')^s = <g,g'>^{\frac{s(s-1)}{2}} \alpha(g,g')^s\sigma(g+g')^s$$

ce qui, appliqué à $s = n$, nous donne (A.1).

Remarque : Le nombre $<g,g'>^{\frac{n(n-1)}{2}}$ est égal à +1 ou -1. En particulier il est égal à +1 si n_2 est impair. Nous voyons donc que pour n_2 impair, ou bien $-1 \in k^{\times n}$, ou bien $<g,g'> = 1$ pour tous g et g' dans G, la fonction $v : G \longrightarrow k^\times$ est un homomorphisme. De plus l'application $v^2 : G \longrightarrow k^\times/k^{\times n}$ définie par $g \longrightarrow$ image de $\sigma(g)^{2n}$ dans $k^\times/k^{\times n}$ est toujours un homomorphisme.

Définition A.3 : Nous notons $\tilde{H}^2(G,k^\times)$ le groupe multiplicatif dont les éléments sont les couples $(< , >, v)$ de fonctions

$$< , > : G \times G \longrightarrow k^\times$$
$$v \quad : G \longrightarrow k^\times/k^{\times n}$$

telles que :

i) $< , >$ soit bilinéaire alternée,

ii) v satisfasse à la condition (A.1).

Théorème A.4 : Si $\mu_n \subset k^\times$ l'application λ qui associe à (E,π) le couple $(< , >, v)$ précédemment défini est un isomorphisme entre $H^2(G,k^\times)$ et $\tilde{H}^2(G,k^\times)$.

Preuve : i) Considérons le diagramme commutatif exact suivant

$$\begin{array}{ccccccccc} 0 & \longrightarrow & k^\times & \longrightarrow & E & \xrightarrow{\pi} & G & \longrightarrow & 0 \\ & & \| & & \varphi \downarrow & & \| & & \\ 0 & \longrightarrow & k^\times & \longrightarrow & E & \xrightarrow{\pi} & G & \longrightarrow & 0 \end{array}$$

Alors il est clair, compte-tenu de la définition de $< , >$ et v, que l'on obtient les mêmes fonctions en remplaçant (E,π) par (E',π'). Il en résulte que $(< , >, v)$ ne dépend que de l'image de (E,π) dans $H^2(G,k^\times)$.

ii) Pour voir que λ est un homomorphisme nous pouvons calculer $< , >$ et v à l'aide du 2-cocycle α associé à la section σ par la relation (A.2). Nous trouvons

$$<g,g'> = \frac{\alpha(g,g')}{\alpha(g',g)}$$

et par récurrence

$$\sigma(g)^n = \alpha(g,g)\alpha(g,2g)\ldots\alpha(g,(n-1)g)\sigma(0)$$

Ces formules montrent que λ est un homomorphisme de $Z^2(G,k^\times)$ dans $\tilde{H}^2(G,k^\times)$. Nous savons déjà que λ ne dépend que de la classe de (E,π) dans $H^2(G,k^\times)$ mais nous retrouvons ce fait de la façon suivante. Si α est un 2.cobord, il existe une fonction f de G dans A telle que

$$\alpha(g,g') = \frac{f(g)f(g')}{f(g+g')}$$

et alors

$$\langle g,g'\rangle = 1$$

tandis que

$$\sigma(g)^n = f(g)^n$$

ce qui donne $v(g) = 1$.

iii) λ est injectif.

Si $\langle g,g'\rangle = 1$ pour tous g et g' c'est que l'extension E qui est engendrée par les éléments de $k^\times$ et par les $\sigma(g)$ est commutative. Si de plus $v(g) = 1$ c'est que $\sigma(g)^n \in k^{\times n}$ et quitte à modifier σ nous pouvons supposer que $\sigma(g)^n = 1$ pour tout $g \in G$. Soit g_i un générateur de G_i. L'élément $\sigma(g_i)^{n_i}$ est dans $k^\times$ et comme $(\sigma(g_i)^{n_i})^{n/n_i} = 1$ nous voyons que $\sigma(g_i)^{n_i} \in \mu_{n/n_i} = \mu_n^{n_i}$ puisque $\mu_n \subset k^\times$. Quitte à modifier σ nous pouvons supposer que $\sigma(g_i)^{n_i} = 1$ pour tout générateur g_i de G_i et pour tout i. Comme le groupe G, qui est un groupe de présentation finie, est défini par les relations $g_ig_j = g_jg_i$ et $g_i^{n_i} = 1$ nous voyons que σ est un relèvement de G et que l'extension (E,π) est scindée.

iv) λ est surjectif.

Soient $(<,>,v)$ dans $\widetilde{H}^2(G,k^\times)$.
Choisissons pour chaque i un générateur g_i de G_i et un relèvement a_i de $v(g_i)$ dans $k^\times$.

Soit E l'ensemble des mots de la forme

$$(t,\alpha_1,\alpha_2,\ldots,\alpha_r)$$

où t désigne un élément de $k^\times$ et $\alpha_1,\ldots,\alpha_r$ des entiers tels que

$$0 \leq \alpha_i < n_i \quad .$$

Nous munissons l'ensemble E de la loi de composition

$$(t,\alpha_1,\alpha_2,\ldots,\alpha_r)(t',\alpha_1',\ldots,\alpha_r') = (t'',\alpha_1'',\ldots,\alpha_r'')$$

avec

$$t'' = tt' \prod_{i>j} \langle g_i, g_j \rangle^{\alpha_i \alpha_j} \prod_{i=1}^{r} a_i^{\left[\frac{\alpha_i+\alpha_i'}{n_i}\right]}$$

$$\alpha''_i = \alpha_i + \alpha_i' - \left[\frac{\alpha_i+\alpha_i'}{n_i}\right] n_i \ .$$

On vérifie que l'ensemble E muni de cette loi est un groupe et que l'application $E \xrightarrow{\pi} G$ définie par

$$\pi(t,\alpha_1,\ldots,\alpha_r) = \alpha_1 g_1 + \ldots + \alpha_r g_r$$

est un homomorphisme surjectif qui a pour noyau le sous-groupe de E isomorphe à $k^\times$ formé des mots du type $(t,0,\ldots,0)$.

Il reste à voir, et c'est immédiat, que les applications $\langle\ ,\ \rangle$ et v associées à l'extension (E,π) sont bien celles dont on était parti et le théorème est démontré.

REFERENCES

[Se] J. P. Serre : Représentations linéaires des groupes finis, Hermann.

[Ei] M. Eichler : Introduction to the theory of algebraic numbers and functions, Academic Press.

[Ba] M. Bachmakov : Cohomologie des courbes elliptiques, Cours à Orsay.

[Ro] P. Roquette : Uber das Hassesche Klassenkörperzerlegungsgesetz und seine Verallgemeinerung für beliebige abelsche Funktionenkörper, J. reine angew. Math. 197, 49-67 (1957).

[De-Ra] P. Deligne et M. Rapoport : Les schémas de modules de courbes elliptiques, Modular Functions of one variable, II, Lecture Notes 349, Springer.

[La] S. Lang : Elliptic functions, Addison Wesley.

[Vé] J. Vélu : Courbes modulaires et courbes de Fermat, Sém. de Théorie des Nombres de Bordeaux, 1975-76.

[Hu] A. Hurwitz, Über endliche Gruppen ..., M. Annalen 27 (1886), p. 183-233 (= Math. Werke, I, p. 189-240).

(Texte définitif
reçu le 27 avril 1978)

Jacques VÉLU
3 Résidence du Parc
91120 PALAISEAU