Courte introduction à la Géométrie Arithmétique

Vincent Bouis

Introduction au Domaine de Recherche, DMA ENS

Introduction : La géométrie arithmétique est l'étude des variétés algébriques définies sur les anneaux arithmétiques usuels, tels que $\mathbb{Z}$, $\mathbb{Q}$ ou leurs versions p-adiques $\mathbb{Z}_p$ et $\mathbb{Q}_p$. On présente certaines des idées fondatrices du domaine, dont le nom est réellement apparu au début des années 1970, et qui nous mèneront naturellement à des directions de recherche beaucoup plus actuelles.

1 Introduction

L'arithmétique, ou théorie des nombres, étudie les liens entre l'addition et la multiplication des nombres entiers. Par exemple : alors qu'il est naturel de démontrer un énoncé dépendant d'un entier positif par récurrence, ou de décomposer (multiplicativement) un entier en facteurs premiers, il est beaucoup plus difficile de prévoir la répartition des nombres premiers. Ici "prévoir" est un terme volontairement flou, qui a progressivement changé de sens au gré des quelques générations qui ont pu réfléchir à sa signification. En Grèce antique, la tendance était aux raisonnements élémentaires, et l'on était capable par exemple de démontrer l'existence d'une infinité de nombres premiers. Beaucoup plus tard avec le développement de l'analyse, puis des probabilités, il est devenu possible de formuler et de démontrer bon nombre de résultats plus "statistiques" sur les nombres premiers : par exemple le théorème des nombres premiers fournit un équivalent très simple [1] du nombre de nombres premiers inférieurs à un entier donné.

Ici on s'intéressera à des méthodes plus récentes, et fondées sur la géométrie algébrique développée par Grotendieck dans les années 1960. Ces méthodes ont d'une part l'avantage de fournir des résultats exacts plutôt que des résultats d'existence ou en moyenne, et d'autre part de développer des intuitions géométriques dans des problèmes qui semblaient jusqu'ici concerner

[1] Plus précisément, si $\pi(x) := |\{p \in \mathbb{P} \mid p \leqslant x\}|$, alors $\pi(x) \sim \frac{x}{\ln x}$ when $x \to +\infty$.

uniquement des ensembles (discrets) de nombres entiers. Le principe est simple : on considère, comme sur $\mathbb{R}$ ou $\mathbb{C}$, que le lieu d'annulation d'une famille de polynômes à coefficients entiers définit une variété sur $\mathbb{Z}$. Une application célèbre de ce type de méthodes (et donc de la géométrie arithmétique !) est la résolution par Wiles et Taylor du théorème de Fermat dans les années 1990.

On commence ici par un bref aperçu historique de quelques résultats qui ont inspiré les débuts de la géométrie arithmétique. On présente ensuite en quoi les conjectures de Weil (formulées dans les années 1940) ont ouvert la voie à des liens concrets entre géométrie complexe et arithmétique. Ces mêmes conjectures de Weil fournissent d'ailleurs une grosse part de la motivation de Grothendieck pour refonder la géométrie algébrique, qui unifie dans un cadre commun géométrie complexe et géométrie arithmétique (qui n'était encore pas développée jusqu'ici). On tentera de présenter quelques aspects de ces fondations, et des développements qu'elles ont mené jusqu'à aujourd'hui.

2 Cohomologie des variétés complexes

Pour étudier des variétés, c'est-à-dire des formes géométriques, il est bon de savoir ce que l'on pourrait avoir envie de dire sur ces variétés. Par exemple pour un cercle (dans le plan, un vrai cercle, comme on les connait), on peut parler de son rayon, de son aire, des parties connexes qu'il délimite dans le plan, de ses coordonnées cartésiennes, ou éventuellement de son équation en fonction des coordonnées cartésiennes. Certaines de ces caractéristiques du cercle sont communes à toute une classe de cercles du plan : par exemple le rayon d'un cercle est le même que le rayon de son translaté par un vecteur donné. Et réciproquement, si l'on veut se donner un cercle d'une "taille" donnée, il suffira de se fixer un rayon, et de considérer n'importe quel cercle du plan qui ait ce rayon. La plupart du temps quand on parle d'une variété plus générale, on va aussi chercher à déterminer des caractéristiques de cette variété, que l'on appellera des *invariants*.

Ces invariants ne sont pas faits simplement pour étudier une variété donnée, mais aussi pour les classifier. Parmi les exemples les plus intuitifs d'invariants, on retrouve la dimension, ou le nombre de composantes connexes. Dans le cas de la dimension 2, il est possible de classifier complètement les surfaces réelles lisses et connexes (plus exactement, les surfaces réelles lisses connexes, compactes et sans bord) par le genre, qui est un entier positif et correspond intuitivement au nombre de "trous" de ces surfaces.

