Progress in Mathematics

Volume 91

Series Editors

J. Oesterlé
A. Weinstein

Séminaire de Théorie des Nombres, Paris 1988–1989

Edited by
Catherine Goldstein

1990

Birkhäuser
Boston · Basel · Berlin

[13] G. Shimura. — On elliptic curves with complex multiplication as factors of the Jacobian of modular function fields, *Nagoya Math. J.* **43**, (1971), 199-208.

[14] G. Shimura. — *Introduction to the arithmetic theory of automorphic functions*, Publ. Math. Soc. Japan No. 11, Iwanami Shoten and Princeton, 1971.

[15] G. Shimura. — Class fields over real quadratic fields and Hecke operators, *Ann. of Math.* **95**, (1972), 130-190.

[16] A. Weil. — Abelian varieties and the Hodge ring, *Collected Papers*, Springer-Verlag **vol. III**, (1980), 421-429.

[17] H. Imai. — On the Hodge groups of some abelian varieties, *Kodai Math. Sem. Rep.* **27**, (1976), 367-372.

Kumar MURTY
Department of Mathematics
University of Toronto
Toronto, CANADA M5S 1A1

Séminaire de Théorie des Nombres
Paris 1988–89

Développement de la loi de groupe sur une cubique

Norbert SCHAPPACHER

0. Rappel mathématique anhistorique
1. Préhistoire de la méthode des tangentes et sécantes
2. La méthode algébrico-géométrique des tangentes et sécantes
   2.1 Newton
   2.2 Lagrange
   2.3 Cauchy
   2.4 Les *Nouvelles Annales de Mathématiques* autour de 1880 — et Monsieur Sylvester
   2.5 Le mémoire de Sylvester
3. La tradition analytique
4. Poincaré
5. Beppo Levi (et Hurwitz)
6. De Mordell à Weil

Dans cet article, j'essaie de tracer les courants majeurs de l'histoire de la loi de composition de points sur une cubique, resp. de la loi de groupe sur les points rationnels d'une courbe elliptique. Donc, contrairement aux us du *Séminaire de Théorie des Nombres Paris*, aucun résultat mathématique nouveau n'est présenté. Toutefois les remarques suivantes sembleront peut-être intéressantes aux arithméticiens d'aujourd'hui qui font partie du fleuve dont on explore ici un affluent. En effet, les travaux de B. Levi discutés au §5 ont récemment attiré

l'attention de quelques arithméticiens intéressés par des méthodes 'naïves' dans l'étude des points rationnels de courbes modulaires — *voir* [Washington 1990].

Personnellement, j'ai commencé à m'occuper de cette partie de l'histoire de l'arithmétique à la suite de plusieurs discussions et échange de lettres et manuscrits avec Catherine Goldstein. Dans l'exposé qui suit, il me serait souvent impossible de séparer ses idées de ce que j'ai trouvé moi-même. D'autre part, la rédaction (y inclus la façon de présenter le matériel) de cet article n'engage pas sa responsabilité, et les erreurs qu'on y trouverait ne seront que les miennes.

La raison principale de publier ce que je sais maintenant sur l'histoire de la loi de groupe sur une courbe elliptique — bien que mes connaissances soient surement encore incomplètes — est que les quelques aperçus de cette histoire qui existent dans la littérature — *voir* par exemple [Scriba 1984] — paraissent inadéquats, du moins dès qu'ils abordent la fin du dix-neuvième et notre siècle. En particulier nous allons voir que ce n'est pas Poincaré qui a découvert la loi de groupe sur les points rationnels d'une courbe cubique.

0. Rappel mathématique anhistorique

Précisons notre sujet tel qu'on le voit aujourd'hui. Soient F un corps[1] et $\mathcal{C}$ une courbe algébrique réduite définie sur F, qui admet sur F un plongement dans $\mathbf{P}^2$ comme courbe donnée par une équation homogène de degré 3. Appelons encore $\mathcal{C}$ son image dans le plan projectif. Alors, si $P, Q \in \mathcal{C}(F) \subset \mathbf{P}^2(F)$ sont deux points rationnels *non-singuliers* de la courbe, on obtient un troisième point R en traçant la droite (*sécante*) par P, Q dans $\mathbf{P}^2$ et en prenant le troisième point d'intersection de cette droite avec $\mathcal{C}$ (qui existe d'après le 'théorème de Bezout'). Si $P = Q$, on prend la *tangente* à $\mathcal{C}$ en ce point au lieu de la sécante. R est de nouveau un point rationnel sur F; en fait ses coordonnées projectives se calculent rationnellement en termes de celles de P, Q et de l'équation de $\mathcal{C}$. De plus, R est un point non-singulier; en fait, ou bien il est de multiplicité un, ou bien il se confond avec P ou Q.

Cette loi de composition $(P, Q) \mapsto R$ — obtenue par ce qu'on appelera *la méthode des tangentes et sécantes* — sur l'ensemble $\mathcal{C}(F)_{\mathrm{ns}}$ des points F-rationnels non-singuliers de $\mathcal{C}$ est évidemment commutative. Mais en général

[1] Le lecteur patient trouvera les quelques endroits où on suppose en fait que la caractéristique de F n'est pas 2 ou 3.

elle n'est pas associative — trouver des contre-exemples, ou étudier l'opération $(x, y) \mapsto -(x + y)$ dans un groupe commutatif!

Si F est suffisamment grand, la loi n'admet pas non plus d'élément neutre : en un tel point O, l'opération devrait satisfaire $(O, O) \mapsto O$. Ce serait donc un point d'inflexion. Mais il y a des points $P \in \mathcal{C}(\overline{F})$ tels que la droite passant par P et n'importe lequel des 9 points d'inflexion dans $\mathcal{C}(\overline{F})$ ne soit pas tangente en P.

Pour obtenir une structure de groupe, supposons que $\mathcal{C}(F)_{\mathrm{ns}}$ contienne un point d'inflexion O.[2] Alors on définit $P + Q$ comme étant le point que construit la méthode des tangentes et sécantes appliquée à O et au point R trouvé avant. Ceci fait de O un élément neutre de l'opération $+$ et, pour chaque point $P \in \mathcal{C}(F)_{\mathrm{ns}}$, la méthode des tangentes et sécantes appliquée à O et P donne un point $-P$ qui satisfait $P + (-P) = O$. Finalement, la loi $+$ est aussi associative. Ceci peut se démontrer algébriquement ou de façon géométrique, comme corollaire du fait que deux cubiques planes qui passent par 8 points en auront en commun un neuvième. — *Cf.* par exemple [Clemens 1980, §2.3].

Vue de cette façon purement géométrique, la modification qui transforme la méthode des tangentes et sécantes en une loi de groupe peut paraître très astucieuse. D'autre part, sur le corps $F = \mathbf{C}$ elle peut être motivée par la paramétrisation analytique des courbes elliptiques :

Si $F = \mathbf{C}$ et $\mathcal{C}$ est lisse, alors choisissant un élément neutre $O \in \mathcal{C}(\mathbf{C})$ comme précédemment, ainsi qu'une différentielle non-nulle $\omega \in H^0(E, \Omega^1)$, il existe un unique réseau $L \subset \mathbf{C}$ et un isomorphisme analytique

$$\psi : (\mathbf{C}/L, 0) \longrightarrow (\mathcal{C}(\mathbf{C}), O), \quad \psi^*\omega = d(z \bmod L).$$

La loi de groupe $+$ sur $\mathcal{C}(\mathbf{C})$ s'obtient alors par transport de structure de la loi du groupe additif de $\mathbf{C}$ modulo L. Quelques auteurs dont on parlera plus loin font allusion à l'existence de ψ en parlant d'un *paramètre* (ou *argument*) *analytique* (ou *elliptique*).

Concluons cette partie mathématique de l'article par une remarque de Weil : Tout groupe algébrique connexe de dimension 1 sur un corps F est de la forme $\mathcal{C}(F)_{\mathrm{ns}}$, pour une cubique $\mathcal{C}$ convenable. — En effet, un tel groupe est soit le

[2] Si $\mathcal{C}(F)_{\mathrm{ns}}$ est non-vide, alors $\mathcal{C}$ est birationnellement équivalente sur F à une cubique ayant un point d'inflexion F-rationnel.

groupe additif $\mathbf{G}_a$ (correspondant au cas où C admet une singularité cuspidale), soit un tore (donné par C ayant un point double), soit enfin une courbe elliptique (C lisse).

