La méthode de Chabauty et Coleman

Nicolas Mascot

Table des matières

Introduction

Notre but est la résolution de certaines équations diophantiennes. Plus précisément, étant donné un corps de nombres[1] K, et un polynôme $f \in K[x, y]$ à deux indéterminées et à coefficients dans K, nous voudrions pouvoir trouver toutes les solutions dans K^2 de l'équation

$$f(x, y) = 0.$$

Ce problème peut se reformuler géométriquement : il s'agit se trouver tous les points à coordonnées dans K de la courbe plane d'équation $f(x, y) = 0$. C'est ainsi que nous sommes amenés à utiliser la géométrie algébrique.

1 Variétés algébriques

Fixons un corps parfait[2] K. On appellera *variété algébrique affine* sur K le lieu des zéros communs d'une famille de polynômes $f_i \in K[x_1, \cdots, x_n]$ dans K^n. Il est naturel d'associer à cette variété son *anneau de fonctions*[3] *régulières*

$$K[x_1, \cdots, x_n]/(f_i).$$

La philosophie de la géométrie algébrique est essentiellement d'étudier cet anneau, plutôt que la variété elle-même. Ceci est légitimé par le fait que l'on puisse récupérer les points de la variété à partir de cet anneau : les "points" sont les idéaux maximaux de l'anneau des fonctions régulières. Il faut remarquer que ceci ne donne pas seulement les points à coordonnées dans K, mais aussi automatiquement ceux à coordonnés dans les extensions finies de K — plus précisément, ceci donne les orbites de points à coordonnées dans $\overline{\mathbb{Q}}$ sous l'action du groupe de Galois $\mathrm{Gal}(\overline{K}, K)$.

Par exemple, prenons des équations à une seule variable ($n = 1$), et considérons la variété donnée par la famille vide d'équations : il s'agit tout simplement de la droite affine sur K. Son anneau de fonctions régulières est

1. Rappelons qu'on appelle *corps de nombres* les extensions finies du corps $\mathbb{Q}$ des nombres rationnels, telles que $\mathbb{Q}$ lui-même, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(i)$, etc.

2. En pratique, K sera un corps de nombres, ou plus rarement un corps parfait.

3. Puisque nous faisons de la géométrie *algébrique*, les seuls fonctions que nous nous autorisons à considérer sont les polynômes, ou éventuellement les fractions rationnelles.

$K[x]$; les points de notre droite affine correspondent donc aux polynômes irréductibles unitaires sur K. Ainsi, le point $a \in K$ correspond au polynôme $x - a$. Si $K = \mathbb{Q}$, les points $\sqrt{2}$ et $-\sqrt{2}$ sont indiscernables, et correspondent au polynôme $x^2 - 2$.

Si X est une variété, on notera $X(L)$ l'ensemble de ses points à coordonnées dans L pour toute extension algébrique L de K. Les éléments de $X(K)$ seront dits *points rationnels*, plus généralement, on parle de points L-rationnels pour désigner les éléments de $X(L)$.

Nous supposerons dans la suite que notre variété est *réduite* , c'est-à-dire que anneau des fonctions régulières $K[x_1, \cdots, x_n]/(f_i)$ n'a pas de nilpotents non nuls [4]. Nous dirons que notre variété est *irréductible* s'il n'est pas possible de la décomposer non trivialement en l'union de deux sous-variétés. Ceci correspond à demander que l'anneau des fonctions régulières $K[x_1, \cdots, x_n]/(f_i)$ soit *intègre* ; on appelle alors *fonctions rationnelles* les éléments de son corps des fractions.

La notion intuitive de *dimension* d'une variété se formalise en considérant la longueur maximale de chaînes strictement croissantes de sous-variétés irréductibles. Par exemple, une "surface" est de dimension 2 car les chaînes maximales sont de forme

$$\begin{array}{ccccc} \text{point} & \subsetneq & \text{courbe} & \subsetneq & \text{surface.} \\ 0 & & 1 & & 2 \end{array}$$

En particulier, on appelle *courbes* les variétés de dimension 1, et *surfaces* les variétés de dimension 2.

Il n'est guère plus difficile de définir de même les variétés algébriques *projectives* comme les lieux des zéros communs dans un espace projectif de polynômes *homogènes*. Dans la suite, nous ne nous intéresserons qu'aux variétés projectives, car elles possèdent de meilleures propriétés.