Dans ce contexte, une théorie cohomologique[2] est un invariant algébrique sur les variétés de dimension finie quelconque, et qui généralise en particulier les invariants classiques : dimension, nombre de composantes connexes, genre. On précise dans ce qui suit ce qu'on appelle "invariant algébrique", mais on peut déjà garder l'intuition suivante : on associe à chaque variété des objets algébriques (groupes, espaces vectoriels) facilement manipulables, et qui permettent de donner des informations précises sur cette variété. On se restreindra ici aux variétés projectives lisses définies sur $\mathbb{C}$, où certains résultats s'expriment plus joliment :

Définition 2.1. *On dit qu'une variété différentielle sur $\mathbb{R}$ est une* variété lisse sur $\mathbb{C}$ *s'il existe un entier positif n tel que X est localement homéomorphe à la boule unité de $\mathbb{C}^n$. On appelle alors n la dimension de X, et on dira que X est projective si X se plonge dans un espace projectif $\mathbb{P}^N(\mathbb{C})$ pour un certain $N \geqslant 0$.*

Par exemple pour chaque $n \geqslant 0$, $\mathbb{C}^n$ et l'espace projectif $\mathbb{P}^n(\mathbb{C})$ sont des variétés lisses et

[2]Littéralement duale (en un sens algébrique) des théories homologiques ; bien que ce que désigne l'homologie soit apparu plus tôt historiquement, beaucoup de théories s'expriment naturellement selon des conventions cohomologiques (*e.g.*, la cohomologie de de Rham).

projectives sur $\mathbb{C}$, de dimension n ; on peut aussi voir la sphère réelle $\mathbb{S}^2$ comme une variété complexe de dimension 1 (en fait isomorphe à $\mathbb{P}^1(\mathbb{C})$ en tant que variété réelle).

On précise maintenant la forme d'invariant que l'on appelle théorie cohomologique :

Définition 2.2. *À chaque variété projective lisse sur $\mathbb{C}$ de dimension n, on peut associer une suite de $\mathbb{C}$-espaces vectoriels $\mathrm{H}^0(X,\mathbb{C})$, $\mathrm{H}^1(X,\mathbb{C})$, ..., $\mathrm{H}^{2n}(X,\mathbb{C})$. De plus, cette construction est compatible avec la plupart des constructions géométriques que l'on peut faire sur la variété de base X : union, intersection, produit cartésien, etc.*

On appelle $\mathrm{H}^i(X,\mathbb{C})$ le $i^{\text{ème}}$ groupe de cohomologie de X, et sa dimension $b_i := \dim_{\mathbb{C}}\mathrm{H}^i(X,\mathbb{C})$ est appelée $i^{\text{ème}}$ nombre de Betti de X.

On remarque que l'on peut définir plus généralement des groupes de cohomologies $H^i(X,\mathbb{C})$ pour chaque entier $i \in \mathbb{Z}$, qui seront nuls si i n'est pas dans l'intervalle $[\![0; 2\dim_{\mathbb{C}}(X)]\!]$. Ainsi, une théorie cohomologique associe à chaque variété X des espaces vectoriels $\mathrm{H}^i(X,\mathbb{C})$, qui permettent à leur tour –par exemple via leurs dimensions– de retrouver des informations géométriques sur la variété X. Par exemple, l'indice $2n$ du groupe de cohomologie non nul d'indice le plus grand est le double de la dimension n de X ; le nombre de composantes connexes de X correspond à la dimension du $\mathbb{C}$-espace vectoriel $\mathrm{H}^0(X,\mathbb{C})$. De manière similaire, on retrouve le genre d'une surface réelle lisse connexe compacte et sans bord comme la moitié de la dimension du premier groupe de cohomologie associé : $2g = \dim_{\mathbb{C}}\mathrm{H}^1(X,\mathbb{C})$. Remarquons que retenir toute la donnée des espaces vectoriels $\mathrm{H}^i(X,\mathbb{C})$, plutôt que simplement leurs dimensions b_i, est utile dès que l'on considère des inclusions de variété : pour une sous-variété $Y \subseteq X$, on a une inclusion de $\mathbb{C}$-espaces vectoriels $\mathrm{H}^i(Y,\mathbb{C}) \subseteq \mathrm{H}^i(X,\mathbb{C})$ pour chaque $i \in \mathbb{Z}$, ce qui est plus fort qu'une simple inégalité de dimensions, et permet de formuler des résultats précis sur les intersections de sous-variétés.

Mais comment est-ce que l'on définit les groupes de cohomologie $\mathrm{H}^i(X,\mathbb{C})$? C'est là que l'histoire devient intéressante : il existe plusieurs manières indépendantes de définir ces groupes. Historiquement, Poicaré a d'abord défini vers 1900 l'homologie simpliciale et l'homologie singulière. Une trentaine d'années plus tard, la cohomologie de de Rham, fondée sur les formes différentielles, fait son apparition. Intuitivement, ces trois théories (co)homologiques sont des recettes, qui respectent la Définition 2.2, et que l'on utilise au gré des goûts et des contextes. Une question naturelle est alors de demander si ces différentes théories (co)homologiques donnent les mêmes groupes de cohomologie $\mathrm{H}^i(X,\mathbb{C})$. La réponse est positive pour nos variétés complexes projectives lisses. Le résultat a été démontré par Poincaré entre l'homologie singulière et l'homologie simpliciale.