1. Préhistoire de la méthode des tangentes et sécantes

Il y a peut-être 10 ans de cela, André Weil donnait à l'ancienne Ecole Normale Supérieure de Jeunes Filles à Montrouge une suite de conférences consacrées à quelques chapitres de ce qui est devenu le livre [Weil 1983]. Je me souviens d'un de ces exposés où Weil s'étonnait du fait que Dieudonné — il me semble que le conférencier évitait de prononcer ce nom —, dans son histoire de la géométrie algébrique [Dieudonné 1974], ne mentionne point Diophante. Weil trouvait ceci d'autant plus surprenant que le même Dieudonné était collaborateur à un ouvrage de première importance dans l'histoire récente de la géométrie algébrique, qui ne traite pourtant que des notions algébriques.

Il me semble légitime de chercher dans l'histoire des mathématiques les endroits où nous reconnaissons, souvent sous une forme encore très vague ou obscure, une idée importante. Ainsi, la classification des exercices dans l'Arithmétique de Diophante selon le genre des courbes sous-jacentes, s'offre clairement à nos yeux instruits. *Cf.* [Weil 1983, chap. I, §X]. C'est autre chose de déduire d'une telle perspective moderne la théorie selon laquelle Diophante a dû posséder la notion du genre d'une courbe, ou au moins les notions de courbes de genre 0, et 1 .... En fait, le mathématicien André Weil évite ce genre de pièges. Mais ceci n'est pas vrai de tous les historiens des mathématiques, même professionnels.

Ainsi, pour revenir à notre sujet, prenons l'article d'Isabelle Bachmakova [Bachmakova 1966]. Après avoir décrit de façon géométrique la méthode des tangentes et sécantes, elle se propose de "montrer" que "ces deux constructions" [*i.e.*, par la tangente et par la sécante] "se trouvent toutes deux dans l'*Arithmétique* de Diophante". La 'démonstration' consiste en l'observation qu'une certaine construction décrite dans sa notation algébrique par Diophante "est équivalent[e] à mener une droite ..... Il est facile de remarquer que la condition de Diophante est équivalente à ce que la droite .. soit tangente." Et ainsi de suite. [Bachmakova 1966, 294]

Disons simplement que ces équivalences géométriques ne se trouvent pas

dans l'œuvre de Diophante et qu'une véritable démonstration du fait qu'il les possédait exigerait des arguments bien plus pertinents que des reformulations mathématiques, même si elles sont pour nous triviales. C'est pour cette raison que nous comptons Diophante dans la *pré*histoire de la méthode des tangentes et sécantes — le terme 'préhistoire' étant expliqué par les phrases précédentes.

De Diophante, Bachmakova passe à Fermat : lui aussi aurait possédé la méthode de la tangente. Ici l'argument semble mieux fondé à première vue; car, contrairement à son prédécesseur grec, Fermat nous a légué des traités géométriques. Ainsi Bachmakova construit un lien entre les découvertes arithmétiques de Fermat et ses travaux sur les extrema et tangentes. [Bachmakova 1966, §6]

Toutefois, ce qu'on sait de Fermat ne permet pas de conclure qu'il connaissait l'interprétation géométrique de la méthode de Diophante qu'il pratiquait avec tant de succès.[3]

De plus, en ce qui concerne l'invention propre de Fermat en théorie des nombres : la *descente infinie*, il affiche une forte tendance à la séparer fermement de la géométrie. Fermat nous a laissé une seule démonstration par *descente infinie* écrite suffisammment en détail pour qu'on puisse la reconstruire avec sureté : la démonstration du théorème qu'il n'y a aucun triangle rectangle dont les côtés sont des nombres rationnels et dont l'aire soit un carré.[4] Vue d'aujourd'hui, la démonstration de Fermat décrit la division par ± 2 de points sur la courbe elliptique $y^2 = x^3 - x$. [5] Mais même si Fermat avait l'interprétation géométrique de l''ascente' en tête, il s'est systématiquement gardé de voir

[3] Ici je parle de ce que Weil traite sous le nom de "ascent" : [Weil 1983, chap. II, §XV]. — "Was Fermat aware of this geometric interpretation? ... For lack of evidence, this intriguing question must remain unanswered." [Weil 1983, p. 108f.]

[4] Note en marge du *Problema XX* de Bachet (édition de Diophante) : [Fermat I, *Observatio* XLV, 340f], traduit : [Fermat III, 271f]. *Cf.* [Fermat II, $\mathcal{N}°$ CI, Fermat à Carcavi, Août 1659, 431f] — Pour l'importance historique du résultat, *cf.* [Dickson 1920, 459–472] et [Koblitz 1984]. Pour des reconstructions mathématiques du texte de Fermat, *voir* par exemple [Zeuthen 1903, 163], [Heath 1910, p.294f], [Weil 1983, 79], [Schappacher 1989, 153]; *cf.* aussi [Goldstein 1990]. Notons toutefois que les reconstructions ne relèvent pas un joli petit détail à la fin : Afin de compléter la descente il faut démontrer que le nouveau triangle rectangle rationnel d'aire carrée, construit dans la démonstration est 'plus petit' que celui supposé exister au début. Fermat prend comme mesure de grandeur la somme des deux 'paramètres pythagoriciens' des triangles et c'est sur la suite décroissante de ces sommes d'entiers positifs qu'il fait jouer l'*απαγωγὴν εισ αδύνατον* qui permet de conlure : ... *dabitur in integris summa duorum quadratorum ejusdem naturæ, priore minor.*

[5] Si le triangle est (a, b, c), $a, b, c \in \mathbf{Z}$, $2|b$, et son aire $\frac{ab}{2} = A^2$, poser $x = \frac{a+c}{b}$, $y = 2A\frac{a+c}{b^2}$. — Je dis '± 2', parce que Fermat ne peut travailler qu'avec des coordonnées positives.

la descente de ce même point de vue. Car pour cette méthode il faut toujours arriver à une suite discrète de quantités positives. Il semble que ceci amenait Fermat à penser qu'il s'agissait d'une méthode incompatible avec des arguments algébriques ou géométriques généraux qui s'étendent forcément à la quantité continue.[6] — Nous ne poursuivons pas ici le développement historique de la *descente infinie*. Disons simplement qu'un lien entre la *descente* et le sujet de cet article est évident au plus tard dans les travaux de Hurwitz, Mordell et Weil cités plus loin (§§5, 6; cf. aussi [Goldstein, Schappacher 1990]).

Dans la suite de cet article, je vais distinguer trois classes d'auteurs qui ont contribué au développement historique de la méthode des tangentes et sécantes. Au §2 on regroupe tous ceux qui ont traité cette méthode sans référence à un paramètre analytique. Au §3, on discutera brièvement la tradition purement analytique. Et dans les numéros ultérieurs sont regroupés des travaux qui traitent la méthode géométrique des tangentes et sécantes, mais qui l'interprètent en même temps en terme d'un paramètre analytique. Cette organisation n'est qu'un schéma convenable pour l'exposé; elle ne veut pas suggérer des 'écoles' différentes dans l'histoire de la méthode des tangentes et sécantes.

[6] [Fermat II, $\mathcal{N}°$ LXXXI, *Second défi de Fermat aux mathmaticiens*, Février 1657; 334] : *Quæstiones pure arithmeticas vix est qui proponat, vix qui intelligat. Annon quia Arithmetica fuit hactenus tractata geometricè potius quam arithmeticè ? Id sane innuunt plerage et Veterum et Recentiorum volumina; innuit et ipse Diophantus. Qui licet à Geometria pulo magis quàm cæteri discesserit, dum Analyticen numeris tantum rationalibus adstringit, eam tamen partem Geometriâ non omnino vacare probant satis superque Zetetica Vietæa, in quibus Diophanti methodus ad quantitatem continuam, ideoque ad Geometriam porrigitur.*

2. La méthode algébrico-géométrique des tangentes et sécantes

2.1 Newton fut — à ma connaissance — le premier auteur à énoncer la méthode des (tangentes et) sécantes sous sa forme géométrique — *voir* [Newton 1971, 110–115]. Il est remarquable de voir Newton discuter la construction de points rationnels sur une courbe algébrique à partir d'un ou plusieurs points rationnels donnés : D'abord pour une conique, donnée par une équation quadratique, où il obtient des points rationnels par des droites de pente rationnelle passant par un point rationnel. Puis il passe aux cubiques pour expliquer laconiquement que, étant donnés trois points rationnels non collinéaires sur une cubique, la *méthode de la sécante* — il ne mentionne pas le cas de points non distincts — appliquée à deux quelconques d'entre eux, et puis itérée avec des points déjà obtenus, permet de "repérer d'innombrables autres" points rationnels. Donc ni dans les données ni dans les résultats, Newton ne s'occupe de points qui se confondent. Le court paragraphe est accompagné d'un dessin (qui contient une petite erreur, dûment rectifiée par l'éditeur).