4. Cette restriction n'est guère contraignante ; en effet, si la variété n'est pas réduite, c'est qu'on a "mal" choisi son équation, par exemple en prenant $(y^2 - x^3 - 1)^2 = 0$ au lieu de $y^2 - x^3 - 1 = 0$. Pour "réduire" une telle variété, il suffit alors de remplacer l'idéal (f_i) par son radical.

2 Variétés abéliennes

Les *variétés abéliennes* sont un type particulièrement intéressant de variétés. Il s'agit de variétés algébriques projectives munies en outre d'une structure de groupe dont la loi est définie par des fonctions rationnelles. Bien que ce ne soit pas du tout évident, on démontre que le groupe obtenu ainsi est toujours abélien, ce qui justifie cette appellation.

L'exemple le plus célèbre de variétés abéliennes est celui des *courbes elliptiques*, dont la loi de groupe est définie par le fameux procédé des "tangentes et cordes".

Le théorème essentiel concernant les variétés abéliennes est dû à Mordell et à Weil ; il dit que le groupe des points rationnels d'une variété abélienne définie sur un corps de nombres est de type fini. Par exemple, dans le cas des courbes elliptiques, ceci nous dit qu'il est possible d'atteindre *tous* les points rationnels par le procédé "tangentes et cordes" à partir d'un nombre *fini* de points.

En tant que groupe de type fini, le groupe d'une variété abélienne est isomorphe à

$$\mathbb{Z}^r \times (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_i\mathbb{Z});$$

l'entier r s'appelle le *rang* de la variété abélienne.

Ce théorème se démontre en construisant une fonction *hauteur* sur les points, qui mesure la complexité arithmétique des points, et qui est telle qu'il n'y ait qu'un nombre fini de points de hauteur bornée. Pour plus de détails, le lecteur est invité à consulter [HS00]. Notons aussi que le concept de hauteur, conjugué à la structure de groupe, permettent en général de calculer [5] algorithmiquement l'ensemble des points rationnels d'une variété abélienne — en tout cas bien plus facilement que pour une variété quelconque.

3 Genre d'une courbe

Revenons au problème initial, à savoir les équations diophantiennes. Il s'agit de trouver les points rationnels d'une courbe plane. On s'imagine bien que ce problème est d'autant plus difficile que le degré du polynôme

5. On se contente en général de trouver des générateurs de la composante sans torsion $\mathbb{Z}^r$, ce qui est plus facile, et aussi souvent suffisant en pratique.

définissant la courbe est élevé. Toutefois, cette classification souffre de graves lacunes ; ainsi, les équations $y^2 = x^5 + x^4$ et $y^2 = x^5 + x$, bien qu'apparemment semblables, ont des comportements très différents puisque la première à une infinité de solutions dans $\mathbb{Q}^2$, tandis que la seconde n'a qu'on nombre fini de solutions sur n'importe quel corps de nombres. Ceci nous motive à introduire un autre invariant, le *genre* d'une courbe, qui mesure beaucoup plus fidèlement la difficulté et le comportement du problème.

Pour ce faire, poursuivons l'idée selon laquelle une courbe s'étudie mieux à travers ses fonctions, et interrogeons-nous quant à l'existence de fonctions rationnelles dont les zéros et les pôles sont prescrits. Bien entendu, parler de fonctions rationnelles implique qu'on se restreint au cas des courbes *irréductibles* ; on se restreint en fait aux courbes *absolument irréductibles*, c'est-à-dire qui restent irréductibles même si on les voit sur la clôture algébrique du corps de base. On montre que les seules fonctions sans pôles ni zéros sur une courbe projective absolument irréductible sont les constantes.

De plus, nous supposerons dorénavant que toutes les courbes que nous étudierons sont *non singulières*, ce qui signifie que l'équation qui les définit et le gradient de celle-ci ne s'annulent jamais simultanément sur la clôture algébrique du corps de base [6].

On appelle *diviseur* sur la courbe X toute combinaison linéaire formelle

$$D = \sum_{P \in X} n_P P$$

de points de X, où les n_P sont des entiers relatifs, tous nuls sauf un nombre fini. Un diviseur est dit *effectif* si les n_P sont tous positifs ou nuls, et on note alors $D \geqslant 0$. Les diviseurs sur X forment de manière évidente un groupe abélien.