L'homologie simpliciale est définie en recouvrant notre variété X par un nombre fini de simplexes, et en démontrant notamment que la construction des groupes $\mathrm{H}^i_{\mathrm{simp}}(X,\mathbb{C})$ne dépend pas de ce recouvrement. L'homologie singulière est définie en considérant cette fois-ci toutes les fonctions continues d'un simplexe de dimension donnée vers notre variété. Les groupes de cohomologie $\mathrm{H}^i_{\mathrm{sing}}(X,\mathbb{C})$ sont définis comme quotients de ces ensembles de fonctions, et l'isomorphisme $\mathrm{H}^i_{\mathrm{sing}}(X,\mathbb{C}) \cong \mathrm{H}^i_{\mathrm{simp}}(X,\mathbb{C})$ montre en particulier que ce sont des espaces vectoriels de dimensions finies. De la même manière, l'isomorphisme entre ces groupes de cohomologie et les groupes de cohomologie de de Rham implique des relations nouvelles, et souvent non triviales, entre des propriétés géométriques (données par l'homologie singulière ou simpliciale) et des propriétés différentielles (cohomologie de de Rham) d'une variété X.

Exemple 2.3. Par exemple, les nombres de Betti de l'espace projectif $\mathbb{P}^1(\mathbb{C})$ de dimension 1 sur $\mathbb{C}$ sont respectivement : $b_0 = 1$, $b_1 = 0$, $b_2 = 1$. Il est possible de les calculer indépendamment via les constructions de l'homologie simpliciale, singulière, ou de la cohomologie de de Rham. On peut interpréter le fait que $b_1 = 0$ comme le fait que la sphère réelle $\mathbb{S}^2$ est une surface de genre 0.

3 Les conjectures de Weil

Quelque soit la théorie de (co)homologie que l'on utilise pour construire les groupes $\mathrm{H}^i(X, \mathbb{C})$ jusqu'ici (simpliciale, singulière, de Rham), on utilise de manière fondamentale la structure de variété complexe de X. Il est en fait possible de définir certaines de ces constructions sur des corps plus généraux que $\mathbb{R}$ ou $\mathbb{C}$. Mais avant d'en venir à ce genre de constructions, on revient d'avoir sur ce qui a motivé en bonne partie leurs développements. Tout d'abord, remarquons que la notion de "variété" peut être définie sur un corps quelconque k, si l'on restreint aux variétés qui peuvent définies de manière algébrique[3] :

Définition 3.1. *Une variété algébrique projective X définie sur un corps k est le lieu d'annulation d'un nombre fini d'équations polynomiales à coefficients dans k. On remarque ici que le lieu d'annulation est typiquement défini dans un espace projectif de dimension le nombre de variables présentes dans notre famille de polynômes.*

À partir de maintenant, toutes les variétés désignerons des variétés algébriques projectives. Cette notion de variété définies sur un corps k existait et était bien définie au début du XX$^{\text{e}}$ siècle. En particulier, il est possible d'étudier des variétés définies non pas sur $\mathbb{R}$ ou $\mathbb{C}$, mais sur un corps de caractéristique p, comme le corps fini $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Rappelons au passage que tout corps fini a un cardinal égal à une puissance $q = p^k$ d'un nombre premier p, et que, pour un tel cardinal fixé, il existe un unique corps fini à isomorphisme près. Pour une variété (algébrique projective) définie sur un corps fini, remarquons enfin que la situation est bien différente de la situation sur $\mathbb{R}$ ou $\mathbb{C}$: l'espace projectif $\mathbb{P}^N(\mathbb{F}_q)$ a un cardinal fini, égal à $1 + q + \cdots + q^N$, et donc toute variété X de $\mathbb{P}^N(\mathbb{F}_q)$ a un nombre fini de points.

Définition 3.2. *Soit p un nombre premier, et X une variété algébrique projective définie sur le corps $\mathbb{F}_p$. On appelle N_m le nombre de points de X à coefficients dans le corps $\mathbb{F}_{p^m}$, et la fonction zêta de X est :*

$$Z_X(T) := \exp\Big(\sum_{m=1}^{\infty} N_m \frac{T^m}{m}\Big).$$

Remarquons que la situation est similaire à la situation sur $\mathbb{R}$. En effet, pour une variété définie sur $\mathbb{R}$, disons définie par le lieu d'annulation du polynôme x^2+y^2-1 (ou, en coordonnées homogènes, $x^2 + y^2 - z^2$), on peut considérer ses points réels : dans $\mathbb{P}^2(\mathbb{R})$, ça forme le cercle unité de centre $[0 : 0 : 1]$. On peut également considérer ses points complexes, c'est-à-dire à coefficients dans une extension algébrique de $\mathbb{R}$: en plus des points $[x : y : 1] \in \mathbb{P}^2(\mathbb{C})$ qui satisfont $x^2+y^2 = 1$, on obtient deux points "à l'infini" $[1 : i : 0]$ et $[1 : -i : 0]$. Ici, les extensions algébriques de $\mathbb{F}_p$ sont exactement les $\mathbb{F}_{p^m}$ pour $m \geqslant 1$, et on peut faire exactement le même type de construction (sauf que cette fois-ci, il y a un nombre fini de points à coefficients dans $\mathbb{F}_{p^m}$, et donc on peut les compter).

On remarque également que la fonction zêta de la Définition 3.2 est par définition une série entière à coefficients dans $\mathbb{Q}$: $Z_X(T) \in \mathbb{Q}[\![T]\!]$, et peut être interprétée comme une série génératrice des nombres de points N_m.

Exemples 3.3.