Cette courte page d'un des cahiers de Newton consacrée à la méthode des sécantes semble se situer à une époque où l'auteur réfléchissait aussi sur les problèmes arithmétiques de Diophante. Il s'est d'ailleurs occupé de la théorie générale des cubiques à deux reprises, à dix ans d'intervalle.

2.2 Lagrange. Dans son travail célèbre [Lagrange 1777], l'auteur présente une analyse très soigneuse des points rationnels de la courbe $x^4 - 2y^4 = \pm z^2$ — en normalisation de Weierstrass qui nous est habituelle aujourd'hui, c'est $Y^2 = X^3 - 2X$. Le groupe des points rationnels de cette courbe est de rang 1. — Dans les deux derniers numéros (12 et 13), Lagrange montre "comment on peut simplifier et généraliser à quelques égards la méthode ordinaire pour les égalités qui passent le second degré [en fait, il traite le degré 3 et certaines équations de degré 4], suivant laquelle, en connaissant une solution, on peut trouver plusieurs autres" [Lagrange 1777, 396]. Ce qu'il décrit est en fait la *méthode de la tangente* qu'il applique à un point donné initialement et puis par itération au dernier point obtenu. La description n'est pourtant pas géométrique mais passe par des formules algébriques, la tangente est décrite par son équation linéaire en termes de dérivées partielles de l'équation de la courbe.

2.3 Cauchy. Dans ces *anciens Exercices* de l'année 1826, Cauchy insère un chapitre *Sur la résolution de quelques équations indéterminées en nombres entiers*,[7] dont le §*V* est consacré à .. *la résolution en nombres entiers de l'équation homogène du troisième degré entre trois variables.* Ici il expose la méthode de la tangente par des formules algébriques, sans allusion à la situation géométrique, ni même la notation de dérivée partielle comme chez Lagrange. Vers la fin de ce § [Cauchy 1887, 312–314], il en fait de même de la méthode de la sécante.

2.4 Les *Nouvelles Annales de Mathématiques* autour de 1880 — et Monsieur Sylvester. Ce *Journal des candidats aux écoles polytechnique et normale* contient un grand nombre de petits exercices (et de longs laïus) élémentaires. Il n'est pas surprenant de voir aussi resurgir de temps à autre la méthode des tangentes et sécantes.

Edouard Lucas, dans [Lucas 1878], aussi bien que Desboves, dans son traité un peu lourd [Desboves 1879], sont dans la tradition de Lagrange en ce qu'ils essayent d'attraper uniquement par la méthode de la tangente tous les points rationnels à partir de points initiaux. Selon le nombre de points indépendants requis au départ — [Desboves 1879, 491] parle de *solutions initiales* —, Lucas classifie les courbes comme étant *monobasiques, bibasiques*, etc.

Mais ce n'est pas la première fois que la notion du rang d'une courbe elliptique est ainsi pressentie dans la littérature. En fait, Lucas ajoute "que cette idée de classification ... est due, je pense, à M. Sylvester, qui possède, depuis longtemps, un Mémoire inédit sur ce sujet intéressant." [Lucas 1878, 509] Et Sylvester avait 20 ans plus tôt publié, sinon ce mémoire, au moins une annonce de ses résultats : [Sylvester 1858]. Là il affirme — moyennant une normalisation de l'équation et de ses solutions — l'existence, pour tout $n > 1$ d'une certaine expression rationnelle de degré n^2, bien déterminée, qui, appliquée aux coordonnées d'un point rationnel de la courbe en question, en donne un autre. Il appelle ceci la n-ième *derivation* sur la courbe. A titre d'exemples géométriques, il cite

> "... the tangential (the name adopted from me by Mr. Cayley to express the point of intersection of a tangent to a cubic curve at any point with the curve)"

comme seconde dérivation (de degré 4), et :

> "So again, as I also suggested to Mr. Cayley, the point in which the conic of closest contact with a cubic curve cuts the curve will necessarily have a derivative system of coordinates of a square-numbered degree in respect of the original ones, which by actual trial Mr. Cayley has found to be the 25th. Mr. Salmon, I believe, has obtained in certain geometrical investigations derivatives of the 49th degree."

Il parle de courbes dont l'ensemble des solutions est "*monobasic*; that is to say, all their solutions are known functions of one of them, which I term the *base*, and which is characterized by this property —that of all the solutions possible it is the one for which the *greatest* of the three variables is the *smallest* number possible." Il affirme avoir trouvé "a large class of equations, soluble, or possibly so, it is true, but enjoying the property that all their solutions in integers [*i.e.*, entiers positifs, ou non négatifs?], when they exist, are *monobasic*." Quelles équations avait-il en tête?

Revenons à l'article [Lucas 1878].[8] Non seulement Lucas y discute la méthode de la tangente; mais il y fait encore une liste de trois méthodes géométriques qui permettent d'obtenir un point rationnel d'une cubique à partir de points rationnels donnés auparavant : premièrement la méthode de la tangente; ensuite la méthode de la sécante; et finalement il propose ceci :

> "Si l'on connaît cinq solutions de l'équation proposée, on obtient, en général, une sixième solution, en prenant le point d'intersection avec la courbe, de la conique passant par les cinq points qui correspondent aux solutions données; on peut d'ailleurs supposer plusieurs de ces points réunis en un seul, et en particulier tous les cinq réunis en un seul."

Lucas ne dit pas que cette méthode se réduit à une combinaison convenable d'applications de la méthode des tangentes et sécantes. Mais Sylvester ne tarda pas à remarquer ce fait [Sylvester 1879/80, 314], dans le grand mémoire — *voir* §2.5 plus loin — par lequel il atteint le but personnel annoncé à la fin de la note de 1858 :

[7] [Cauchy 1826, 233–260] = [Cauchy 1887, 286–315].

[8] Je n'ai pas réussi à consulter [Lucas 1877].

> "I hope to have tranquillity of mind ere long to give to the world my memoir, or a fragment of it, "On an Arithmetical Theory of Homogeneous and the Cubic Forms," the germ of which, now, alas! many years ago, first dawned upon my mind on the summit of the Righi, during a vacation ramble." [Sylvester 1858, 109]

Notons en passant qu'une variante — avec deux paraboles — de la troisième méthode géométrique de Lucas est utilisée par Mordell dans la démonstration de son célèbre théorème selon lequel — comme on dit aujourd'hui — le groupe des points rationnels d'une courbe elliptique est de type fini [Mordell 1922], *voir* §6 plus loin.

Restons encore brièvement avec les *Nouvelles Annales* avant d'aborder plus en détail le grand mémoire de Sylvester.

La plus grande partie de l'article [Desboves 1886] est une reformulation de Cauchy. A la fin il propose de transformer une équation cubique en une équation biquadratique qui peut être plus facile à résoudre. Ceci encore nous rappelle l'article [Mordell 1922] où Mordell préfère les formes biquadratiques aux modèles cubiques des courbes elliptiques que nous aimons aujourd'hui — *voir* à ce sujet [Cassels 1986].

