COURS DE L'INSTITUT FOURIER

ARMAND BRUMER

Introduction

Cours de l'institut Fourier, tome 10 (1975), p. I-V

<http://www.numdam.org/item?id=CIF_1975__10__A1_0>

INTRODUCTION

Le CHAPITRE I est consacré à l'étude des courbes elliptiques et la définition des courbes modulaires. Dans le paragraphe 1, on définit les courbes elliptiques sur un corps de base quelconque K, et on en donne une classification à isomorphisme près, d'abord sur un corps algébriquement clos (par l'invariant j), puis sur un corps quelconque (par un groupe de cohomologie). Ensuite, on étudie le cas classique où K est le corps des complexes (§2), puis le cas où K est un corps local (§3). On énonce en particulier le théorème d'Abel-Jacobi dans chacun de ces deux cas. La paragraphe 4 contient l'étude des points d'ordre N d'une courbe elliptique : ils forment un groupe isomorphe à un sous-groupe de $(\mathbb{Z}/N\mathbb{Z})^2$, et isomorphe à $(\mathbb{Z}/N\mathbb{Z})^2$ lui-même lorsque la caractéristique de K ne divise pas N. Si K est égal à $\mathbb{C}$, on montre que les couples formés d'une courbe elliptique et d'un sous-groupe cyclique d'ordre N sont classifiés, à isomorphisme près, par le quotient du demi-plan de Poincaré par un certain "groupe de congruence" ; en ajoutant à ce quotient un nombre fini de "pointes", on obtient une surface de Riemann compacte, notée $X_0(N)$ et appelée courbe modulaire, dont on calcule le genre. On étudie ensuite quelques propriétés élémentaires des isogénies (c'est-à-dire les homomorphismes non nuls) entre courbes elliptiques. Enfin l'"accouplement de Weil" établit une dualité sur les points d'ordre N d'une courbe elliptique. Au paragraphe 5, on généralise la notion de courbe modulaire, en définissant $X(N)$ et $X_1(N)$, et on montre que $X_0(N)$ est rationnelle sur $\mathbb{Q}$.

Le CHAPITRE II établit une relation entre la série L d'une courbe modulaire et un produit de séries de Dirichlet associées à certaines formes modulaires. Les trois premiers paragraphes étudient les séries de Dirichlet associées aux formes modulaires : le paragraphe 1 généralise la notion de forme modulaire (resp. de forme parabolique) qui a été donnée en (I.2) , et définit la série de Dirichlet associée à une forme parabolique. Au paragraphe 2, on définit les opérateurs de Hecke sur les formes modulaires et on montre que, si une forme parabolique est fonction prore pour tous les opérateurs de Hecke, sa série de Dirichlet admet un certain développement en produit eulérien. Au paragraphe 3, on justifie ce dernier résultat en montrant, à l'aide d'une étude de l'involution d'Atkin-Lehner et des "newforms", qu'il existe "autant que possible" de fonctions propres pour tous les opérateurs de Hecke .

Les paragraphes 4 à 6 introduisent des notions nécessaires à la définition de la série L de $X_o(N)$ et à la démonstration du résultat annoncé : on introduit la notion de jacobienne d'une courbe (§4) ; puis on étudie de plus près les endomorphismes d'une courbe elliptique (en particulier, on énonce ici des résultats concernant ces courbes elliptiques avec multiplication complexe, qui ne seront utilisés qu'au chapitre IV) (§5) ; le paragraphe 6 est consacré à la notion de réduction modulo un idéal maximal de l'anneau des entiers de K , lorsque K est un corps de nombres ou un corps local. Enfin, le paragraphe 7 démontre l'égalité entre la série L de $X_o(N)$ et un produit de séries de Dirichlet associées à des fonctions propres pour tous les opérateurs de Hecke. La clef de cette démonstration est le théorème d'Eichler-Shimura, reliant les opérateurs de Hecke et les traces d'opérateurs de Frobenius. On l'obtient ici à partir des congruences de Kronecker . On trouve à la fin du chapitre II (§8) une étude de la courbe modulaire $X_o(11)$.

Le CHAPITRE III réunit : Dans le paragraphe 1 , l'étude des courbes elliptiques à mauvaise réduction, en particulier le cas de la

"courbe de Tate" , et la définition de la loi de groupe formel associée à une cubique plane ; la hauteur de la loi de groupe formel associée à la réduction d'une courbe elliptique permet de déterminer le "type" de cette réduction. Au paragraphe 2, on étudie le groupe $E(K)$ des points de E rationnels sur K , lorsque K est égal à $\mathbb{C}$, à $\mathbb{R}$, à un corps local, ou à $\mathbb{Q}$; dans ce dernier cas, on énonce plus de conjectures que de résultats. Le paragraphe 3 étudie les propriétés galoisiennes des points d'ordre fini sur une courbe elliptique (d'après J.P. Serre), d'abord sur un corps local, puis sur $\mathbb{Q}$. On n'utilisera pas du tout ce dernier paragraphe dans le chapitre IV .