- Si X est la variété vide (c'est-à-dire qui n'a aucun point, dans aucune des extensions de $\mathbb{F}_p$), alors $N_m = 0$ pour tout $m \geqslant 1$, et $Z_X(T) = \exp(0) = 1$.
- Si la variété X est réduite à 1 point (y compris dans les extensions $\mathbb{F}_{p^m}$ de $\mathbb{F}_p$), alors $Z_X(T) = \exp(1 + T + \frac{T^2}{2} + \frac{T^3}{3} + \dots) = \exp(\ln(\frac{1}{1-T})) = \frac{1}{1-T}$. Remarquons que bien

[3] C'est en fait un sujet de recherche encore actif de pouvoir dire si des variétés différentielles (sur $\mathbb{R}$ ou $\mathbb{C}$ typiquement) peuvent être exprimées, à isomorphisme près, comme lieu d'annulation d'un ensemble de polynômes.

qu'exprimée sous forme d'une fraction rationnelle, il est toujours possible de voir $\frac{1}{1-T}$ comme la série entière $1 + T + T^2 + T^3 + \cdots \in \mathbb{Q}[\![T]\!]$.

- Si $X = \mathbb{A}^n(\mathbb{F}_p)$ est l'espace affine de dimension n sur $\mathbb{F}_p$, alors $N_m = p^{nm}$ pour tout $m \geqslant 1$, et on montre de la même manière que :

$$Z_{\mathbb{A}^n(\mathbb{F}_p)}(T) = \frac{1}{1 - p^n T}.$$

- Si $X = \mathbb{P}^n(\mathbb{F}_p)$ est l'espace projectif de dimension n sur $\mathbb{F}_p$, alors $N_m = 1+p+p^2+\cdots+p^n$, et

$$Z_{\mathbb{P}^n(\mathbb{F}_p)}(T) = \frac{1}{(1-T)(1-pT)\dots(1-p^nT)}.$$

  Il est possible de déduire ce calcul de l'exemple précédent, en remarquant que $Z_{A \amalg B}(T) = Z_A(T)Z_B(T)$ pour des variétés disjointes A et B, et que $\mathbb{P}^n(\mathbb{F}_p) = \mathbb{A}^0(\mathbb{F}_p) \amalg \cdots \amalg \mathbb{A}^n(\mathbb{F}_p)$.

Nous sommes maintenant parés pour énoncer les conjectures de Weil. Ce dernier les a formulées vers 1940, comme déduction de nombreux calculs des fonctions zêtas de certaines variétés particulières. Une première partie du travail pour formuler ces conjectures consistait à faire sens d'hypothèses géométriques telles que "lisse", ou "connexe", sur notre variété X, quand bien même celle-ci est définie sur $\mathbb{F}_p$ et n'a qu'un nombre fini de points. Il s'avère que cette partie de l'histoire n'est pas la plus ardue : il est possible de définir ces notions de manière purement algébrique, et qui s'applique ainsi à des variétés définies sur n'importe quel corps. Par exemple, la lissitude d'une variété s'exprime en fonction de la nullité du déterminant de la jacobienne associée à notre famille de polynômes ; de la même manière on peut définir, comme sur $\mathbb{R}$ ou $\mathbb{C}$, la dimension d'une variété lisse et connexe définie sur $\mathbb{F}_p$. On a alors les énoncés suivants :

Théorème 3.4. (Conjectures de Weil) *Soit X une variété algébrique projective sur $\mathbb{F}_p$, que l'on suppose connexe, lisse et de dimension n. Remarquons que l'hypothèse de connexité est là uniquement pour faciliter l'expression des énoncés suivants, puisque la fonction zêta se comporte très bien avec les unions disjointes.*

- (Rationalité) *$Z_X(T)$ est une fraction rationnelle en T, i.e., est le quotient de deux polynômes à coefficients rationnels.*

- (Hypothèse de Riemann) *Il est possible d'écrire $Z_X(T)$ sous la forme :*

$$Z_X(T) = \frac{P_1(T)P_3(T)\dots P_{2n-1}(T)}{P_0(T)P_2(T)\dots P_{2n}(T)}$$

  où $P_0(T) = 1 - T$, $P_{2n}(T) = 1 - p^nT$, et $P_i(T)$ est un polynôme à coefficients entiers, et a des racines complexes $\alpha_{i,j}$ toutes de module $p^{-i/2}$.

- (Equation fonctionnelle) *Soit $\chi := \sum_i (-1)^i \deg P_i$ la "caractéristique d'Euler-Poicaré" de X. Alors $Z_X(T)$ vérifie l'équation :*

$$Z_X(\frac{1}{q^nT}) = \pm q^{n\chi/2} T^\chi Z_X(T).$$

- (Nombres de Betti) *Soit $B_i := \deg P_i$. On suppose que X est obtenue à partir d'une famille de polynômes à coefficients dans $\mathbb{Z}$ par réduction modulo p. Cette famille de polynômes définit une variété algébrique complexe Y (i.e., on considère le lieu d'annulation sur $\mathbb{C}$ de cette famille de polynômes à coefficients entiers), de nombres de Betti $b_i = \dim_{\mathbb{C}} \mathrm{H}^i(Y, \mathbb{C})$. Alors $b_i = B_i$ pour tout i.*

Quelques remarques s'imposent. Tout d'abord, la seconde conjecture implique la première, bien que celle-ci ait été démontré plus tôt historiquement. On appelle la seconde "Hypothèse de Riemann" (ou "Hypothèse de Riemann sur les corps finis") car, dans le cas d'une courbe (*i.e.*, $n = 1$), et en posant le changement de variable usuel[4] $T = p^{-s}$, la condition $|T| = p^{-1/2}$ sur les racines de $Z_X(T)$ redonne la condition classique $\mathrm{Re}(s) = \frac{1}{2}$.