Desboves dans [Desboves 1879] étudie la famille des courbes $aX^m + bY^m = cZ^n$ (où m, n, a, b, c sont des entiers, m, n positifs). Il sait que la nature de l'ensemble des solutions dépend sensiblement du degré de l'équation. Mais les auteurs des *Nouvelles Annales* ne disposent apparemment pas de la notion de *genre*. On ne s'étonnera donc pas de trouver, dans ce journal dans la tradition de l''analyse diophantienne' orientée plus vers l'étude d'exemples que vers la théorie générale, quelques énoncés généraux incorrects.[9]

2.5 Le mémoire de Sylvester.

Le grand mémoire [Sylvester 1879/89] représente le point culminant de l'histoire de la méthode des tangentes et sécantes dans la mesure où il contient l'analyse la plus avancée de la structure algébrique induite par cette méthode sur l'ensemble

[9] Par exemple [Jonquières 1878, 444] : "... Ce résultat ... vient à l'appui de l'observation déjà signalée par M. Lucas, qu'une équation indéterminée du quatrième degré à trois inconnues ..., qui admet une solution en nombres entiers, n'en admet très-souvent pas d'autre, contrairement à ce qui a lieu pour l'équation du troisième degré, où une première solution en entraîne une infinité d'autres."

des points rationnels d'une cubique, sans la moindre référence à un paramètre analytique.[10] D'autre part, peut-être à cause du style de travail et de rédaction qu'on lui connaît, Sylvester ne parvient pas à une présentation bien finie de cette structure algébrique. Il est d'ailleurs peu probable qu'il disposait de la notion abstraite d'un groupe abélien.[11] Voici sommairement ce qui se trouve sur notre sujet dans ce mémoire [Sylvester 1879/80, 351–365] qui en traite aussi d'autres.

Première Observation de Sylvester. Un point sur la cubique étant fixé, l'ensemble des points qui s'en déduisent par application itérée de la méthode de la tangente est fermé par rapport à la méthode des tangentes et sécantes.

Sylvester adopte la notation suivante. Le point de départ est appelé 1. Le point qui résulte par la méthode des tangentes et sécantes de deux points représentés par les nombres k et l respectivement est noté (k, l) ou (l, k). Le premier 'tangential' de 1 est donc $(1, 1)$ ce que Sylvester appelle aussi 2, et il pose $4 = (2, 2)$. Ensuite il définit, pour tout k, $k + 1 = (1, k)$ et $k + 2 = (2, k)$ (ce qui est compatible avec la définition de 4). Puis il affirme — référant le lecteur à la théorie de la 'residuation'[12] — la règle suivante, que nous pouvons voir aujourd'hui comme une variante de l'associativité de la loi de groupe.

$$((a, b), (c, d)) = ((a, c), (b, d)).$$

Sylvester en déduit formellement que si r, s sont des entiers non divisibles par 3 et que $r > s$, alors $(r, s) = r \ddagger s$, où $r \ddagger s = r \pm s$ le signe étant choisi tel que $3 \nmid r \ddagger s$. Par conséquent, l'ensemble de tous les points qui se déduisent de 1 par la méthode des tangentes et sécantes est $\{k \in \mathbf{Z} |\ k > 1, 3 \nmid k\}$. Il calcule (sur une forme normalisée de la cubique) que les coordonnées de k sont des fonctions rationnelles de degré k^2 des coordonnées de 1.[13]

[10] Sylvester affiche, dans un autre contexte, une certaine prédilection pour "... an intuitional proof ... without any recourse to concepts drawn from reticulated arrangements, as in the applications of geometry to arithmetic made by Dirichlet and Eisenstein." [Sylvester 1879/80, 344]

[11] Dans [Sylvester 1879/80, 353ff] le mot "group" désigne un ensemble de points fermé par rapport à la méthode des tangentes et sécantes.

[12] Le lecteur trouvera un exposé très clair de cette théorie dans le traité de Salmon : [Salmon 1879, §§158–161, pp. 136–140]. La notion clé est la suivante. "If two systems of points [*nous dirions aujourd'hui :* deux diviseurs] ... together [*i.e.*, leur somme] make up the complete intersection with the cubic of a curve of any order, one of these [*i.e.*, chacun des deux] is said to be the *residual* of the other." [Salmon 1879, 136]

[13] Cette constatation est accompagnée, [Sylvester 1879/80, 356], par cette note en bas de page :

Deuxième Observation de Sylvester. Un point d'inflexion I étant fixé sur la courbe, Sylvester appelle *opposé* d'un point p le point qui résulte de I et de p par la méthode des tangentes et sécantes : $p' = (I,p)$. Alors l'ensemble formé des points considérés dans la première observation et de ses opposés est fermé sous la méthode des tangentes et sécantes.

Sylvester pose $(1', 3i-1) = 3i$ [14] et vérifie explicitement cas par cas que $\{I\} \cup \{k|\ k \geq 1\} \cup \{k'|\ k \geq 1\}$ est fermé sous l'opération (,). Il se convainc aussi de ce que le degré de l'expression rationnelle des coordonnées des points k et k' est k^2, pour tout k.

Traduisons ce que trouve Sylvester en termes de la loi de groupe sur la courbe relative à l'élément neutre I. L'opération $k \mapsto k'$ est aussi le passage au négatif dans le groupe. Si P est le point de départ 1, alors on trouve pour tout $i \geq 0$:

$$(3i) = 3iP, \quad (3i+1) = (3i+1)P, \quad (3i+2)' = (3i+2)P.$$

Les notations adoptées par Sylvester ont donc, pour un oeil moderne, tendance à voiler la présence du groupe, isomorphe à (un quotient de) $\mathbf{Z}$, engendré par P.

"The proof here supplied is sufficiently exact to dispel any reasonable doubt as to the truth of the law; but an exact proof which does not assume but demonstrates the non-existence of latent common measures .... will be furnished under Title 5 — one of the most surprising feats of demonstration which it has ever fallen to the author's lot to accomplish." — Il revient sur ce point 5 pages plus loin où il avoue avoir démontré seulement que le degré de k est borné par k^2. Il ajoute : "... before I come to an end of the discussion I trust to be able to establish with *Dirichletian* rigour that the order is actually equal to the square ..." — phrase à laquelle est rajoutée la note en bas de page : "This anticipation (for it was only such when these words were written) will be found fully realised under Title 5."

[14] Corriger les fautes d'impression [Sylvester 1979/80, 361, ligne 12].

3. La tradition analytique

Dans ce numéro je répète une observation de Scriba sur les théorèmes d'Euler relatifs aux intégrales elliptiques et sur une petite note apparemment peu connue de Jacobi. Commençons avec Euler. Je cite un passage de [Scriba 1984, 25f] relatif à l'équation $y^2 = f(x) = ax^3 + bx^2 + cx + d$:

> "Beim Studium elliptischer Integrale hatte Euler bemerkt, daß, falls man für einen Punkt $A(x,y)$ ... definiert
>
> $$\Pi(A) = \int_\infty^x \frac{d\xi}{y} = \int_\infty^x \frac{d\xi}{\sqrt{f(\xi)}},$$
>
> es zu zwei entsprechend definierten Punkten A und B immer einen dritten C auf [der Kurve] gibt, daß
>
> $$\Pi(A) + \Pi(B) = \Pi(C),$$
>
> wobei sich die Koordinaten von C rational aus denen von A und B ausdrücken lassen [Euler 1912/13]. Zu diesem Additionstheorem tritt das Eulersche Multiplikationstheorem
>
> $$\Pi(D) = n.\Pi(C),$$
>
> d.h. es gilt auch hier, daß sich für ganzzahliges n die Koordinaten von D rational aus denen von A ausdrücken lassen. Sind also einer oder zwei rationale Punkte bekannt, kann man [mit diesen Sätzen] weitere finden."

Mais cette façon analytique de construire de nouveaux points rationnels à partir d'un ou deux points donnés n'était jamais appliquée aux problèmes diophantiens par Euler. Ceci étonnait Jacobi tant qu'il rédigea un petit article de propagande pour l'"usage de la théorie des intégrales elliptiques et abéliennes dans l'analyse diophantienne' : [Jacobi 1835]. Il généralise les deux théorèmes d'Euler en un troisième concernant des $\mathbf{Z}$-combinaisons linéaires arbitraires,

$$\Pi(x) = m_1\Pi(x_1) + \ldots + m_n\Pi(x_n),$$

où x et $\sqrt{f(x)}$ s'expriment encore rationnellement en x_i, $\sqrt{f(x_i)}$.

J'ignore s'il y a un seul travail qui reprend la suggestion de Jacobi. Sinon, faudrait-il conclure que, en mathématiques, la propagande est inutile et toute suggestion doit être menée jusqu'au bout par celui qui la propose?[15] Implicitement le message de Jacobi se transmet dans une grande partie du développement de la théorie des intégrales abéliennes au siècle dernier —*voir passim* le rapport tout à fait impressionnant [Brill, Noether 1892/93]. En particulier on peut mentionner Clebsch — *voir* [Clebsch 1863], [Klein 1926, 298ff]. Tout ce développement forme l'arrière-plan du travail de Poincaré avec lequel nous entrons dans notre siècle.