Étant donnée une fonction rationnelle f non nulle sur X, on définit son *diviseur* par la formule

$$\operatorname{div}(f) = \sum_{P \in X} \operatorname{ord}_P(f) P,$$

où $\operatorname{ord}_P(f)$ dénote l'ordre d'annulation de la fonction f au point P (positif si f a un zéro, négatif si f a un pôle). Les diviseurs ainsi obtenus s'appellent les *diviseurs principaux* ; ils forment un sous-groupe du groupe des diviseurs

6. On aura reconnu une ressemblance avec la notion de sous-variété différentielle définie par une équation implicite.

puisque $\mathrm{div}(f) + \mathrm{div}(g) = \mathrm{div}(fg)$. On appelle *groupe de Picard* de X le quotient $\mathrm{Pic}(X)$ du groupe des diviseurs pas le sous-groupe des diviseurs principaux [7]. Ce groupe mesure donc à quel point il existe des diviseurs non principaux sur X.

On définit le *degré* d'un point de la courbe comme étant le degré de l'extension du corps de base K par les coordonnées du point [8], ainsi, les points rationnels sont exactement les points de degré 1. On prolonge cette notion aux diviseurs par linéarité, en posant

$$\deg\left(\sum_{P\in X} n_P P\right) = \sum_{P\in X} n_p \deg(P).$$

On montre que sur une courbe *projective*, une fonction rationnelle a autant de zéros que de pôles, autrement dit, que le degré d'un diviseur principal est nul. Par conséquent, le groupe de Picard $\mathrm{Pic}(X)$ contient toujours au moins $\mathbb{Z}$, et il est plus intéressant d'étudier le sous-quotient $\mathrm{Pic}^0(X)$ des diviseurs de degré nul par les diviseurs principaux.

Notons $K(X)$ le corps des fonctions rationnelles sur X, et pour tout diviseur D, posons

$$L(D) = \{f \in K(X)^* \mid \mathrm{div}(f) + D \geqslant 0\} \cup \{0\}.$$

$L(D)$ est clairement un K-espace vectoriel, et on montre qu'il est de dimension finie ; notons $l(D)$ sa dimension.

Si D et D' représentent la même classe dans $\mathrm{Pic}(X)$, mettons $D' = D + \mathrm{div}(f)$, alors la multiplication par f induit un isomorphisme de $L(D')$ vers $L(D)$; on peut donc parler du l (et aussi du degré) d'un élément de $\mathrm{Pic}(X)$.

Le célèbre théorème de Riemann-Roch s'énonce alors ainsi : il existe une classe $C \in \mathrm{Pic}(X)$, dite *classe canonique*, telle que pour tout diviseur D, on

7. On aura reconnu l'analogie parfaite avec le groupe des classes en théorie algébrique des nombres. En fait, la théorie des schémas permet de faire de la géométrie beaucoup plus abstraite en remplaçant l'anneau des fonctions régulières par un anneau commutatif quelconque ; en particulier, si on choisit l'anneau des entiers d'un corps de nombres, on obtient une "courbe" abstraite, c'est-à-dire un schéma de dimension 1, dont le groupe de Picard est le groupe des classes du corps de nombres. La notion de groupe de Picard généralise donc celle de groupe des classes.

8. Si on travaille avec des coordonnées projectives, ceci signifie qu'on déshomogénéise les coordonnées projectives en forçant l'une d'entre elles à valoir 1, puis qu'on prend le corps engendré par les coordonnées obtenues.

ait

$$l(D) = \deg(D) + 1 - g + l(C - D),$$

où on a posé $g = l(C)$; de plus, si le corps de base K est parfait, on peut montrer que la classe canonique est celle du diviseur du coefficient de n'importe quelle 1-forme différentielle sur X. Ce théorème répond donc complètement au problème d'existence de fonctions rationnelles de diviseur prescrit. Il se démontre naturellement avec de la cohomologie des faisceaux, comme on peut le vérifier dans [Har77]. Notons au passage qu'en l'appliquant à $D \in C$, on trouve que le degré de la classe canonique est $2g - 2$.

L'entier g que nous venons d'introduire est un invariant extrêmement important de la courbe X, qu'on appelle *genre* de la courbe [9]. C'est lui l'invariant mesurant la complexité de la courbe que nous avions annoncé. Par exemple, on montre à l'aide du théorème de Riemann-Roch que les courbes de genre 0 sont grosso modo isomorphes [10] à la droite projective, et que les courbes de genre 1 sont isomorphes à des cubiques projectives.