De plus, la condition sur le module des racines de P_i détermine le polynôme P_i uniquement à constante près (et sous réserve d'existence) : en tant que fraction rationnelle sur $\mathbb{C}$, et donc sur $\mathbb{Q}$ ou $\mathbb{Z}$, l'expression $\frac{P_1(T)P_3(T)...P_{2n-1}(T)}{P_0(T)P_2(T)...P_{2n}(T)}$ est nécessairement irréductible ; on peut alors identifier $P_i(T)$ comme produit des facteurs irréductibles (sur $\mathbb{C}$) ayant des racines de module exactement $p^{-i/2}$. Il s'agit donc de montrer ici que les racines et les pôles de $Z_X(T)$, en supposant sa rationalité, ont toutes et tous des modules une puissance entière de $\frac{1}{\sqrt{p}}$, dont la parité est alternée régulièrement.

L'équation fonctionnelle est analogue à l'équation fonctionnelle sur la fonction zêta de Riemann $\zeta(s)$, bien qu'elle fasse ici apparaître une constante χ de nature plus géométrique.

La conjecture sur les nombres de Betti fournit l'interprétation géométrique de l'Hypothèse de Riemann, et forme ce qu'il y a de plus profond dans les conjectures de Weil. On interprète les degrés de polynômes $P_i(T)$, définis de manière formelle à partir du nombre de points fini de notre variété sur $\mathbb{F}_{p^m}$ (une donnée complètement discrète, donc), comme des données purement géométriques –les nombres de Betti– d'une variété complexe. Une conséquence absolument non triviale de cette interprétation géométrique est la suivante. Si l'on part d'une famille de polynômes sur $\mathbb{Z}$ (avec des bonnes propriétés pour que toutes la variétés soient lisses, projectives, ...), alors on peut construire notre variété complexe Y et considérer ses nombres de Betti b_i. D'autre part on peut considérer la réduction modulo p de ces polynômes, et former la fonction la fonction zêta de la variété obtenue sur $\mathbb{F}_p$. Ce que nous disent les conjectures de Weil est alors que non seulement on peut relier très concrètement ces informations, mais aussi que les degrés des polynômes $P_i(T)$, qui ne dépendent que de Y, ne dépendent pas du nombre premier p choisi.

La formulation de ces conjectures suggère l'existence d'une théorie cohomologique, similaire à la cohomologie des variétés qui existait alors sur $\mathbb{C}$, et qui s'applique également aux variétés définies sur un corps fini. Comme l'a suggéré Weil lui-même, l'existence d'une théorie cohomologique qui satisferait de bonnes propriétés, et qui serait compatible en un certain sens avec les théories cohomologiques sur $\mathbb{C}$ (*e.g.*, la cohomologie singulière), permettrait de démontrer ces conjectures. Seulement, si définir des variétés sur un corps fini était possible dans les années 1940, la géométrie algébrique –qui étudie les variétés algébriques– manquait encore de fondations générales suffisantes. C'est ce que va entreprendre Grothendieck dans les années 1960 (largement motivé par la compréhension des conjectures de Weil), et qui donne naissance à la théorie des schémas.

4 Un peu de schémas

La notion de schéma est une généralisation de celle de variété, et qui peut être définie en particulier sur n'importe quel anneau plutôt que seulement sur un corps. En particulier, il est possible de parler de schéma sur l'anneau des entiers $\mathbb{Z}$, où des équations diophantiennes prennent un sens géométrique beaucoup plus concret. Par exemple on peut considérer le schéma associé à l'anneau $\mathbb{Z}$ lui-même, et dont les points sont en bijection avec les nombres premiers, plus un point "à l'infini" (qui correspond intuitivement au corps $\mathbb{Q}$ de charactéristique 0) : c'est le début de la *géométrie arithmétique* à proprement parler.

[4] Dans le contexte des fonctions zêtas.