4. Poincaré

Il ne s'agit pas ici de rendre justice à toutes les idées du long article de Poincaré sur l'arithmétique des courbes algébriques, [Poincaré 1901]. Le lecteur intéressé consultera surtout les notes des éditeurs des œuvres de Poincaré. Je me bornerai essentiellement au traitement de la méthode des tangentes et sécantes. Toutefois il faut souligner que cette méthode est discutée par Poincaré dans un cadre nouveau : celui de l'étude des points rationnels de courbes algébriques dans la perspective de l'invariance birationnelle.

"Les propriétés arithmétiques de certaines expressions et, en particulier, celles des formes quadratiques binaires, se rattachent de la façon la plus étroite à la transformation de ces formes par des substitutions linéaires à coefficients entiers. Je n'ai pas à insister ici sur le parti qui a été tiré de l'étude de ces substitutions et qui est assez connu de tous ceux qui s'intéressent à l'Arithmétique.

On peut supposer que l'étude de groupes de transformations analogues est appelée à rendre de grands services à l'Arithmétique. C'est ce qui m'engage à publier les considérations suivantes, bien qu'elles constituent plutôt un programme d'études qu'une véritable théorie.

Je me suis demandé si beaucoup de problèmes d'Analyse indéterminée ne peuvent pas être rattachés les uns aux autres par un lien systématique, grâce à une classification nouvelle des polynomes homogènes d'ordre supérieur de trois variables, analogue à certains égards à la classification des formes quadratiques.

Cette classification aurait pour base le groupe des transformations birationnelles, *à coefficients rationnels,* que peut subir une courbe algébrique." [Poincaré 1901, *Introduction*, 483f]

[15] Ou est-ce que les temps ont changé?

Le genre[16] étant un invariant birationnel, Poincaré se lance dans son vaste programme en commençant par les "courbes unicursales", *i.e.*, les courbes de genre 0. Sur ce point il a été devancé par Hilbert et Hurwitz [Hilbert, Hurwitz 1890] qui classifient complètement les ensembles possibles de points rationnels des courbes de genre 0 (même avec singularités). Dans [Hurwitz 1917, 446, note 1], Hurwitz dit que Poincaré avait retrouvé indépendamment une partie de leurs résultats. Ainsi Poincaré établit le fait [Poincaré 1901, 488] qu'une courbe de genre 0 est toujours birationnellement équivalente à une droite ou une conique. Ceci remonte à Noether [Noether 1884] et est précisé dans [Hilbert, Hurwitz 1890].

La méthode des tangentes et sécantes fait son apparition, bien sûr, quand Poincaré passe aux courbes de genre 1.

"On voit avec quelle facilité se traite le cas des courbes unicursales. Passons maintenant aux courbes de genre 1 et d'abord aux plus simples d'entre elles, je veux dire aux cubiques.

Étudions d'abord la distribution des points rationnels sur ces courbes.

J'observe que la connaissance de deux points rationnels sur une cubique rationnelle suffit pour en faire connaître un troisième. En effet, la droite qui joint deux points rationnels donnés va couper la cubique en un troisième point qui, étant unique, est encore rationnel.

De même, si nous connaissons un point rationnel, nous pouvons en déduire un second; la tangente à la cubique en un point rationnel est une droite rationnelle qui coupe la cubique en un autre point rationnel." [Poincaré 1901, 490]

Pour voir ce que donne cette méthode il exprime les opérations en termes des *arguments elliptiques* des points rationnels. Ainsi il constate qu'en partant

[16] Cette notion est, bien sûr, un des fruits les plus importants du développement des mathématiques au dix-neuvième siècle. Faute d'en pouvoir dire plus ici, je renvoie sommairement à [Brill, Noether 1892/93] et à [Scholz 1980].

du point qui correspond au nombre complexe α, la méthode des tangentes et sécantes engendre précisément les points correspondant aux nombres de la forme $(3k+1).\alpha$, $k \in \mathbf{Z}$. Et en partant de plusieurs points il trouve :

"Plus généralement, si les points d'arguments elliptiques

$$\alpha,\ \alpha_1,\ \alpha_2,\ \ldots,\ \alpha_q$$

sont rationnels, il en est de même de tous les points dont les arguments elliptiques sont compris dans la formule

$$(1) \qquad \alpha + 3n\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \ldots + p_q(\alpha_q - \alpha),$$

où n et les p sont entiers." [Poincaré 1901, 492]

Nulle part, Poincaré n'essaie de combler les lacunes dans cette série : Il ne se demande pas si toutes les $\mathbf{Z}$-combinaisons linéaires des arguments des points de départ appartiennent à des points rationnels, et par quelle opération géométrique on peut les atteindre. Ceci malgré le fait qu'il sait très bien qu'"une cubique qui a un point rationnel est toujours équivalente à une cubique qui a un point d'inflexion rationnel." [Poincaré 1901, 538]

Poincaré n'atteint donc pas du tout le niveau de l'analyse de la méthode des tangentes et sécantes que nous avons vu dans Sylvester — et pourtant ses notations sont beaucoup plus suggestives, étant guidées par la paramétrisation analytique, que celles de Sylvester. En particulier, *Poincaré ne découvre pas la loi de groupe géométrique sur les points rationnels d'une cubique non-singulière.* Il ne dispose dans sa description ni d'un élément neutre ni de l'inverse, et l'opération binaire qu'il étudie n'est pas associative.

Comment s'est donc développée la *légende* selon laquelle Poincaré aurait "montré [Poincaré 1901] qu'...on peut introduire, dans l'ensemble des points rationnels de la courbe, l'opération d'addition, de manière que cet ensemble soit muni d'une structure de groupe abélien" [Bachmakova 1966, 294] ? Même Scriba qui est beaucoup plus soigneux[17] semble pris dans le piège de ne pas pouvoir nier une découverte de plus à un esprit aussi fécond que Poincaré. Ainsi il remarque bien que Poincaré associe le point d'argument $-\gamma = -(\alpha+\beta)$ aux points d'arguments α, β. Mais il fait comme si ceci n'avait pas d'importance.[18] Cette erreur, qu'on pardonnerait facilement à un mathématicien soucieux de trouver des sources d'inspiration, semble essentielle dans le travail d'un historien professionnel des mathématiques.

[17] A la fin de sa discussion de Fermat il souligne, "daß auch Fermat — wie Diophantos — nur algebraische Substitutionen und Transformationen ausführte. Wie stark er sich dabei vielleicht von geometrischen Bildern leiten ließ, wird nicht offenkundig." [Scriba 1984, 24]

Pour finir notre discussion de l'article de Poincaré, regardons le passage célèbre où il définit sa notion du rang d'une cubique, qui suit le dernier passage cité de [Poincaré 1901] :

"On peut se proposer de choisir les arguments

$$(2) \qquad \alpha,\ \alpha_1,\ \alpha_2,\ \ldots,\ \alpha_q,$$

de telle façon que la formule (1) comprenne tous les points rationnels de la cubique. Les $q+1$ points rationnels qui ont les arguments (2) forment alors ce que nous appelerons un *système de points rationnels fondamentaux.*

Il est clair que l'on peut choisir d'une infinité de manières le système des points rationnels fondamentaux. On doit tout d'abord, dans ce choix, s'arranger de telle façon que le nombre $q+1$ des points fondamentaux soit aussi petit que possible. Cette valeur minimum de ce nombre $q+1$ est ce que j'appelerai le *rang* de la cubique; c'est évidemment un élément très important de la classification des cubiques rationnelles." [Poincaré 1901, 492f]

Dans la mesure où Poincaré n'envisage point la situation où aucun nombre fini de points fondamentaux ne suffit à engendrer tous les points rationnels on peut voir dans ce texte une façon de conjecturer le théorème de la base finie des points rationnels, démontré dans [Mordell 1922].[19] Il est aussi possible que, étant intéressé par une analyse plutôt constructive des points rationnels, il ait exclu tout de suite le cas d'un rang infini.[20]

Comme Poincaré ne dispose ni d'un élément neutre ni de l'inverse dans sa structure, sa notion de rang n'est pas bien calibrée de notre point de vue. En fait, le rang n'est pas un invariant birationnel pour la raison triviale que, de

[18] "Da Poincaré ... das Integral .. mit entgegengesetztem Vorzeichen versah, ist γ durch $-\gamma$ zu ersetzen." [Scriba 1984, 36]

[19] *Cf.* la formulation du jeune A. Weil [Weil [1929], 47] : "Il y a quelques années, Mordell a démontré un théorème remarquable, qui avait été entrevu déjà par Poincaré ...."