Un théorème extrêmement puissant, conjecturé en 1922 par Mordell mais démontré seulement en 1983 par Faltings, affirme qu'une courbe de genre $g \geqslant 2$ sur un corps de nombres n'a qu'on nombre fini de points rationnels. Ceci est un contraste frappant avec le cas des courbes elliptiques (qui, rappelons-le, sont de genre 1 en tant que cubiques projectives), puisque celles-ci sont des variétés abéliennes de rang en général non nul, donc qui ont en général un nombre infini de points rationnels. Une démonstration du théorème de Faltings est disponible dans [HS00].

Ceci explique la différence de comportement relevée au début de cette section entre $y^2 = x^5 + x^4$ et $y^2 = x^5 + x$: la première est de genre 0, tandis que la seconde est de genre 2.

L'inconvénient majeur de la preuve de Faltings est qu'elle n'est pas du tout effective ; en fait, elle ne donne même pas de borne raisonnable sur le nombre de points rationnels de la courbe, ni sur la "complexité" [11] de leurs

9. En vue de la remarque ci-dessus, le genre est donc la dimension de l'espace des 1-formes différentielles sans pôles sur la courbe.

10. Pour être précis, il s'agit de birationalité.

11. Par exemple, si on est sur $K = \mathbb{Q}$, on souhaiterait une borne sur la taille des numérateurs et des dénominateurs des coordonnées des points rationnels. Cette notion de "complexité" est formalisée par la notion de *hauteur* d'un point.

coordonnées. Par la suite, nous allons tenter de remédier à cette situation. Notre problème est donc le suivant : Étant donnée une courbe X de genre supérieur ou égal à 2 sur un corps de nombres K, calculer $X(K)$. On constate en fait empiriquement que si le genre n'est pas trop grand, une recherche naïve fournit une liste de points rationnels très souvent complète [12] ; notre objectif est donc la recherche d'une méthode permettant de prouver que la liste obtenue est effectivement complète.

4 Jacobienne d'une courbe

Comme nous l'avons vu, la structure de groupe d'une variété abélienne aide grandement à déterminer ses points rationnels. L'idée de la méthode de Chabauty va être de plonger notre courbe de genre supérieur ou égal à 2 dans une variété abélienne, puis de trier les points rationnels de cette variété abélienne pour ne garder que ceux qui sont sur la courbe. C'est ici qu'intervient la notion de *jacobienne* d'une courbe.

On démontre en effet que pour toute courbe projective absolument irréductible non singulière X de genre $g \geqslant 1$ sur un corps K admettant au moins un point rationnel [13] O, il existe une variété abélienne J_X sur K, dite *jacobienne de la courbe* X, qui est de dimension g et munie d'un plongement $j : X \hookrightarrow J_X$, défini sur K, et qui, étendu par linéarité au groupe des diviseurs de X, induit un isomorphisme [14] entre $\mathrm{Pic}^0(X)$ et $J_X(K)$. La jacobienne d'une courbe est donc unique à isomorphisme près.

Par exemple, les courbes elliptiques sont de genre 1, donc leur jacobienne est aussi une courbe. En fait, les courbes elliptiques sont leurs propres jacobiennes ; en effet, une analyse du procédé définissant la loi de groupe d'une courbe elliptique révèle que si P, Q et R sont trois points rationnels sur une

12. Là encore, la situation est très différente entre le genre 1 et le genre supérieur ou égal à 2 : on trouve en effet des courbes elliptiques sur $\mathbb{Q}$ d'équations raisonnables mais dont tous les points sans torsion — les points de torsion d'une courbe elliptique sont toujours à coordonnées entières — ont des coordonnées monstrueuses.

13. Si toutefois X n'avait aucun point rationnel, on peut tout de même construire sa jacobienne en remplaçant le corps de base K par une extension L telle que X admette un point L-rationnel. La jacobienne ainsi obtenue est alors toujours définie sur K, mais l'injection j risque de n'être définie que sur L.

14. En langage savant, la jacobienne représente donc le foncteur qui va des extensions L de K telles que X admette un point L-rationnel vers les groupes abéliens, et qui à L associe le groupe $\mathrm{Pic}^0(X_L)$; voir [Liu02], theorem 7.4.39.

telle courbe, alors $P+Q=R$ si et seulement les diviseurs $P+Q$ et $R+O$ représentent la même classe dans le groupe de Picard de la courbe, où O est le point "élément neutre" ; la loi de groupe de la courbe elliptique provient donc en quelque sorte de la loi de son groupe de Picard.