Une idée centrale de la théorie est de redéfinir les variétés sous une forme plus intrinsèque, c'est-à-dire ne dépendant plus d'un espace de définition. Ainsi, on définit le cercle $\mathbb{S}^1$ non plus comme un ensemble de points dans le plan (réel, complexe, ou même sur $\mathbb{F}_p$), mais seulement par rapport à sa définition algébrique, donnée par le polynôme x^2+y^2-1 à coefficients entiers. Pour retrouver les points réels du cercle, on considérera alors les *idéaux maximaux* de l'anneau $\mathbb{R}[x,y]/(x^2+y^2-1)$. On remarque en effet que pour un point $(a,b) \in \mathbb{R}^2$ qui vérifie $a^2+b^2=1$, l'idéal $(x-a, y-b) \subset \mathbb{R}[x,y]$ engendré par $x-a$ et $y-b$ est un idéal maximal de $\mathbb{R}[x,y]$, et contient (x^2+y^2-1) si et seulement si $a^2+b^2-1=0$. Il est possible de définir de la même manière les schémas dits "affines", c'est-à-dire qui se plongent dans un espace affine de dimension finie. Ceux-ci seront définis par un anneau de polynômes, dont l'ensemble des points correspondront aux idéaux maximaux[5]. Par exemple, les points du schéma $\mathbb{A}^n_{\urcorner}$ correspondant à l'espace affine k^n de dimension n sur un corps k sont en bijection avec les idéaux maximaux de l'anneau $k[x_1,\ldots,x_n]$. Lorsque le corps k est algébriquement clos, ces idéaux maximaux sont en bijection avec les n-uplets $(a_1,\ldots,a_n) \in k^n$, et on retrouve la définition classique de l'espace affine. Lorsque le corps k n'est pas algébriquement clos, des points supplémentaires apparaissent dans le schéma $\mathbb{A}^n_k$: par exemple pour $k=\mathbb{R}$ et $n=1$, l'idéal $(x^2+1) \subset \mathbb{R}[x]$ est maximal ($\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$ est un corps), mais n'est pas de la forme $(x-a)$ pour un certain $a \in \mathbb{R}$. Ce nouveau "point" de $\mathbb{A}^1_{\mathbb{R}}$ correspond intuitivement à une paire de points complexes conjugués de la droite affine : si l'on tensorise par $\mathbb{C}$ l'anneau $\mathbb{R}[x]$, on obtient l'anneau de polynômes $\mathbb{C}[x] = \mathbb{R}[x] \otimes_{\mathbb{R}} \mathbb{C}$ dans lequel l'idéal (x^2+1) se scinde en les idéaux maximaux $(x+i)$ et $(x-i)$.

Pour construire des schémas plus généraux que des schémas affines (comme des schémas projectifs, tels que $\mathbb{P}^n_{\mathbb{Z}}$), on "recolle" des parties affines entre elles. La construction formelle de ce recollage est elle aussi purement algébrique, et utilise la notion de faisceaux que l'on ne détaillera pas ici. Il est alors possible de formaliser, dans le langage des schémas, les notions de dimension, de lissitude et de connexité que l'on avait utilisé dans la formulation des conjectures de Weil.

Le fait d'avoir défini les schémas (*i.e.*, la notion de variété) de manière aussi générale permet d'avoir un cadre commun pour étudier non seulement des variétés définies sur des corps archimédéens (comme $\mathbb{R}$, ou $\mathbb{C}$), mais aussi les variétés définies sur des corps finis $\mathbb{F}_q$, ou sur $\mathbb{Z}$: c'est un premier pas pour non seulement démontrer, mais aussi *comprendre* les conjectures de Weil.

Seulement un problème se pose : là où on définissait nos théories cohomologiques sur les variétés complexes à l'aide de procédés analytiques (formes différentielles, fonctions continues), tous nos schémas sont maintenant définis de manière complètement algébriques. Il existe bien une topologie naturelle sur les schémas, appelée topologie de Zariski, mais qui est trop grossière pour espérer démontrer des résultats assez fins pour les conjectures de Weil.

Pour y remédier, Grothendieck introduit une notion affaiblie de "topologie" (appelée topologie de Grothendieck), et en particulier la notion de topologie étale. Dans ce contexte, il developpe avec Artin la *cohomologie étale*, qui s'applique en particulier aux variétés définies sur des corps de caractéristique p (comme $\mathbb{F}_p$). Le but de cette cohomologie étale est notamment de fournir la machinerie nécessaire à la démonstration des conjectures de Weil. Ce programme est finalisé par Deligne au début des années 1970 avec la preuve de l'hypothèse de Riemann sur les corps finis ; on ne détaillera pas cette preuve, qui dépasse d'assez loin le niveau de cette exposition.

[5]La définition de schéma fait intervenir tous les idéaux premiers (et pas seulement les idéaux maximaux) de cet anneau. L'ensemble des idéaux premiers d'un anneau A est appelé le spectre de cet anneau, et est noté $\mathrm{Spec}(A)$.

5 Quelles implications pour l'arithmétique ?

Revenons à des considérations plus arithmétiques. Gauss démontre en 1801 la célèbre loi de réciprocité quadratique :

Théorème 5.1. (Loi de réciprocité quadratique) *Soient ℓ et p deux nombres premiers impairs distincts.*

(1). Si ℓ ou p est congru à 1 modulo 4, alors ℓ est un carré modulo p si et seulement si p est un carré modulo ℓ.

(2). Si ℓ et p sont congrus à 3 modulo 4, alors ℓ est un carré modulo p si et seulement si p n'est pas un carré modulo ℓ.

Celle-ci affirme en particulier qu'il est possible de déterminer "rapidement" si un entier est un entier modulo un nombre premier p. Par exemple, 3 est un carré modulo 13 (ou plus généralement modulo tout nombre premier congru à 1 modulo 12) puisque $13 \equiv 1[4]$ et $13 \equiv 1 \equiv 1^2[3]$.