[20] C'est E. Brieskorn qui me proposait cette interprétation dans une discussion.

deux cubiques équivalentes, une, mais pas l'autre, peut avoir un point rationnel d'inflexion.[21] Cet inconvénient allait être bientôt remarqué et corrigé par Beppo Levi dans [Levi 1906/08, 758f] — travail impressionnant auquel nous passons maintenant.

5. Beppo Levi (et Hurwitz)

Levi se place, avec [Levi 1906/08], consciemment dans la tradition de Sylvester et Poincaré, bien que ses informations sur Sylvester ne soient apparemment basées que sur les indications indirectes des *Nouvelles Annales* ; il ne cite pas le mémoire américain [Sylvester 1879/80].

Plus généralement et plus géométriquement que ses prédecesseurs, il commence par la définition [Levi 1906/08, 752f] selon laquelle

> "un punto razionale o un gruppo [*on dirait aujourd'hui :* ensemble] razionale di punti di una cubica a coefficienti razionali è dedotto razionalmente dai punti razionali $A_1, A_2, ..., A_r$ quando è univocamente determinato mediante intersezioni della cubica con curve a coefficienti razionali, completamente definiti dai punti $A_1, A_2, ..., A_r$ e dai valori (razionali) di un certo gruppo di coefficienti che vi compaiono come parametri; per assegnare questi parametri costringeremo generalmente la curva a passare per altrettanti punti razionali fissati arbitrarimente sul piano."

Mais il montre aussitôt, en faisant intervenir les paramètres analytiques, que cette notion *a priori* plus générale de la déduction rationnelle de points sur une cubique, se ramène à l'application itérée de la méthode des tangentes et sécantes.

En corrigeant la notion de *rang* comme nous l'avons vu, Levi s'approche de ce que nous appelons aujourd'hui le rang (libre) du groupe abélien des points rationnels.[22] Toutefois, il ignore les problèmes de la torsion : un groupe d'ordre 6, par exemple, admet comme ensemble de générateurs indépendants — "*tali che nessuno di essi possa dedursi razionalmente da altri*" [Levi 1906/08, 758] — soit un élément d'ordre 6, soit deux, d'ordres 2 et 3 respectivement : Le rang

[21] Il n'est donc pas étonnant que Poincaré ne démontre pas l'invariance birationnelle du rang, comme remarque Scriba [Scriba 1984, 36].

[22] [Levi 1906/08, 758f, en particulier la première formule p. 759]. Noter pourtant qu'il considère toutes les courbes dans une classe d'équivalence birationnelle à la fois.

de Levi n'est pas bien défini en général. Cette bavure peut surprendre[23] dans la mesure où ce que nous appelons la torsion dans le groupe des points rationnels, est le sujet principal de l'article [Levi 1906/08]. Mais il ne faut pas oublier que Levi est surtout un géomètre, dans la tradition italienne, et il voit ce que nous traitons prosaïquement comme les éléments d'ordre fini d'un groupe, comme des configurations finies de points sur une cubique[24] qui sont fermées par rapport aux tangentes et sécantes.[25]

C'est avec ce langage géométrique que Levi se lance dans l'exploration systématique de ce que nous appelons les sous-groupes de torsion qu'on peut rencontrer dans les groupes des points rationnels de courbes elliptiques sur $\mathbb{Q}$. Nous savons, bien sûr, qu'il n'y a que très peu de possibilités [Mazur 1978, Thm 2] : les groupes cycliques d'ordre 1,2, ..., 10,12, et les groupes isomorphes à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\nu\mathbb{Z}$, pour $\nu = 1, ..., 4$. Il est impressionnant de voir Levi se rapprocher de cette liste complète par des analyses détaillées des configurations finies sur les cubiques rationnelles.

Plus précisément, Levi discute essentiellement les configurations engendrées par un point d'ordre t dans le groupe des points rationnels. (Ses normalisations sont pourtant différentes; il part systématiquement d'un point de paramètre elliptique de la forme $\frac{\omega}{3t}$, où ω est une période : *voir* [Levi 1906/08, 101], ainsi que [Levi 1906/08, 676–680].) Ceci revient plus ou moins à traiter l'existence d'un sous-groupe cyclique d'ordre t du groupe des points rationnels.

Commençant par le cas $t = 2^\nu$, il trouve que de telles configurations existent sur certaines cubiques rationnelles, pour $\nu = 1, 2, 3$. Mais qu'il n'y en a pas pour $\nu = 4$. Levi démontre l'impossibilité du cas $t = 16$ — qui implique l'impossibilité

[23] Généralement, le travail de Levi me semble assez fiable. *Voir* les quelques remarques là-dessus au cours de ma discussion de Levi. — En particulier, je n'ai trouvé nulle part, ni dans [Levi 1906/08], ni dans [Levi 1909], la faute, concernant la forme normale d'une cubique ayant un point rationnel, dont Cassels accuse Levi [Cassels 1986, 33] : Chaque fois que Levi utilise l'équation dont Cassels remarque qu'elle n'est pas valable en général, il impose soigneusement une condition supplémentaire. La formulation malicieuse de Cassels, "Levi ... appears to claim ..." donne d'ailleurs l'impression *trompeuse* que les travaux de Levi sont rédigés de façon embrouillée. — Toutefois, je n'ai pas vérifié tous les détails des démonstrations de Levi cités plus loin.

[24] *Configurazioni arborescenti* et *Configurazioni poligonali (semplici* ou *misti)* [Levi 1906 /08, 101ff]. Quand il aborde le cas que nous décrivons comme $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$, il prend, bien sûr, un seul générateur comme base : [Levi 1906/08, 420]; *cf.* [Levi 1906/08, 681].

[25] Sylvester avait déjà souligné à plusieurs endroits l'éventualité que la méthode des tangentes et sécantes revienne sur elle même après un nombre fini d'opérations, en partant de certains points rationnels : [Sylvester 1879/80 : 314 (*), 340 (*), 351, 354].

d'une courbe elliptique sur $\mathbb{Q}$ avec un point rationnel d'ordre 16 — en déduisant d'abord une équation d'une courbe paramétrisant les cubiques admettant une telle configuration. Autrement dit, il déduit ce que nous reconnaissons comme un modèle de la courbe modulaire $X_1(16)$:

$$[y^2 =] \ \Delta = (c^2+1)(c-1)(c^3-c^2-3c-1)$$

[Levi 1906/08, 113], *cf.* [Washington 1990, dernier §]. Ensuite il montre par une descente infinie [Levi 1906/08, 113–115] qu'il n'y a pas de point rationnel sur cette "courbe modulaire" correspondant à une cubique non dégénérée admettant une configuration de points avec $t = 16$.[26]

Pour les petites valeurs impaires de t, Levi trouve des équations paramétrisant les familles ("*fascio*") des cubiques ayant un point rationnel d'ordre t. Mais dans le cas $t = 11$, il n'arrive pas à conclure [Levi 1906/08, 417ff]. Plus précisément, il écrit l'équation de la cubique paramétrisant les cubiques ayant un point rationnel d'ordre 11, *i.e.*, il écrit un modèle de la courbe que nous appelons aujourd'hui $X_1(11)$, [Levi 1906/08, no (7), p. 418] ; et il repère là-dessus les cinq points rationnels que nous reconnaissons comme étant les pointes de cette courbe modulaire.[27] Mais il n'arrive pas à démontrer que ce sont les seuls points rationnels.

Finalement, en traitant les 'configurations polygonales mixtes' — qui correspondent aux sous-groupes de la forme $\mathbf{Z}/2^\nu\mathbf{Z}\times\mathbf{Z}/t'\mathbf{Z}$ —, Levi démontre l'impossibilité sur $\mathbb{Q}$ du cas $\nu = 1$, $t' = 7$ et conjecture la même chose pour $\nu = 1$, $t' > 7$. Si $\nu = 2$, il montre que $t' = 3$ est possible, mais $t' = 5$ ne l'est pas. Il se résigne à ne pas aborder le cas $\nu = 3$: "questa recerca presenta notevoli difficoltà arithmetiche e noi l'abbandiamo per ora" [Levi 1906/08, 434].