Plus généralement, une fois fixé un isomorphisme entre $\mathrm{Pic}^0(X)$ et $J_X(K)$, le plongement j induit sur les points rationnels une injection

$$\begin{array}{ccc} X(K) & \hookrightarrow & \mathrm{Pic}^0(X) \simeq J_X(K) \\ P & \mapsto & \text{classe de } P-O \end{array} .$$

Dans le cas des courbes elliptiques, on retrouve ainsi la formule précédente.

Revenons à nos moutons : soit X une courbe de genre $g \geqslant 2$ définie sur un corps de nombres K, et soit $J=J_X$ sa jacobienne. Nous avons donc un plongement $j : X \hookrightarrow J$ défini sur le corps de base K, ce qui permet au passage de représenter les points de J comme des combinaisons linéaires formelles de points de X et ainsi d'éviter l'utilisation d'équations explicites de J, ce qui est algorithmiquement préférable. Puisque J est abélienne, on doit pouvoir calculer $J(K)$, et il nous faut trouver quels points de $J(K)$ sont sur X.

Voyons maintenant, suivant Chabauty, comment ces idées pourraient servir à démontrer le théorème de Faltings. Prenons $K=\mathbb{Q}$ pour simplifier. Soit $J_{\mathbb{R}}$ la variété abélienne sur $\mathbb{R}$ définie par les équations définissant J, mais vues comme des équations à coefficients dans [15] $\mathbb{R}$. L'ensemble des points $J_{\mathbb{R}}(\mathbb{R})$ est alors un groupe de Lie analytique réel compact. Essayons d'analyser géométriquement la situation. L'adhérence de $J(\mathbb{Q})$ dans $J_{\mathbb{R}}(\mathbb{R})$ est un sous-groupe de ce dernier ; s'il est de dimension strictement inférieure à celle de $J_{\mathbb{R}}(\mathbb{R})$, il sera alors "mince" dans $J_{\mathbb{R}}(\mathbb{R})$, et il semble alors plausible qu'il ne rencontre alors la courbe $X(\mathbb{R})$ qu'en un nombre localement fini de points, donc fini puisque $J_{\mathbb{R}}(\mathbb{R})$ est compact. Ainsi $X(\mathbb{R}) \cap \overline{J(\mathbb{Q})}$ serait fini, donc *a fortiori* $X(\mathbb{Q})$ aussi. De plus, en analysant les intersections, on devrait pouvoir majorer son cardinal.

Malheureusement, une conjecture de Mazur prédit que $\overline{J(\mathbb{Q})}$ est souvent [16] ouvert dans $J_{\mathbb{R}}(\mathbb{R})$, ce qui ruine nos espoirs. Il faudrait en fait remplacer $\mathbb{R}$ par autre chose...

15. En géométrie algébrique, on appelle *changement de base* ce procédé d'"extension des scalaires".

16. Cette conjecture de Mazur dit que $\overline{J(\mathbb{Q})}$ est ouvert dans $J_{\mathbb{R}}(\mathbb{R})$ si $J(\mathbb{Q})$ est Zariski-dense dans J, ce qui est souvent le cas.

5 Nombres p-adiques

La notion de norme sur un espace vectoriel réel ou complexe est bien connue. Son analogue pour les corps est la notion de *valeur absolue* : il s'agit d'applications $|\cdot|$ allant du corps vers $\mathbb{R}^+$, et telles que, pour tous x et y éléments du corps,

- $|x| = 0 \iff x = 0$,
- $|x \times y| = |x| \times |y|$,
- $|x + y| \leqslant |x| + |y|$.

De la même manière qu'une norme sur un espace vectoriel, une valeur absolue sur un corps munit celui-ci d'une topologie compatible avec les lois de composition. On dit que deux valeurs absolues sur un même corps sont *équivalentes* si elles induisent la même topologie sur ce corps.

Par exemple, un théorème d'Ostrowski, démontré dans [Kob84], affirme qu'à équivalence près, les valeurs absolues sur le corps $\mathbb{Q}$ sont la valeur absolue usuelle, ainsi qu'une *valeur absolue p-adique* $|\cdot|_p$ pour chaque nombre premier p, définie par

$$\left|\frac{a}{b}\right|_p = p^{\mathrm{ord}_p(b)-\mathrm{ord}_p(a)} \ (a, b \in \mathbb{Z}^*), \quad |0|_p = 0,$$

où $\mathrm{ord}_p(a)$ désigne l'exposant auquel p apparaît dans la décompositions de a en facteurs premiers.