De manière moins pragmatique, la loi de réciprocité quadratique permet de déceler une régularité dans la répartition des nombres premiers : non pas dans leurs tailles, mais dans leurs propriétés algébriques. La reformulation suivante peut clarifier la situation :

Corollaire 5.2. *Soit $n \in \mathbb{Z}$ un entier, et N la fonction qui à un nombre premier p associe le nombre $N(p)$ de solutions de l'équation $x^2 \equiv n[p]$. Alors la fonction N est "périodique" : elle ne dépend que de la classe de congruence de p modulo $4n$.*

Proof. Comme $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ est un corps, le nombre $N(p)$ est véritablement le nombre de racines du polynômes $x^2 - n \in \mathbb{F}_p[x]$, qui est égal à 0 (si n n'est pas un carrément modulo p), 1 (si n a une racine double modulo p) ou 2 (si n a deux racines carrées modulo p). La seule racine carrée double possible modulo p doit être égale à son contraire, et donc $N(p) = 1$ si et seulement si p divise n (ce qui se produit pour un nombre fini de nombres premiers p). Remarquons que ce cas se produit exactement lorsque p est un diviseur premier de n, ce qui se détecte tout à fait à partir de la classe de p modulo $4n$. De manière similaire, le cas $p = 2$ est trivial à traiter dans notre cas.

Si p est impair et premier avec n, on peut alors déterminer si n est un carré ou non modulo p en décomposant n en facteurs premiers, en utilisant le fait que le sous groupe des carrés modulo p est d'indice 2 dans $(\mathbb{Z}/p\mathbb{Z})^\times$, et en utilisant la loi de réciprocité quadratique. En particulier, on utilise alors uniquement la classe de congruence de p modulo n (pour déterminer si p est un carré ou non modulo chacun des facteurs premiers de n) et modulo 4 (pour appliquer la loi de réciprocité quadratique). Le fait que n soit un carré ou non modulo p ne dépend donc que de la classe de congruence de p modulo $4n$[6]. ◆

De nombreuse preuves de la loi de réciprocité quadratique ont été données (par Gauss, et depuis). Parmi les plus récentes interprétations (et preuves) de ce résultat, on peut citer la reformulation en termes de groupes de Galois. Ainsi le polynôme $x^2 - n \in \mathbb{Q}[x]$, pour un entier $n \in \mathbb{Z}$, définit une extension de corps $\mathbb{Q}(\sqrt{n})$ de $\mathbb{Q}$: de degré 1 si n est un carré dans $\mathbb{Q}$ (on dit que c'est une extension triviale), ou de degré 2 dans le cas contraire. Intuitivement, on ajoute une racine au polynôme $x^2 - n$, c'est-à-dire une racine carrée de n, au corps de base $\mathbb{Q}$. Plus généralement on associe une extension de corps $K_f := \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ de $\mathbb{Q}$ à tout polynôme $f \in \mathbb{Z}[x]$, où K_f est engendré par les racines complexes α_i de f. À de telles extensions de corps on peut associer un groupe de Galois $\mathrm{Gal}(K_f/\mathbb{Q})$, qui classifie les symétries algébriques des racines

[6] On utilise ici secrètement la loi de réciprocité quadratique "secondaire", qui traite du cas où p ou ℓ peut être égal à 2 ; les facteurs 2 se compensent tout à fait gentiment.

α_i. On dira que le polynôme $f \in \mathbb{Z}[x]$ est *abélien* si le groupe de Galois associé $\mathrm{Gal}(K_f/\mathbb{Q})$ est un groupe abélien. Par exemple $\mathrm{Gal}(\mathbb{Q}(\sqrt{n})/\mathbb{Q})$ est soit trivial (si n est un carré dans $\mathbb{Q}$) soit isomorphe à $\mathbb{Z}/2\mathbb{Z}$ (si n n'est pas un carré dans $\mathbb{Q}$), et donc le polynôme $x^2 - n \in \mathbb{Z}[x]$ est abélien pour tout $n \in \mathbb{Z}$. On a alors la généralisation suivante de la loi de réciprocité quadratique :

Théorème 5.3. (Loi de réciprocité abélienne) *Soit $f \in \mathbb{Z}[x]$ un polynôme abélien. Alors $\{p \in \mathbb{P} \mid f$ has $n := \deg(f)$ roots modulo $p\}$ peut être décrit uniquement via des congruences modulo N_f, où $N_f \in \mathbb{N}$ est un entier qui ne dépend que de f.*

Remarque 5.4. Pour $f = x^2 - n$, l'entier N_f est égal à $4n$, et la description est détaillée dans la preuve du Corollaire 5.2.

Par glissement terminologique, on appelle maintenant une "loi de réciprocité" un résultat qui prédit toutes sortes de structures sur les variations, quand p varie, du nombre de solutions modulo p d'une équation algébrique $f(x_1, \ldots, x_n) = 0$. C'est précisément ici que la géométrie arithmétique entre en jeu : une telle équation algébrique définit une variété (ou plus précisément un schéma) sur l'anneau des entiers $\mathbb{Z}$. Il est possible de compter le nombre de points de ce schéma, une fois réduit modulo un certain nombre premier p[7]. La question est alors ici de prédire comment ce nombre de points évolue lorsque p varie.