Vu les résultats considérables de Levi, l'article de Hurwitz [Hurwitz 1917], qui aborde essentiellement les mêmes problèmes, mérite à peine d'être mentionné.

[26] R. Schoof a remarqué dans cet argument des lacunes que L. Washington m'a obligeamment communiquées : Levi a tendance à oublier des possibilités de signes variés dans les identités quadratiques. Ainsi, on pourrait aussi avoir $-q$ et $-r^2$ au lieu de q, r^2 dans [Levi 1906/08, 114, *l.* – 10], pourtant ceci ne ferait qu'échanger les rôles de p, q dans les équations qui suivent. De même, les omissions analogues [Levi 1906/08, 113, no (8)] et [Levi 1906/08, 115, *l.*5] sont facilement comblées.

[27] Je dois à R. Schoof l'observation que l'équation de Levi donne en fait un modèle de $X_1(11)$. (C'est même ce qu'on appelle aujourd'hui un modèle minimal sur $\mathbf{Z}$.) — Levi ignore, bien sûr, le contexte analytique des courbes modulaires qu'il étudie. Mais il repère les "pointes" comme étant les points rationnels correspondant à des cubiques dégénérées.

Hurwitz explique [Hurwitz 1917, 446, note 2] qu'il a eu connaissance des notes de Levi seulement après la rédaction de son article. Contrairement à Levi il ne démontre aucun théorème excluant l'existence de cubiques ayant certaines structures finies de points rationnels. Et ses résultats et démonstrations ne surpassent en rien ceux de Levi — exception faite peut-être de l'écriture lucide de la forme générale des "vollständigen Gruppen" (finis) de points rationnels [Hurwitz 1917, 451], et la facilité avec laquelle Hurwitz travaille sur des corps de nombres, par exemple [Hurwitz 1917, 458ff].

Toutefois, c'est l'exposé très clair de Hurwitz qui servit comme point d'appui au travail de M.I. Logsdon, [Logsdon 1925] — "une mathématicienne de Chicago"[28] dont le passage à Rome fit connaître à André Weil le mémoire de Mordell [Mordell 1922].

6. De Mordell à Weil

Le théorème de finitude démontré dans [Mordell 1922] s'exprime très bien sans référence à la notion de groupe abélien : "I shall now prove that if an ... equation .. [of genus one has] an infinite number of solutions, then the method of infinite descent applies, that is to say, all the solutions can be expressed rationally in terms of a finite number by means of the classic method," *i.e.*, par la méthode des tangentes et sécantes. [Mordell 1922, 108]

Mordell ne montre pas clairement si oui ou non il dispose de la notion de groupe abélien dans ce contexte. D'autre part, la présentation de la démonstration par André Weil dans le petit 'digest' [Weil [1929]] est parfaitement moderne. Il nous semble donc que la notion du groupe abélien a été définitivement introduite dans la théorie des points rationnels sur les cubiques (courbes elliptiques) seulement vers le milieu des années 1920. Weil était peut-être le premier auteur qui en faisait un usage systématique.

Nous ne discutons pas en détail l'article fondamental mais assez particulier de Mordell. Pour une analyse intéressante de l'arrangement de la démonstration de Mordell, *voir* [Cassels 1986]. De même nous passons sous silence la thèse de Weil et les travaux ultérieurs sur les courbes de genre supérieur, resp. leurs variétés jacobiennes.

La démonstration du théorème de Mordell (ainsi que de sa généralisation aux

[28] *Voir* [Weil [1917c], [1928]*, *524*].

variétés abéliennes sur les corps de nombres par Weil) se coupe naturellement en deux parties. D'abord on établit le 'théorème de Mordell(-Weil) faible'. Dans la formulation actuelle, celui-ci dit que le groupe quotient $\mathcal{C}(\mathbb{Q})/2.\mathcal{C}(\mathbb{Q})$ — plus généralement $\mathcal{C}(\mathbb{Q})/n.\mathcal{C}(\mathbb{Q})$, pour tout $n > 1$ — est un groupe fini. C'est un énoncé un peu lourd à exprimer en termes de la seule méthode des tangentes et sécantes. Ensuite il faut mesurer le comportement de la 'taille' des points rationnels quand on leur applique la méthode de la tangente — plus généralement, la multiplication par n. C'est aujourd'hui le début de la 'théorie des hauteurs'.[29]

Concluons ce rapport — sans doute préliminaire — sur la méthode des tangentes et sécantes par une réflexion générale. Le théorème de Mordell marque, par sa généralité, un point tournant dans l'histoire de ce domaine des mathématiques : c'est un énoncé fondamental qui vaut pour toutes les courbes elliptiques sur $\mathbb{Q}$. Traditionnellement, l'analyse diophantienne se pratiquait par bribes : équation par équation, descente par descente. C'est Poincaré qui a énoncé le programme pour sortir de cette industrie désœuvrée, et entamé l'étude systématique de l'arithmétique des courbes algébriques. Ce n'était pas la technique de démonstration qui manquait aux prédécesseurs de Mordell, c'était l'esprit théorique qui faisait défaut dans une branche mathématique qui allait à la dérive, avant son renouement avec le développement de la géométrie algébrique.

Le monde avec lenteur, arrive à la vertu.

Fr. Ancillon

Consid. sur la philos. de l'hist., Paris 1796

Manuscrit reçu le 20 décembre 1989
corrigé le 16 mai 1990

[29] Nous reconnaissons aujourd'hui des débuts de la notion de hauteur dans les démonstrations par descente infinie : *cf.* notre remarque (note 4 plus haut) sur la façon dont Fermat mesure la taille des triangles rectangles dans sa démonstration mentionnée au §1. Le mot "Höhe" apparaît dans ce contexte dans [Hurwitz 1917, 458].

Bibliographie

I. Bachmakova [1966], Diophante et Fermat, *Revue d'Histoire des Sciences et de leurs Applications* **19**, 289–306.

A. Brill, M. Noether [1892/93], Die Entwicklung der Theorie der algebraischen Functionen in älterer und neuerer Zeit, *Jber. DMV* **3** (issued 1894), 107–566.

J.W.S. Cassels [1973], Louis Joel Mordell 1888–1972 (Elected F.R.S. 1924), *Biographical Memoirs of Fellows of The Royal Society* **19**, December 1973, 493–520.

J.W.S. Cassels [1986], Mordell's finite basis theorem revisited, *Math. Proc. Camb. Phil. Soc.* **100**, 31–41.

A. Cauchy [1826], *Exercices de mathématiques (anciens exercices)*, année 1826, Paris (de Bure Frères).

A. Cauchy [1887], *Œuvres*, sér. 2, t. **6**, Paris (Gauthier-Villars).

A. Clebsch [1863], Über die Anwendung der Abelschen Functionen in der Geometrie, *J. reine angew. Math.* **63**, 189–243.

C.H. Clemens [1980], *A Scrapbook of Complex Curve Theory*; New York – London (Plenum).

J. Coates [1984], Elliptic Curves and Iwasawa Theory, *in :* R.A. Rankin (ed.), *Modular Forms [Proc. Durham Symp.* 1983], Horwood : Chichester; chapter 3 : 51–73.

A. Desboves [1879], Mémoire sur la résolution en nombres entiers de l'équation $aX^m + bY^m = cZ^n$; *Nouvelles Annales de Mathématiques*, $2^{ème}$ série, t. **18**; 265–279, 398–410, 433–444, 481–499.

A. Desboves [1886], Résolution, en nombres entiers et sous sa forme la plus générale, de l'équation cubique, homogène, à trois inconnues; *Nouvelles Annales de Mathématiques*, $3^{ème}$ série, t. **5**; 545–579.

J. Dieudonné [1974], *Cours de géométrie algébrique*, I : Aperçu historique sur le développement de la géométrie algébrique; Paris (PUF, Coll. SUP)

L.E. Dickson [1920], *History of the Theory of Numbers*, vol II : Diophantine Analysis, Washington (Carnegie Institute); reprint Bronx (Chelsea) 1971.

L. Euler [1912/13], *Opera Omnia (1)*, **20, 21**, Leipzig – Berlin

P. de Fermat [I – IV], *Œuvres*, publiées par P. Tannery et Ch. Henry; Paris

(Gauthier-Villars), 1891–1912.