La topologie induite sur $\mathbb{Q}$ par $|\cdot|_p$ est très différente de la topologie usuelle ; ainsi, deux entiers sont d'autant plus proches pour cette topologie que leur différence est divisible par une grande puissance de p. On note $\mathbb{Q}_p$ le complété de $\mathbb{Q}$ pour cette topologie, c'est donc l'analogue p-adique de $\mathbb{R}$, et comme $\mathbb{R}$, c'est un corps ; intuitivement, ses éléments s'écrivent en base p avec un nombre fini de décimales, mais un nombre potentiellement infini de chiffres vers la gauche, alors qu'un réel s'écrit avec un nombre fini de chiffres à gauche et un nombre potentiellement infini de décimales. Pour un aperçu des propriétés de $\mathbb{Q}_p$, le lecteur est invité à consulter [Kob84].

Dans la suite, l'idée va donc être de remplacer $\mathbb{R}$ par un $\mathbb{Q}_p$. Plus généralement, si on travaille avec un corps de nombres K quelconque plutôt que $\mathbb{Q}$, on remplacera sa complétion usuelle $\mathbb{R}$ ou $\mathbb{C}$ par une complétion p-adique $K_\mathfrak{p}$ qui se construit de manière similaire à $\mathbb{Q}_p$; on remplace le nombre premier p

par un idéal premier $\mathfrak{p}$ de l'anneau des entiers de K, on construit la valeur absolue $\mathfrak{p}$-adique comme pour $|\cdot|_p$, et on complète [17].

6 La méthode de Chabauty

Comme précédemment, notons $J_{K_\mathfrak{p}}$ la variété sur $K_\mathfrak{p}$ définie par les mêmes équations que J ; $J_{K_\mathfrak{p}}(K_\mathfrak{p})$ est alors un groupe de Lie p-adique analytique. Notons $H^0(J_{K_\mathfrak{p}}, \Omega^1)$ l'espace des 1-formes différentielles sans pôles sur $J_{K_\mathfrak{p}}$. On montre que c'est un $K_\mathfrak{p}$-espace vectoriel de dimension g [18], et que, étant donnée une 1-forme ω, il est possible de l'intégrer, c'est-à-dire de définir une application

$$\begin{array}{rcl} J_{K_\mathfrak{p}}(K_\mathfrak{p}) & \longrightarrow & K_\mathfrak{p} \\ P & \longmapsto & \displaystyle\int_0^P \omega \end{array},$$

d'où un morphisme ϕ de $J_{K_\mathfrak{p}}(K_\mathfrak{p})$ dans $H^0(J_{K_\mathfrak{p}}, \Omega^1)^*$, qui est un difféomorphisme local.

L'adhérence de $J(K)$ dans $J_{K_\mathfrak{p}}(K_\mathfrak{p})$ est un sous-groupe de Lie de celui-ci, de dimension

$$\dim \overline{J(K)} = \dim \phi\big(\overline{J(K)}\big) = \dim \overline{\phi\big(J(K)\big)}$$

car ϕ est un difféomorphisme local. Or l'adhérence p-adique d'un sous-groupe de ${K_\mathfrak{p}}^g$ est le sous-groupe qu'il engendre sur $\mathbb{Z}_p$ — et c'est ça qui fait que ce qui ne marchait pas sur $\mathbb{R}$ marche en p-adique ! — donc, dans ce cas précis,

$$= \dim \big(\mathbb{Z}_p \phi(J(K))\big) = \mathrm{rg}_{\mathbb{Z}_p} \big(\mathbb{Z}_p \phi\big(J(K)\big)\big) \leqslant \mathrm{rg}_{\mathbb{Z}}\, \phi\big(J(K)\big) \leqslant \mathrm{rg}_{\mathbb{Z}}\, J(K).$$

Ainsi, le sous-groupe $\overline{J(K)}$ est de dimension au plus le rang de la jacobienne J de X. Par conséquent, si ce rang est inférieur au genre de X, alors nous sommes dans une situation très favorable. Et en effet, Chabauty a démontré dans [Cha41] que si le rang de la jacobienne de X est strictement inférieur au genre de X, alors $X(K)$ est fini. Il faut noter que ce résultat, qui date de 1941, était à l'époque la seule avancée significative vers ce qui était alors la conjecture de Mordell, qui ne serait démontrée que plus de 40 ans plus tard par Faltings.

17. Les complétés obtenus sont les facteurs de la $\mathbb{Q}_p$-algèbre étale $K \underset{\mathbb{Q}}{\otimes} \mathbb{Q}_p \simeq \prod_{\mathfrak{p}|p} K_\mathfrak{p}$.