Le CHAPITRE IV est consacré à la détermination des points rationnels (i.e. rationnels sur $\mathbb{Q}$) sur les courbes modulaires et leurs jacobiennes (d'après B. Mazur). On étudie les courbes $X_0(N)$ de genre non nul, avec N premier. On montre, en étudiant les points rationnels sur la jacobienne de $X_0(N)$, que le nombre de points rationnels sur $X_0(N)$ est fini. L'involution d'Atkin-Lehner permet de "couper" la jacobienne J de $X_0(N)$ en deux sous-variétés, notées J_+ et J_- . Le paragraphe 1 montre qu'il y a en général une infinité de points rationnels sur J_+ (*) ; on est amené à définir les courbes hyperelliptiques et à déterminer les courbes modulaires hyperelliptiques. On étudie ensuite (§2) la variété J_- : elle possède deux sous-groupes cycliques de même ordre $n = \frac{N-1}{(N-1,12)}$, le premier (noté C) étant formé de points rationnels, et le second (noté Σ) étant seulement "globalement" rationnel. Ces deux sous-groupes sont annulés par un même idéal (appelé idéal d'Eisenstein) de l'algèbre engendrée par tous les opérateurs de Hecke, considérés comme endomorphismes de J ; on étudie ensuite les localisées de cette algèbre aux idéaux maximaux P engendrés par l'idéal d'Eisenstein et un diviseur premier p de n . Pour simplifier les démonstrations, on suppose toujours p

---

(*) On suit ici une conférence de B. Mazur faite à Grenoble en mai 1975.

impair ; lorsque $p = 2$, les résultats ont été démontrés par B. Mazur, mais c'est beaucoup moins facile. Le but du paragraphe 3 est de montrer que C et Σ sont les seuls sous-groupes "de ce type" de J ; pour cela, on a besoin de résultats de Deligne-Rapoport sur le schéma de Néron de J (la démonstration d'une partie de ces résultats est esquissée au paragraphe 5). On montre alors que le groupe de torsion des points rationnels sur J est égal à C . Ensuite, en admettant que tous les points de J rationnels sur $\mathbb{R}$ et annulés par l'idéal P sont en fait rationnels sur $\mathbb{Q}$ (ce qui a été montré par B. Mazur), on détermine la structure du groupe des points de J annulés par P . Ce résultat permet de faire des calculs de dimension de groupes de cohomologie, pour la topologie f.p.p.f. de faisceaux, au paragraphe 4. On obtient ainsi une double inégalité qui permet de montrer qu'un certain quotient de J , non trivial, n'a qu'un nombre fini de points rationnels ; mais alors un argument facile prouve que $X_0(N)$, lui aussi, n'a qu'un nombre fini de points rationnels. On termine le paragraphe en montrant sur des exemples, comment la double inégalité obtenue plus haut donne aussi des résultats sur des propriétés de divisibilité de nombres de classes d'extensions quadratiques imaginaires.

Le paragraphe 5 est un appendice qui groupe : une "démonstration" d'une partie des résultats utilisés sur le schéma de Néron de J . Puis une étude de la conjecture de Ogg selon laquelle les seuls points rationnels de $X_0(N)$ sont les pointes ; on montre ici que la conjecture est vérifiée lorsque le nombre de points rationnels sur $J_{\mathbb{Q}}$ est fini . Comme il reste un nombre fini de valeurs de N auxquelles notre démonstration ne s'applique pas, on voit sur trois exemples comment la théorie de la multiplication complexe ou la réduction des courbes elliptiques permettent de se tirer d'affaire.

Il a été récemment démontré par B. Mazur [21] que, pour tout entier $N \geq 13$ et pour $N = 11$, les seuls points rationnels de la courbe modulaire $X_1(N)$ sont ses pointes ; autrement dit, si une courbe elliptique définie sur $\mathbb{Q}$ a un point d'ordre N rationnel sur $\mathbb{Q}$, alors : $N \leq 10$ ou $N = 12$.

La lecture des 3 premiers chapitres ne suppose guère que quelques connaissances sur les surfaces de Riemann (théorèmes de Riemann-Roch et de Riemann-Hurwitz). On espère que les lecteurs ne connaissant presque pas de géométrie algébrique ne seront pas rebutés par le chapitre IV, et que les autres seront indulgents.

La plupart de ce qu'on trouve ici se trouve : pour le chapitre I, dans : Cassels [4] , Tate [47] , Lang [18] ou Robert [31] ; pour le chapitre II, dans : Shimura [43] , Ogg [26] , ou Joly [16] ; pour le chapitre III, dans : Tate [47] et Serre [39] ; pour le chapitre IV, dans : Mazur [21] ou Mazur-Serre [22] .

Chaque chapitre (A) est partagé en paragraphes (a) , en sous-paragraphes (b) , et en sections (c) . La référence à un sous-paragraphe du même chapitre (resp. d'un autre chapitre) est de la forme (a.b) (resp. (A,a.b)) ; la référence à une section est de la forme (a.b.c) (resp. (A,a.b.c)) .

Ce texte est basé sur un cours professé par A. BRUMER au Laboratoire de Mathématiques Pures de l'Université de Grenoble en 1975. Nous remercions J.M. FONTAINE, J.R. JOLY et J.J. PAYAN pour leurs nombreux conseils et explications.

Nous tenons aussi à remercier Madame GUTTIN-LOMBARD et Messieurs GAUDE et GIRARD pour la compétence et la gentillesse avec lesquelles ils ont effectué la réalisation matérielle de ce travail.