C. Goldstein [1990], *Descentes infinies au XVIIème siècle : une comparaison de Fermat et Frénicle de Bessy, prépublication.*

C. Goldstein et N. Schappacher [1990], *On the history of infinite descent : a research project, preprint.*

T.L. Heath [1910], *Diophantus of Alexandria — A Study in the History of Greek Algebra*, with a Supplement Containing an Account of Fermat's Theorems and Problems Connected with Diophantine Analysis and some Solutions of Diophantine Problems by Euler, 2nd edition, Cambridge.

T.L. Heath [1956], *Euclid's Elements*, with introduction and commentary; three volumes, reprinting of 2nd edition, New York (Dover).

D. Hilbert & A. Hurwitz [1890], Über die diophantischen Gleichungen vom Geschlecht Null; *Acta Mathematica* **14**, 217–224 = Hilbert, *Gesammelte Abhandlungen II*, 258–263 = Hurwitz, *Math. Werke II*, 116–121.

A. Hurwitz [1917], Über ternäre diophantische Gleichungen dritten Grades; *Vierteljahresschrift der Naturforschenden Gesellschaft in Zürich*, **62**, 207–229 = *Math. Werke II*, 446–468.

C.G.J. Jacobi [1835], De usu theoriæ integralium ellipticorum et integralium abelianorum in analysi diophantea, *Journal reine angew. Math.* **13**, 353–355.

E. de Jonquières [1878], Décomposition du carré d'un nombre N et de ce nombre lui-même en sommes quadratiques de la forme x^2+ty^2, t étant un nombre rationnel, positif ou négatif; résolution en nombres entiers du système des équations indéterminées $y = x^2 + t(x+\alpha)^2$, $y^2 = z^2 + t(z+\beta)^2$; *Nouvelles Annales de Mathématiques*, $2^{ème}$ série, t. **17**, 419–424, 433–446.

F. Klein [1926/1927], *Vorlesungen über die Entwicklung der Mathematik im 19. Jahrhundert*, Berlin (Springer); Teil I 1926, Teil II 1927.

N. Koblitz [1984], *Introduction to Elliptic Curves and Modular Forms*, Springer GTM **97** : New York etc.

J.L. de Lagrange [1777], Sur quelques problèmes de l'analyse de Diophante; *in : Œuvres*, publ. par J.-A. Serret, vol. IV, Paris (Gauthier-Villars) 1869 [Nachdruck Hildesheim/New York (Olms) 1973], 377–398.

B. Levi [1906/08], Saggio per una teoria aritmetica delle forme cubiche ternarie,

Atti Accad. Reale delle Scienze Torino, I : **41** (1906) 739–764, II–IV : **43** (1908) 99–120, 413–434, 672–681.

B. Levi [1909], Sull'equazione indeterminata del 3° ordine, *Atti IV Congresso Mat.*, Roma 1909, vol. II, 173–177.

M.I. Logsdon [1925], Complete groups of points on a plane cubic curve of genus one, *Transactions AMS* **27**, 474–490.

E. Lucas [1877], Recherches sur plusieurs ouvrages de Léonard de Pise et sur diverses questions d'arithmétique supérieure, *Bulletino di Bibliografia e di Storia delle Scienze Matematiche e Fisiche* **10**, 129–193, 239–293.

E. Lucas [1878], Sur l'analyse indéterminée du troisième degré et sur la question 802 (Sylvester); *Nouvelles Annales de Mathématiques*, $2^{ème}$ série, t. **17**, 507–514.

B. Mazur [1978], Rational Isogenies of prime degree, *Inventiones Math.* **44** (1978), 129–162.

L.J. Mordell [1921], *Three Lectures on Fermat's Last Theorem*, Cambridge Univ. Press.

L.J. Mordell [1922], On the Rational Solutions of the Indeterminate Equations of the Third and Fourth Degrees; *Proceedings of the Cambridge Philosophical Society* **XXI** (1922/23), p. 179–192.

L.J. Mordell [1947], *A Chapter in the Theory of Numbers. An Inaugural Lecture*; Cambridge Univ. Press.

L.J. Mordell [1972], *Two Papers on Number Theory*, mit einem Vorwort von O. Neumann; réédition de Mordell [1921] et Mordell [1947], Berlin, GDR (VEB Deutscher Verlag d. Wiss.).

I. Newton [1971], *The Mathematical Papers* of Isaac Newton, vol. IV, ed. D.T. Whiteside, Cambridge.

M. Noether [1871], Über Flächen, welche Schaaren rationaler Kurven besitzen, *Math. Annalen* **3**, 161–227.

M. Noether [1884], Rationale Ausführung der Operationen in der Theorie der algebraischen Funktionen, *Math. Annalen* **23**, 311–358.

H. Poincaré [1901], Sur les propriétés arithmétiques des courbes algébriques, *Journal de Mathématiques*, $5^{ème}$ série, t. **7**, fasc. III, 1901, 161–233) = *Œuvres* **V**, 483–550.

G. Salmon [1879], *A Treatise on the Higher Plane Curves* : intended as a

sequel to *A Treatise on Conic Sections*; troisième édition (*cité d'après la reproduction photographique par* G.E. Stechert, New York 1934).

N. Schappacher [1989], Neuere Forschungsergebnisse in der Arithmetik elliptischer Kurven; *Didaktik der Mathematik* **17** (1989), 149–158

E. Scholz [1980], *Geschichte des Mannigfaltigkeitsbegriffs von Riemann bis Poincaré, Boston*, etc. (Birkhäuser)

C. Scriba [1984], Zur Geschichte der Bestimmung rationaler Punkte auf elliptischen Kurven — Das Problem von Behā-Eddin 'Amūlī; *Ber. a.d. Sitzungen d. Joachim Jungius-Gesellschaft der Wissenschaften e.V. Hamburg*, **1** (1982/83), Heft 6, Göttingen (Vandenhoeck & Ruprecht).

J.H. Silverman [1986], *The Arithmetic of Elliptic Curves*, Springer GTM **106** : New York etc.

J.J. Sylvester [1858], Note on the algebraic theory of derivative points of curves of the third degree; *Philosophical Magazine* **XVI**, 116–119 = *Mathematical Papers* II, 107–109.

J.J. Sylvester [1879/80], On certain ternary cubic-form equations; *American Journal Math.* **2** (1879), 280–285, 357–393; **3** (1880), 58–88, 179–189 = *Mathematical Papers* III, 312–391.

L.C. Washington [1990], A family of cyclic quartic fields arising from modular curves, prépublication.

A. Weil [1983], *Number Theory. An approach through history. From Hammurapi to Legendre*; Boston, etc. (Birkhäuser)

A. Weil [19**], *d'autres travaux de Weil sont cités selon la nomenclature dans l'édition de ses Œuvres scientifiques, Collected Papers*, Volume I, Springer 1979.

Zeuthen [1903], *Geschichte der Mathematik im XVI. und XVII. Jahrhundert*, Leipzig (Teubner).

Norbert Schappacher
Max-Planck-Institut für Mathematik
Gottfried-Claren-Str. 26
D-5300 Bonn 3

Séminaire de Théorie des Nombres
Paris 1988–89

The structure of the minus class groups of abelian number fields

René SCHOOF*

Abstract. It is shown that sometimes one can read off the structure of the minus class groups of abelian number fields from certain Stickelberger elements; the question is raised whether one can always determine the structure of these class groups from Stickelberger elements. Some numerical and theoretical evidence for an affirmative answer is presented.

1. — Introduction

Ideal class groups of cyclotomic or abelian number fields have been a subject of study for a long time [5,14]. The problem naturally falls apart in two. The class groups of real abelian number field are still relatively poorly understood. But about the other parts, the minus parts of the class groups of imaginary abelian number fields, much more is known. For an imaginary abelian number field K the minus class group Cl_K^- of K is defined to be $Cl_K/\mathrm{im}(Cl_{K^+})$ where K^+ is the maximal real subfield of K. The analytic class number formula gives an expression for the cardinality of Cl_K^- in terms of certain generalized Bernoulli numbers which are defined in terms of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}^{\mathrm{ab}}/\mathbb{Q})$. This formula is quite practical and can be used to compute the cardinalities of minus class groups of abelian fields of small conductor, see [7,12,16]. More precise results were recently obtained by B. Mazur and A. Wiles [9]. They took the action of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ into account. They obtained formulas for the cardinalities of certain eigenspaces for this action. Apart from their results there does not appear to be a general way to describe the structure of the minus class groups as abelian groups in similar terms. For instance, in the case of a complex quadratic field K, there does not seem to be a way to tell, in terms of