18. On peut même montrer que l'inclusion $j : X_{K_\mathfrak{p}} \hookrightarrow J_{K_\mathfrak{p}}$ induit un isomorphisme entre l'espace des 1-formes sur $J_{K_\mathfrak{p}}$ et l'espace des 1-formes sur $X_{K_\mathfrak{p}}$.

7 La méthode de Coleman

Les complétés p-adiques peuvent faire encore mieux ; ainsi, Coleman [Col85] est parvenu en 1985 à rendre quantitatif ce résultat de Chabauty, voyons comment. Quitte à renormaliser, on peut supposer que l'équation définissant X est à coefficients *entiers* (algébriques). Soit $\mathfrak{p}$ un idéal maximal de K au dessus d'un nombre premier p pour lequel X admet une *bonne réduction*, c'est-à-dire tel que l'équation de X vue comme une équation sur le corps résiduel $\mathbb{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ définisse encore une courbe irréductible, réduite, et non singulière — si tout ceci effraie le lecteur, il peut se restreindre a cas où $K = \mathbb{Q}$, il s'agit alors tout simplement de réduire modulo p pour p premier. Notons $X_{\mathbb{F}_\mathfrak{p}}$ la courbe ainsi obtenue par réduction ; on montre que son genre est le même que celui de X.

Si ω est une 1-forme sans pôles sur $J_{K_\mathfrak{p}}$, posons, pour tous $P, Q \in X(K_\mathfrak{p})$,

$$\int_P^Q \omega = \int_0^{Q-P} \omega.$$

On définit ainsi une notion d'*intégration le long de la courbe* X ; à titre d'exemple, on a donc

$$\sum_i \int_{P_i}^{Q_i} \omega = 0 \quad \text{dès que } \sum_i (Q_i - P_i) \text{ est un diviseur principal sur } X_{K_\mathfrak{p}}.$$

Comme le rang de J est par hypothèse strictement inférieur au genre de X, $\phi\big(\overline{J(K)}\big)$ est un sous-espace strict de $H^0(J_{K_\mathfrak{p}}, \Omega^1)^*$; il existe donc une forme linéaire non nulle qui s'annule sur ce sous-espace, autrement dit, une 1-forme $\omega \neq 0$ telle que

$$\sum_i \int_{P_i}^{Q_i} \omega = 0 \quad \text{si } \sum_i (Q_i - P_i) \in \overline{J(K)}.$$

Or, si les P_i sont suffisamment proches des Q_i — on démontre qu'en fait, il suffit que P_i se réduise au même point que Q_i sur $\mathbb{F}_\mathfrak{p}$, cette intégrale peut se calculer en développant ω en série entière au voisinage des P_i, et en intégrant terme à terme. En utilisant une *uniformisante* t, c'est-à-dire une fonction s'annulant à l'ordre exactement 1 en P_i [19], on peut donc exprimer l'intégrale

$$\int_{P_i}^{Q_i} \omega$$

19. La notion d'uniformisante est donc le pendant algébrique de la notion de coordonnée locale.

comme une série entière en $t(Q_i)$, dont les coefficients se déduisent de ceux de ω.

Or il existe un procédé appelé *polygone de Newton*, au sujet duquel nous renvoyons le lecteur à [Kob84] pour de plus amples détails, qui permet d'estimer le nombre de zéros d'une série entière sur un corps p-adique par un simple examen de ses coefficients. Coleman utilise ceci pour majorer le nombre de zéros de

$$\int_P^Q \omega$$

pour Q se réduisant au même point que P sur $\mathbb{F}_p$.

Plus précisément, on peut, quitte à multiplier ω par un scalaire, supposer que ω se réduit modulo $\mathfrak{p}$ en une 1-forme non nulle $\widetilde{\omega}$; notons aussi $\widetilde{P} \in X_{\mathbb{F}_\mathfrak{p}}(\mathbb{F}_\mathfrak{p})$ la réduction d'un $P \in X(K_\mathfrak{p})$, et soit t une uniformisante en P. Notons enfin $m_{\widetilde{P}}$ l'ordre d'annulation de $\widetilde{\omega}$ en $\widetilde{P}$. Alors pour tout $Q \in X(K_\mathfrak{p})$ se réduisant aussi à $\widetilde{P}$, l'intégrale

$$\int_P^Q \omega$$

est une série entière en $t(Q)$, dont Coleman montre grâce aux polygones de Newton que si $m_{\widetilde{P}} < p-2$, alors elle a au plus $m_{\widetilde{P}}+1$ zéros. Ainsi, si $m_{\widetilde{P}} < p-2$, il existe au plus $m_{\widetilde{P}}+1$ points de $\overline{J(K)}$ qui se réduisent à $\widetilde{P}$.