La reformulation de nos lois de réciprocité en termes de groupes de Galois n'est pas anodine. Beaucoup de problèmes en arithmétique se reformulent aisément en termes de groupes de Galois (*e.g.*, le groupe de Galois "absolu" $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ de $\mathbb{Q}$, où $\overline{\mathbb{Q}}$ est une clôture algébrique de $\mathbb{Q}$). En fait, comme il est généralement compliqué d'exprimer des éléments explicites des groupes de Galois (on connait essentiellement l'identité, la conjugaison complexe et le Frobenius dans certains contextes), on préfère étudier les *représentations* des groupes de Galois plutôt que les groupes de Galois eux-mêmes. Par exemple, pour un groupe abélien fini G (comme les groupes de Galois du Théorème 5.3), l'ensemble des morphismes de groupes $G \to \mathbb{C}^\times \cong \mathrm{GL}_1(\mathbb{C})$ est en bijection avec le groupe G lui-même. Si G est un groupe de Galois (c'est-à-dire le groupe des automorphismes d'une extension de corps galoisienne), ces morphismes de G vers $\mathrm{GL}_1(\mathbb{C})$ sont appelés *représentations galoisiennes de degré* 1. En particulier ces représentation galoisiennes sont définies pour des groupes de Galois pas nécessairement abéliens. De la même manière, les morphismes $G \to \mathrm{GL}_n(\mathbb{C})$ sont des *représentations galoisiennes de degré n.*

L'étude des représentations galoisiennes est un sujet ardent en géométrie arithmétique, notamment depuis le lien conjectural proposé par Langlands entre représentations galoisiennes et représentations automorphes (qui sont des objects en analyse, également très profonds, mais qui a priori n'ont pas de lien direct avec l'arithmétique). Une partie du programme de Langlands a pour but de construire de manière systématique des lois de réciprocité (qui généralisent en particulier celles des Théorèmes 5.1 et 5.3). Il existe aujourd'hui, comme conséquences de ces constructions, de nombreuses loi de réciprocité "non-abéliennes". L'intérêt du programme de Langlands ici est de fournir une interprétation beaucoup plus profonde des lois de réciprocité : alors que la plupart des preuves se faisaient jusqu'ici essentiellement à la main (quoique avec des mains très habiles), elles sont maintenant des conséquences d'idées géométriques. Comme on l'a dit précédemment, on compte en effet les nombres de points de certaines variétés modulo p. Ce que fait le programme de Langlands est ici de se faire correspondre deux variétés a priori non reliées ; et c'est en calculant des nombres de points sur ces variétés que l'on retrouve nos lois de réciprocité.

Que vient faire la géométrie arithmétique dans tout ça ? Déjà, elle permet de formaliser toutes les idées de "variétés sur $\mathbb{F}_p$", et tout un tas d'autres propriétés géométriques qui, en

[7] Plus précisément, on passe du schéma $X = \mathrm{Spec}(\mathbb{Z}[x_1, \ldots, x_n]/(f(x_1, \ldots, x_n)))$ au schéma $X_{\mathbb{F}_p} := X \times_{\mathrm{Spec}(\mathbb{Z})} \mathrm{Spec}(\mathbb{F}_p) = \mathrm{Spec}(\mathbb{F}_p[x_1, \ldots, x_n]/(f(x_1, \ldots, x_n)))$.

un sens, sont bien plus riches que sur $\mathbb{R}$ ou $\mathbb{C}$[8]. Par exemple la cohomologie étale des variétés algébriques forment bon nombre d'exemples de représentations galoisiennes ; un exemple fameux en est la démonstration du théorème de Fermat, qui passe par l'étude de la représentation galoisienne donnée par la cohomologie étale d'une courbe elliptique. D'autre part, beaucoup d'idées arithmétiques (et typiquement provenant du programme de Langlands) ont motivé le développement de certaines parties de la géométrie algébrique ou arithmétique, comme la théorie des motifs, devenue ensuite centrale dans le programme de Langlands.

References

[BMS19] Bhargav Bhatt, Matthew Morrow, and Peter Scholze. "Topological Hochschild homology and integral p-adic Hodge theory". In: *arXiv:1802.03261 [math]* (Apr. 2019). arXiv: 1802.03261. URL: http://arxiv.org/abs/1802.03261 (visited on 08/12/2020).

[Del74] Pierre Deligne. "La conjecture de Weil : I". fr. In: *Publications Mathématiques de l'IHÉS* 43 (1974), pp. 273–307. URL: http://www.numdam.org/item/PMIHES_1974__43__273_0/ (visited on 10/03/2020).

[GD71] A. Grothendieck and Jean Dieudonné. *Éléments de géométrie algébrique*. Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen Bd. 166. Berlin, New York: Springer-Verlag, 1971. ISBN: 978-3-540-05113-8.

[Lan] Robert Langlands. *Le programme de Langlands*. fr. Publisher: Pour la Science. URL: https://www.pourlascience.fr/sd/mathematiques/le-programme-de-langlands-1060.php (visited on 10/03/2020).

[Sit] Analysis Situs. *Analysis Situs*. URL: http://analysis-situs.math.cnrs.fr/ (visited on 10/03/2020).

[8] Par exemple, il est possible d'interpréter géométriquement des classes de torsion dans les groupes de cohomologie de variétés réelles ou complexes.