C'est le moment de nous souvenir du théorème de Riemann-Roch : le diviseur du coefficient de $\widetilde{\omega}$ représente la classe canonique de $X_{\mathbb{F}_\mathfrak{p}}$, donc est de degré $2g-2$; il est de plus effectif car $\widetilde{\omega}$ n'a pas de pôles. Ainsi, $\widetilde{\omega}$ a $2g-2$ zéros sur $X_{\mathbb{F}_\mathfrak{p}}(\overline{\mathbb{F}_\mathfrak{p}})$, donc

$$\sum_{\widetilde{P} \in X_{\mathbb{F}_\mathfrak{p}}(\mathbb{F}_\mathfrak{p})} m_{\widetilde{P}} \leqslant 2g-2.$$

En particulier, si $p > 2g$, alors la condition $m_{\widetilde{P}} < p-2$ est automatiquement vérifiée, donc

$$|X(K)| \leqslant \sum_{\widetilde{P} \in X_{\mathbb{F}_\mathfrak{p}}(\mathbb{F}_\mathfrak{p})} (m_{\widetilde{P}}+1) \leqslant |X_{\mathbb{F}_\mathfrak{p}}(\mathbb{F}_\mathfrak{p})| + 2g - 2.$$

On obtient ainsi la *borne de Coleman* :

$$|X(K)| \leqslant |X_{\mathbb{F}_\mathfrak{p}}(\mathbb{F}_\mathfrak{p})| + 2g - 2.$$

Cette borne est très bonne, comme nous allons le vérifier pour conclure sur un exemple. Prenons $K = \mathbb{Q}$, et soit X la courbe définie par l'équation

$$y^2 = x(x-1)(x-2)(x-5)(x-6).$$

Une recherche naïve rapide donne dix points rationnels de X :

$(0,0),\ (1,0),\ (2,0),\ (5,0),\ (6,0),\ (3,\pm 6),\ (10,\pm 120)$ et un point à l'infini.

On montre que X est de genre 2, et qu'elle a bonne réduction modulo $7 > 2 \times 2$; de plus sa Jacobienne est de rang 1. On peut donc lui appliquer la méthode de Coleman avec $p = 7$; comme $X_{\mathbb{F}_7}$ a huit points rationnels

$$(0,0),\ (1,0),\ (2,0),\ (5,0),\ (6,0),\ (3,1),\ (3,6) \text{ et } \infty,$$

comme on le vérifie facilement, la borne de Coleman donne

$$|X(\mathbb{Q})| \leqslant 8 + 2 \times 2 - 2 = 10.$$

Ainsi, cette borne est optimale, et la recherche naïve avait bien trouvé tous les points rationnels.

Remerciements

Je suis heureux de remercier Monsieur Jean-Marc Couveignes, qui m'a encouragé à me lancer dans ce beau sujet, ainsi que Monsieur Boas Erez, grâce auquel j'ai enfin découvert la géométrie arithmétique.

Références

[Cha41] Chabauty, Claude, **Sur les points rationnels des courbes algébriques de genre supérieur à l'unité**. C. R. Acad. Sci. Paris 212, (1941). 882–885.

[Col85] Coleman, Robert F., **Effective Chabauty**. Duke Math. J. 52 (1985), no. 3, 765–770.

[Har77] Hartshorne, Robin, **Algebraic geometry**. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977. xvi+496 pp. ISBN : 0-387-90244-9.

[HS00] Hindry, Marc ; Silverman, Joseph H., **Diophantine geometry, An introduction**. Graduate Texts in Mathematics, 201. Springer-Verlag, New York, 2000. xiv+558 pp. ISBN : 0-387-98975-7 ; 0-387-98981-1.

[Kob84] Koblitz, Neal, **p-adic numbers, p-adic analysis, and zeta-functions**. Second edition. Graduate Texts in Mathematics, 58. Springer-Verlag, New York, 1984. xii+150 pp. ISBN : 0-387-96017-1.

[Liu02] Liu, Qing, **Algebraic geometry and arithmetic curves**. Translated from the French by Reinie Erné. Oxford Graduate Texts in Mathematics, 6. Oxford Science Publications. Oxford University Press, Oxford, 2002. xvi+576 pp. ISBN : 0-19-850284-2.